

bitdefender



INTERNET SECURITY₂₀₀₉

Guia de usuário

 **bitdefender**



BitDefender Internet Security 2009

Guia de usuário

Publicado 2009.01.05

Copyright© 2009 BitDefender

Nota Legal

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

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

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

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



BitDefender Internet Security 2009





Índice

Acordo de Licença de Software para Usuários Finais	x
Prefácio	xv
1. Convenções usadas neste livro	xv
1.1. Convenções tipográficas	xv
1.2. Avisos	xvi
2. A Estrutura do Livro	xvi
3. Convite a Comentários	xvii
Instalação	1
1. Requisitos de Sistema	2
1.1. Requisitos do Sistema	2
1.2. Requisitos de Software	3
2. Instalar BitDefender	4
2.1. Assistente de Registro	6
2.1.1. Passo 1/2 - Registrar BitDefender Internet Security 2009	7
2.1.2. Passo 2/2 - Criar uma conta BitDefender	8
2.2. Assistente de Configuração	10
2.2.1. Passo 1/9 - Janela Boas-vindas	11
2.2.2. Passo 2/9 - Escolher Modo de Visão	12
2.2.3. Passo 3/9 - Configurar a Rede BitDefender	13
2.2.4. Passo 4/9 - Configurar o Controle de Identidade	14
2.2.5. Passo 5/9 - Configurar o Controle dos Pais	17
2.2.6. Passo 6/9 - Configurar Relatório de Vírus	19
2.2.7. Passo 7/9 - Seleccionar as Tarefas a Serem Executadas	20
2.2.8. Passo 8/9 - Esperar que as Tarefas Terminem	21
2.2.9. Passo 9/9 - Terminar	22
3. Atualização de versão	23
4. Remover ou Reparar o BitDefender	24
Administração básica.	26
5. Introdução	27
5.1. Iniciar o BitDefender Internet Security 2009	27
5.2. Modo de Visão do Interface do usuário	27
5.2.1. Modo Básico	27
5.2.2. Modo Avançado	29
5.3. Ícone BitDefender na Área de Notificação	32
5.4. Barra de Actividade da Análise	33



5.5. Análise Manual BitDefender	33
5.6. Modo de Jogo	34
5.6.1. Usar o Modo de Jogo	34
5.6.2. Mudar a Hotkey do Modo de Jogo	35
5.7. Integração com Clientes de Mail	35
5.7.1. Barra de ferramentas Antispam	35
5.7.2. Assistente de Configuração Antispam	44
5.8. Integração com Exploradores web	49
5.9. Integração com Messenger	51
6. Painel	53
6.1. Sumário	125
6.2. Tarefas	55
6.2.1. A analisar com BitDefender	55
6.2.2. Actualizar o BitDefender	56
7. Segurança	58
7.1. Componentes Monitorizados	58
7.1.1. Segurança Local	114
7.1.2. Segurança On-line	115
7.1.3. Analisar Vulnerabilidades	117
7.2. Tarefas	62
7.2.1. A analisar com BitDefender	63
7.2.2. Actualizar o BitDefender	63
7.2.3. Procurar Vulnerabilidades	65
8. Parental	73
8.1. Componentes Monitorizados	73
8.1.1. Controle dos Pais	74
8.2. Tarefas	75
8.2.1. A analisar com BitDefender	75
8.2.2. Actualizar o BitDefender	76
9. Cofre de arquivos	78
9.1. Componentes Monitorizados	79
9.1.1. Cofre de arquivos	116
9.2. Tarefas	80
9.2.1. Adicionar arquivos ao Cofre	81
9.2.2. Remover arquivos do Cofre	87
9.2.3. Ver arquivos do Cofre	92
9.2.4. Fechar o Cofre	96
10. Rede	100
10.1. Tarefas	100
10.1.1. Aderir à Rede BitDefender	101
10.1.2. Adicionar Computadores à Rede BitDefender	102
10.1.3. Gerir a Rede BitDefender	104



10.1.4. Analisar Todos os Computadores	106
10.1.5. Actualizar Todos os Computadores	107
10.1.6. Registrar Todos os Computadores	108
11. Definições Básicas	109
11.1. Segurança Local	110
11.2. Segurança On-line	110
11.3. Definições do Controle dos Pais	111
11.4. Definições de rede	111
11.5. Definições do Cofre de arquivos	111
11.6. Configurações Gerais	112
12. Barra de Estado	114
12.1. Segurança Local	114
12.2. Segurança On-line	115
12.3. Cofre de arquivos	116
12.4. Analisar Vulnerabilidades	117
13. Registro	119
13.1. Passo 1/1 - Registrar BitDefender Internet Security 2009	119
14. Histórico	121
Administração Avançada	123
15. Geral	124
15.1. Painel	124
15.1.1. Estatísticas	125
15.1.2. Sumário	125
15.2. Opções	126
15.2.1. Configurações Gerais	127
15.2.2. Configurações do Relatório de Vírus	129
15.3. Informação do Sistema	129
16. Antivírus	131
16.1. Protecção em Tempo-real	131
16.1.1. Configurar Nível de Protecção	132
16.1.2. Personalizando Nível de Protecção	133
16.1.3. Configurar o Analisador Comportamental	137
16.1.4. Desactivando a Protecção em Tempo-real	140
16.1.5. Configurar Protecção Antiphishing	140
16.2. Análise A-pedido	141
16.2.1. Tarefas de Análise	143
16.2.2. Usando o Menú de Atalho	145
16.2.3. Criando Tarefas de Análise	146
16.2.4. Configurar Tarefas de Análise	146
16.2.5. Analisar objectos	159



16.2.6. Ver os Relatórios da Análise	165
16.3. Objectos a Excluir da Análise	167
16.3.1. Excluir Caminhos da Análise	169
16.3.2. Excluir Extensões da Análise	172
16.4. Área de Quarentena	176
16.4.1. Gerir arquivos em Quarentena	177
16.4.2. Configurar opções da Quarentena	178
17. Antispam	180
17.1. Compreender o Antispam	180
17.1.1. Filtros Anti-spam	180
17.1.2. Operação Antispam	182
17.2. Status	184
17.2.1. Definir Nível de Protecção	185
17.2.2. Configurar a Lista de Amigos	187
17.2.3. Configurar a lista de Spammers	188
17.3. Opções	190
17.3.1. Configurações de Antispam	192
17.3.2. Filtros Antispam Básicos	192
17.3.3. Filtros Antispam Avançados	192
18. Controle dos Pais	194
18.1. Definir Estado por usuário	195
18.1.1. Proteger as Definições do Controle dos Pais	197
18.1.2. Configurar Filtro Web Heurístico	198
18.2. Controle Web	199
18.2.1. Assistente de Configuração	200
18.2.2. Especifique as exceções	201
18.2.3. Lista Negra Web BitDefender	202
18.3. Controle de Aplicações	203
18.3.1. Assistente de Configuração	204
18.4. Filtragem Palavra-chave	204
18.4.1. Janela de configuração	205
18.5. Controle de Mensagens Instantâneas (IM)	207
18.5.1. Janela de configuração	208
18.6. Limitador de Horário Web	209
19. Controle Privacidade	211
19.1. Estado do Controle de Privacidade	211
19.1.1. Configurar Nível de Protecção	212
19.2. Controle de Identidade	213
19.2.1. Criar Regras de Identidade	215
19.2.2. Definir Excepções	218
19.2.3. Gerir Regras	219
19.3. Controle de Registro	220
19.4. Controle de Cookie	222



19.4.1. Janela de configuração	224
19.5. Controle de Scripts	226
19.5.1. Janela de configuração	227
20. Firewall	229
20.1. Opções	229
20.1.1. Definir a Acção por Defeito	231
20.1.2. Configuração Avançada da Firewall	232
20.2. Rede	234
20.2.1. Alterar o Nível de Confiança	235
20.2.2. Configurar o Modo Stealth	236
20.2.3. Configurar Definições Gerais	236
20.2.4. Zonas de Rede	236
20.3. Regras	237
20.3.1. Adicionar Regras Automaticamente	240
20.3.2. Apagar Regras	240
20.3.3. Criar e Modificar Regras	240
20.3.4. Gestão Avançada de Regras	244
20.4. Controle de Conexão	246
21. Encriptação	248
21.1. Encriptação de Mensagens Instantâneas (IM)	248
21.1.1. Desativar a Encriptação para usuários Especificos	250
21.2. Cofre de arquivos	250
21.2.1. Criar um Cofre	251
21.2.2. Abrir um Cofre	253
21.2.3. Fechar um Cofre	253
21.2.4. Mudar senha do Cofre	254
21.2.5. Adicionar arquivos ao Cofre	255
21.2.6. Remover arquivos do Cofre	255
22. Vulnerabilidade	256
22.1. Status	256
22.1.1. Consertando pontos vulneráveis	257
22.2. Opções	264
23. Modo de Jogo / Portátil	266
23.1. Modo de Jogo	266
23.1.1. Configurar Modo de Jogo Automático	267
23.1.2. Gerir a Lista de Jogos	268
23.1.3. Configurar as Definições do Modo de Jogo	270
23.1.4. Mudar a Hotkey do Modo de Jogo	270
23.2. Modo de Portátil	271
23.2.1. Configurar Definições do Modo de Portátil	272
24. Rede	274
24.1. Aderir à Rede BitDefender	275



24.2. Adicionar Computadores à Rede BitDefender	275
24.3. Gerir a Rede BitDefender	277
25. Atualização	280
25.1. Atualização Automática	280
25.1.1. Solicitar uma Actualização	282
25.1.2. Desabilitar Atualização Automática	282
25.2. Opções de Actualização	283
25.2.1. Definir local para atualização	284
25.2.2. Configurar Atualização Automática	284
25.2.3. Configurar Atualização Manual	285
25.2.4. Configurar Opções Avançadas	285
25.2.5. Gerir Proxies	285
26. Registro	288
26.1. Registrar BitDefender Internet Security 2009	289
26.2. Criar uma conta BitDefender	290
Ajuda	293
27. Suporte	294
27.1. BitDefender Knowledge Base	294
27.2. Pedir Ajuda	294
27.2.1. Vá até ao Self-Service Web	294
27.2.2. Abrir um ticket de suporte	295
27.3. Informação sobre contato	295
27.3.1. Brasil	296
CD de Resgate BitDefender	297
28. Sumário	298
28.1. Requisitos de Sistema	298
28.2. Software incluído	299
29. Como Usar o CD de Emergência BitDefender	302
29.1. Iniciar CD de Resgate BitDefender	302
29.2. Parar o CD de Resgate BitDefender	303
29.3. Como executo uma verificação antivírus?	304
29.4. Como posso configurar a Ligação à Internet?	305
29.5. Como eu posso atualizar o BitDefender?	306
29.5.1. Como posso actualizar o BitDefender através de um proxy?	307
29.6. Como posso salvar os meus dados?	308
Glossário	311



Acordo de Licença de Software para Usuários Finais

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

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

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

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

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

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

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



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

LICENÇA DE USUÁRIO DE COMPUTADOR INDIVIDUAL. Esta licença aplica-se ao software BitDefender que pode ser instalado num único computador que não providencie serviços de rede. O primeiro usuário pode instalar este software num único computador e fazer uma cópia adicional num dispositivo distinto para efeitos de backup. O número de usuários permitidos corresponde ao número de usuários abrangidos pela licença.

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

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

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

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



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

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

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

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

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



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

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

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

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

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

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

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

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



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

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

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

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



Prefácio

Este é direcionado para todos os usuários que escolheram o **BitDefender Internet Security 2009** como a solução de segurança em seus computadores pessoais. A informação apresentada neste livro é aplicada não somente para usuários avançados de computação, mas também para qualquer pessoa que esteja apta a trabalhar com o sistema Windows.

Este livro irá descrever para você o **BitDefender Internet Security 2009**, a empresa e a team que o construiu, irá guiá-lo através do processo de instalação e o ensinará como configurá-lo. Você irá descobrir como usar o **BitDefender Internet Security 2009**, como atualizar, testar e customizá-lo. Você aprenderá como aproveitar melhor o BitDefender.

Desejamos a você uma agradável e útil leitura.

1. Convenções usadas neste livro

1.1. Convenções tipográficas

Vários estilos de texto são usados para implementar a leitura. O aspecto e significado dos mesmos estão representados na tabela abaixo.

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



Aparência	Descrição
<code>sample code listing</code>	Listas de código são impressos em caracteres do tipo <code>monospaced</code> .

1.2. Avisos

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



Nota

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



Importante

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



Atenção

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

2. A Estrutura do Livro

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

Instalação. Instruções passo a passo para instalar o BitDefender em uma estação de trabalho. Este é um tutorial compreensivo de como instalar o **BitDefender Internet Security 2009**. Começando com os pré-requisitos para uma instalação de sucesso, você será guiado através de todo o processo de instalação. Finalmente, o procedimento de remoção é descrito caso você precisa desinstalar o BitDefender.

Administração básica. Descrição da administração e manutenção inicial do BitDefender

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



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

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

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

3. Convite a Comentários

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

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



Importante

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



Instalação



1. Requisitos de Sistema

Pode instalar o BitDefender Internet Security 2009 apenas nos computadores com os seguintes sistemas operativos:

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

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



Nota

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

1.1. Requisitos do Sistema

Para Windows XP

- Processador de 800MHz ou superior
- 512 MB de memória RAM (1 GB recomendado)
- Mínimo de 170 MB de espaço disponível em disco (recomendado 200 MB)

Para Windows Vista

- Processador de 800MHz ou superior
- 512 MB de memória RAM (1 GB recomendado)
- Mínimo de 170 MB de espaço disponível em disco (recomendado 200 MB)

Para Windows Home Server

- Processador de 800MHz ou superior
- 512 MB de memória RAM (1 GB recomendado)
- Mínimo de 170 MB de espaço disponível em disco (recomendado 200 MB)



1.2. Requisitos de Software

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

A protecção antiphishing está disponível apenas para:

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

Encriptação para Instant Messaging (IM) está disponível para:

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

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

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



2. Instalar BitDefender

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

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



Passos de instalação



Siga estes passos para instalar o BitDefender Internet Security 2009:

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

O BitDefender Internet Security 2009 avisa-o em caso de ter outros produtos antivírus instalados no seu computador. Clique em **Remover** para começar a desinstalação do produto. Se deseja continuar sem remover os produtos detectados, clique em **Próximo**.



Atenção

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

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



Importante

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

4. De modo padrão, BitDefender Internet Security 2009 será instalado em C:\Program Files\BitDefender\BitDefender 2009. Se você deseja selecionar outra pasta, clique **Procurar** e na janela que aparecerá, selecione a pasta que você deseja que o BitDefender seja instalado.

Clique em **Próximo**.

5. Selecione as opções que tem a ver com o processo de instalação. Algumas delas serão selecionadas por padrão:
 - **Abra o arquivo leíame** - para abrir o arquivo leíame no final da instalação.
 - **Criar um atalho no desktop** - para colocar um atalho do BitDefender Internet Security 2009 no seu desktop no final da instalação.
 - **Ejectar o CD quando a instalação terminar** - para obter que o CD seja ejetado no final da instalação esta opção aparece quando instala o produto a partir do CD.
 - **Desligar a Firewall do Windows** - para desligar a Firewall do Windows.



Importante

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

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

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

Espere até que a instalação termine.

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



Importante

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

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

2.1. Assistente de Registo

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

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



Nota

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

2.1.1. Passo 1/2 - Registrar BitDefender Internet Security 2009

Assistente de Registo BitDefender - Passo 1 de 2

Por favor siga as instruções abaixo para registar o seu produto BitDefender.

O estado atual da licença do seu BitDefender é: **Trial**
A sua chave de licença BitDefender atual é: **BE1B409B7E067AD03090**
Esta chave de licença irá expirar em: **30 dias**

Opções de Licença

Se deseja manter a chave atual, por favor seleccione a primeira opção. Se deseja adicionar uma nova chave, por favor seleccione a segunda opção e insira a chave na caixa abaixo.

Continuar a usar a chave atual
 Quero registar o produto com uma nova chave
 Digite uma nova chave de licença:

Compre uma Chave de Licença
Para adquirir uma chave de licença, clique no link abaixo.
[Renove a sua chave de licença do seu BitDefender](#)

Aqui é onde pode encontrar a sua Chave de Licença:

- 1) Etiqueta do CD-Rom
- 2) Cartão de registo do produto
- 3) E-mail da compra online

Registo

Retornar Avançar Cancelar

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

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

Para registar BitDefender Internet Security 2009:

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



Nota

Pode encontrar a sua chave de licença:

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

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

Clique em **Seguinte** para continuar.

2.1.2. Passo 2/2 - Criar uma conta BitDefender

Assistente de Registo BitDefender - Passo 2 de 2

Registro da Minha Conta

Para que seu produto seja atualizado com as mais novas vacinas e ferramentas antivírus, favor registrar e criar uma conta BitDefender. Desta forma, seu computador estará inteiramente protegido e você terá acesso prioritário ao nosso suporte. Você poderá adiar o processo de registo por 15 dias caso esteja testando nosso produto ou 30 dias caso tenha uma licença paga. Para saber mais sobre sua conta, favor acessar: http://www.bitdefender.com/why_register.

Entre na Conta BitDefender já existente

Endereço E-mail:

Senha:

[Esqueceu a sua senha?](#)

Registrar mais tarde (o registo é obrigatório)

Crie uma nova Conta BitDefender

Endereço E-mail:

Senha (6-16 caracteres):

Redigite a senha:

Nome:

Apellido:

País:

Enviar-me todas as mensagens da BitDefender

Enviar-me só as mensagens mais importantes

Não me envie quaisquer mensagens

Retornar **Concluir** **Cancelar**

bitdefender

Criar uma Conta

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

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



- “Já tenho uma conta BitDefender” (p. 10)



Importante

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

Não tenho uma conta BitDefender

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

- **E-mail** - insira o seu endereço de e-mail.
- **Senha** - insira uma Senha para a sua conta BitDefender. A senha deve ter pelo menos seis caracteres em tamanho.
- **Re-insira a senha** - insira novamente a senha previamente definida.
- **Nome** - insira o seu nome.
- **Apelido** - insira o seu apelido.
- **País** - selecciona o país onde reside.



Nota

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

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

Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta. Escolha uma das seguintes opções:

- **Enviem-me todas as mensagens da BitDefender**
- **Enviem-me apenas as mensagens mais importantes**
- **Não me enviem quaisquer mensagens**

Clique em **Finalizar**.



Já tenho uma conta BitDefender

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

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

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

Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta. Escolha uma das seguintes opções:

- **Enviem-me todas as mensagens da BitDefender**
- **Enviem-me apenas as mensagens mais importantes**
- **Não me enviem quaisquer mensagens**

Clique em **Finalizar**.

2.2. Assistente de Configuração

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

Completar a ação 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 Internet Security 2009 estar instalado.



Nota

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



2.2.1. Passo 1/9 - Janela Boas-vindas

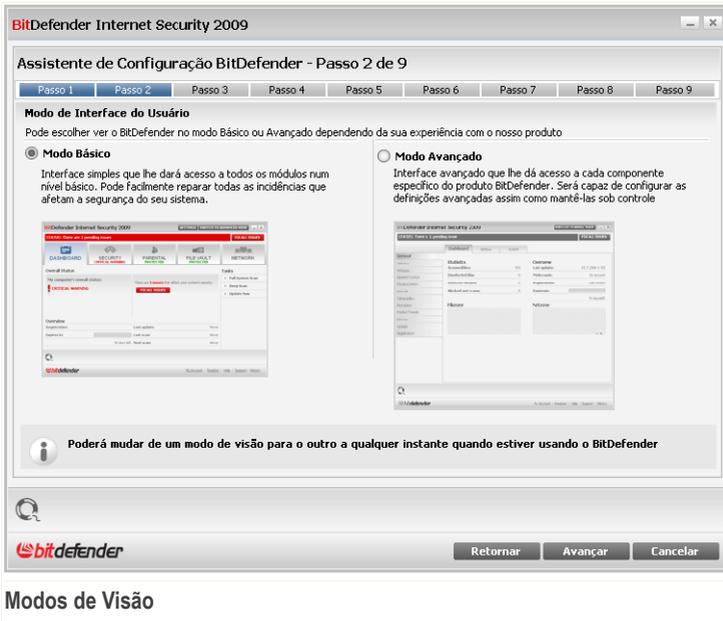


Janela de Boas-Vindas

Clique em **Seguinte** para continuar.



2.2.2. Passo 2/9 - Escolher Modo de Visão



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

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

Clique em **Seguinte** para continuar.



2.2.3. Passo 3/9 - Configurar a Rede BitDefender

BitDefender Internet Security 2009

Assistente de Configuração BitDefender - Passo 3 de 9

Passo 1 Passo 2 **Passo 3** Passo 4 Passo 5 Passo 6 Passo 7 Passo 8 Passo 9

Configuração da Gestão Rede Pessoal

BitDefender Internet Security 2009 inclui um novo componente, Gestão de Rede Pessoal, que lhe permite criar uma rede virtual com todos os computadores na sua casa e/ou Escritório e gerir todos os produtos BitDefender instalados nessa rede. Pode agir como um administrador de uma rede que você criou ou pode fazer parte de uma rede criada e gerida a partir de outro computador.

Clique na caixa abaixo se deseja fazer parte da Rede Pessoal BitDefender. Ser-lhe-á solicitado que insira uma senha de Gestão de Rede Pessoal que permitirá ao administrador da sua rede controlar as definições do BitDefender e as ações neste computador de forma remota.

Desejo fazer parte da Rede Pessoal BitDefender

Senha para Gestão de Rede Pessoal.

Redigite a senha:

Retornar Avançar Cancelar

Configuração da Rede BitDefender

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

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

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



Importante

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

Clique em **Seguinte** para continuar.



Clique em **Seguinte** para continuar.

Criar Regras de Controle de Identidade

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

Adicionar Regra de identidade

Nome de regra: NSS Analisar HTTP

Tipo de regra: Cartão de crédito Analisar Smtip

Dados da Regra: 123412341234 Igualar todas as palavras

Igualar maiúsculas

Analisar Mens. Instantâneas

Ok Cancelar

Regra de Controle de Identidade

Deve definir os seguintes parâmetros:

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



Nota

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

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



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

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

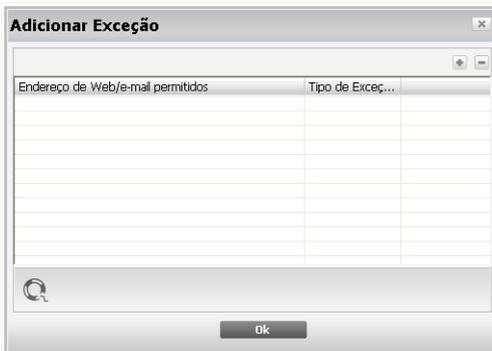
- **Analisar HTTP** - analisa o tráfego HTTP (web) e bloqueia os dados de saída que correspondem aos dados da regra.
- **Analisar SMTP** - analisa todo o tráfego SMTP (mail) e bloqueia as mensagens de e-mail de saída que contém os dados da regra.
- **Analisar Mensagens Instantâneas** - analisa todo o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

Clique **OK** para adicionar a regra.

Definir Exceções do Controle de Identidade

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

Para abrir a janela onde pode gerir as exceções, clique em **Exceções**.



Exceções do Controle de Identidade



Para adicionar uma exceção, siga os seguintes passos:

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

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

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

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

BitDefender Internet Security 2009

Assistente de Configuração BitDefender - Passo 5 de 9

Passo 1 Passo 2 Passo 3 Passo 4 **Passo 5** Passo 6 Passo 7 Passo 8 Passo 9

Controle dos Pais BitDefender

O Controle dos Pais BitDefender permite-lhe controlar o acesso à Internet e a uma série de aplicações de cada usuário que tenha uma conta Windows neste sistema. Para usar este módulo deve-se ativar e configurar.

Clique no botão direito do mouse no nome da Conta Windows para configurar as definições que lhe correspondem no Controle dos Pais.

Quero usar o Controle dos Pais

Lista de Usuários	Status
Administrator	Adulto
cosmin	Criança
vdanciu	Adolescente

Retornar Avançar Cancelar

Configuração do Controle dos Pais

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



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

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

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



Nota

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

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

Clique em **Seguinte** para continuar.



2.2.6. Passo 6/9 - Configurar Relatório de Vírus



Opções do Relatório de Vírus

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

Você pode configurar uma das seguintes opções:

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



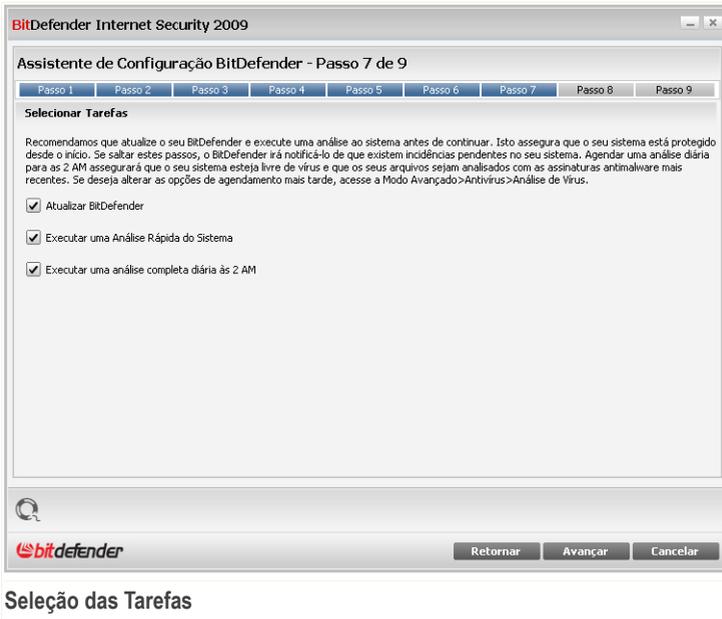
Nota

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

Clique em **Seguinte** para continuar.



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



Seleção das Tarefas

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

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



Importante

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

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

Clique em **Seguinte** para continuar.

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

BitDefender Internet Security 2009

Assistente de Configuração BitDefender - Passo 8 de 9

Passo 1 | Passo 2 | Passo 3 | Passo 4 | Passo 5 | Passo 6 | Passo 7 | **Passo 8** | Passo 9

Atualização do BitDefender

O BitDefender executará a tarefa selecionada durante o passo anterior. Abaixo pode verificar o estado do processo de Atualização. Assim que a atualização terminar, uma análise ao solicitar irá se iniciar. Pode clicar em Avançar para terminar este assistente (a tarefa de análise seguirá em background)

Status: A verificar a existência de atualizações

Arquivo:	0 %	0 kb
Total da atualização:	62 %	0 kb

Retornar | Avançar | Cancelar

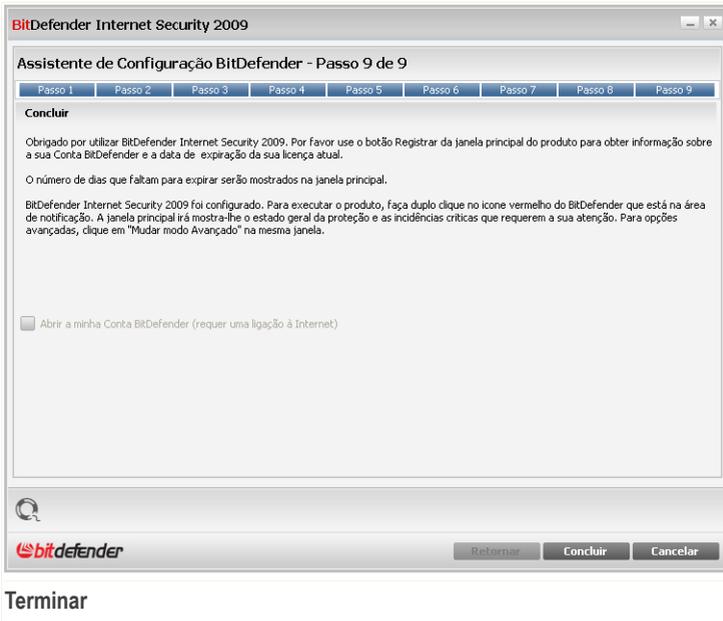
Estado das Tarefas

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

Clique em **Seguinte** para continuar.



2.2.9. Passo 9/9 - Terminar



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

Clique em **Finalizar**.



3. Atualização de versão

A fim de efetuar um upgrade da versão antiga da BitDefender para a versão Antivirus 2009 siga estes passos:

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



4. Remover ou Reparar o BitDefender

Se pretende reparar ou desinstalar o **BitDefender Internet Security 2009**, faça o seguinte a partir do menu Iniciar do Windows: **Iniciar** → **Programas** → **BitDefender 2009** → **Reparar ou Desinstalar**.

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

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

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

Reinicie o computador quando for solicitado para tal, e depois, clique em **Instalar** para reinstalar o BitDefender Internet Security 2009.

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

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



Nota

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

Se escolher desinstalar BitDefender, surgirá uma nova janela.



Importante

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

Clique em **Desinstalar** - para dar início à desinstalação do BitDefender Internet Security 2009 do seu computador.

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

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



Nota

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

Ocorreu um erro ao desinstalar o BitDefender

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



Administração básica.



5. Introdução

Uma vez instalado o BitDefender o seu computador fica protegido.

5.1. Iniciar o BitDefender Internet Security 2009

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

Para aceder ao interface principal do BitDefender Internet Security 2009, utilize o menu do Iniciar do Windows, seguindo o caminho **Iniciar** → **Programas** → **BitDefender 2009** → **BitDefender Internet Security 2009** ou mais rapidamente, duplo-clique no  **ícone BitDefender** a partir da área de notificação.

5.2. Modo de Visão do Interface do usuário

O BitDefender Internet Security 2009 satisfaz as necessidades de segurança quer de uma pessoa técnica quer de um principiante de informática. Assim, o interface do usuário está desenhado para servir todo o tipo de categorias de usuários.

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



Nota

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

5.2.1. Modo Básico

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



Modo Básico

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

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

- No meio da janela estão disponíveis cinco barras.



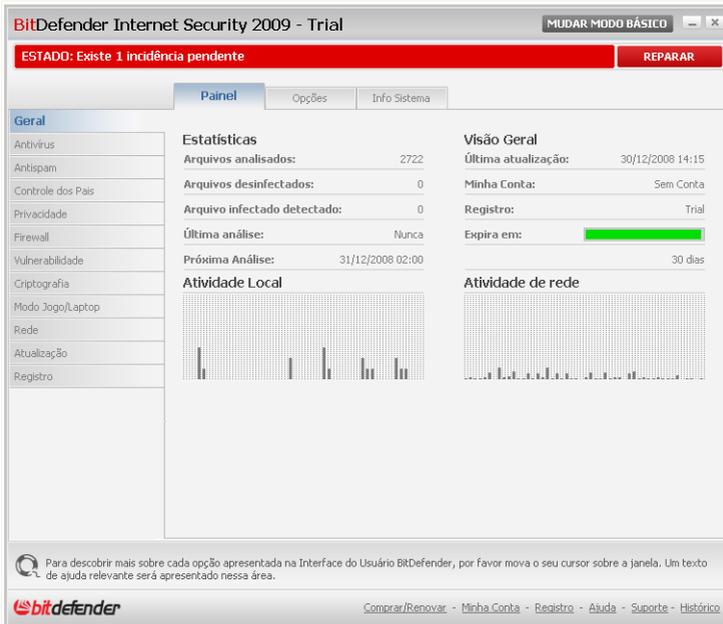
Barra	Descrição
Painel	Mostra informação substancial das estatísticas do produto e do seu estado de registo juntamente com links para as mais importantes tarefas a-pedido.
Segurança	Mostra o estado dos módulos de segurança (antivírus, antiphishing, firewall, antispam, encriptação IM, privacidade, análise de vulnerabilidade e actualização) juntamente com os links para as tarefas de antivírus, actualização e análise de vulnerabilidade.
Parental	Mostra o estado dos módulos que lhe permitem restringir o acesso das suas crianças à internet e a determinadas aplicações.
Gerir arquivos	Mostra o estado do cofre de arquivos juntamente com os links para o mesmo.
Rede	Mostra a estrutura da rede pessoal BitDefender.

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

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

5.2.2. Modo Avançado

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



Modo Avançado

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

Item	Descrição
Mudar para Modo Básico	Abre a janela do Modo Básico. É aqui onde pode ver o interface básico BitDefender incluindo os módulos principais (Segurança, Tuneup, Gestão Arquivo, Rede) e um painel. O BitDefender memoriza esta opção para a próxima vez que abrir o interface do usuário.
Status	Contém informação sobre as vulnerabilidades de segurança do seu computador e ajuda-o a repará-las.

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



Módulo	Descrição
Geral	Permite-lhe aceder às definições gerais ou ver o painel e a info detalhada do sistema.
Antivírus	Permite-lhe configurar o escudo de vírus e as operações de análise em detalhe, definir excepções e configurar o módulo de quarentena.
Antispam	Permite-lhe manter a pasta A Receber livre de SPAM e também configurar as definições do antispam em detalhe.
Firewall	A Firewall protege o seu computador de tentativas de ligações internas e externas não-autorizadas. É bastante semelhante a um guarda que está à sua porta – irá manter um olhar atento na sua ligação à Internet e rastrear a quem permitir e a quem bloquear o acesso à mesma.
Controle de Privacidade	Permite-lhe evitar que sejam roubados dados do seu computador e protege a sua privacidade enquanto se encontra on-line.
Controle dos Pais	Permite-lhe proteger as suas crianças contra o conteúdo inapropriado, ao usar as suas regras personalizadas de acesso ao computador.
Encriptação	Permite-lhe encriptar as comunicações do Yahoo e Windows Live (MSN) Messenger e também encriptar localmente os seus arquivos críticos, as suas pastas ou partições.
Vulnerabilidade	Permite-lhe manter o software crucial para o seu PC sempre actualizado.
Modo de Jogo/Portátil	Permite-lhe adiar as tarefas agendadas BitDefender enquanto o seu portátil está a funcionar a bateria e também elimina alertas e pop-ups enquanto está a jogar.
Rede	Permite-lhe configurar e gerir vários computadores do seu lar.
Actualização	Permite-lhe obter info das últimas actualizações, actualizar o produto e configurar o processo de actualização em detalhe.
Registro	Permite-lhe registar o BitDefender Internet Security 2009, para alterar a chave de licença ou criar uma conta BitDefender.



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

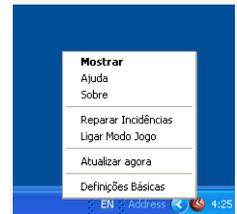
Link	Descrição
Minha Conta	Permite-lhe criar ou fazer login à sua conta BitDefender. A conta BitDefender dá-lhe acesso a suporte técnico gratuito.
Registrar	Permite-lhe inserir uma nova chave de licença ou ver a actual e o estado do seu registo.
Ajuda	Dá-lhe acesso ao arquivo de ajuda que o ensina a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

5.3. Ícone BitDefender na Área de Notificação

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

Se fizer duplo-clique neste ícone, o BitDefender irá abrir. Também clicando com o botão direito do mouse sobre ele aparecerá um menu contextual que lhe permitirá uma administração rápida do BitDefender.

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



Ícone BitDefender



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

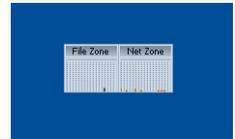
Se existirem incidências críticas a afectar a segurança do seu sistema, um ponto de exclamação é mostrado sobre o  ícone do BitDefender. Pode passar o mouse sobre o ícone e ver o número de incidências que afectam a segurança do seu sistema.

5.4. Barra de Actividade da Análise

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

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

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



Barra de Actividade



Nota

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

Pode usar a **Barra de Actividade da Análise** para analisar objectos. Apenas arraste os objectos que deseja analisar para cima dela. Para mais informação, por favor consulte o *“Verificação Arraste & Solte”* (p. 160).

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

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

5.5. Análise Manual BitDefender

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



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



Análise Manual BitDefender

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

5.6. Modo de Jogo

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

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

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

5.6.1. Usar o Modo de Jogo

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

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



Importante

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

5.6.2. Mudar a Hotkey do Modo de Jogo

Se deseja mudar a hotkey, siga estes passos:

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

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



Nota

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

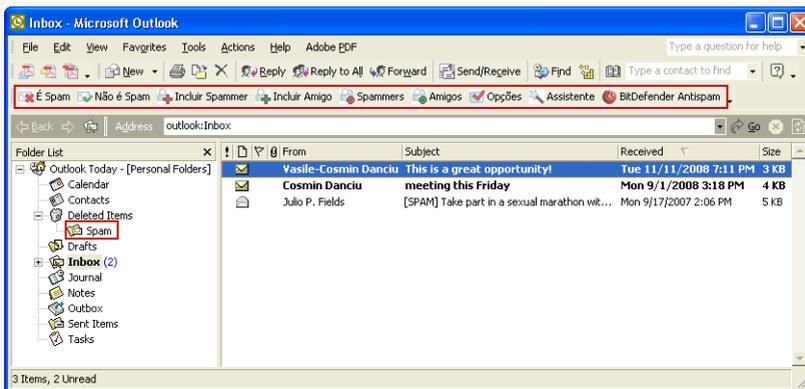
5.7. Integração com Clientes de Mail

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

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

5.7.1. Barra de ferramentas Antispam

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



Barra de ferramentas Antispam



Importante

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

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

Cada botão será explicado abaixo:

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

Mensagens futuras com as mesmas características serão marcadas como SPAM.



Nota

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

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

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



Nota

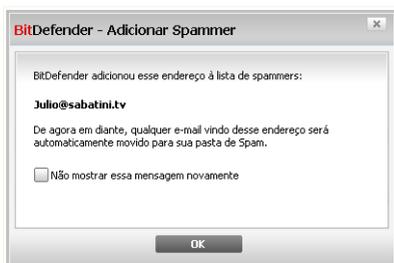
Você pode escolher um e-mail ou quantas mensagens quiser.



Importante

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

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



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

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

Adicionar Spammer

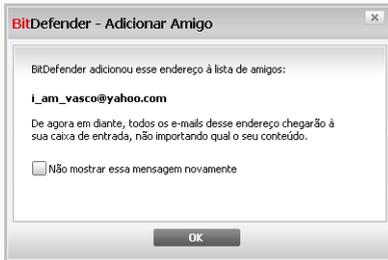
Mensagens futuras daquele endereço serão marcadas como SPAM.



Nota

Você pode seleccionar um remetente ou quantos você quiser.

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



Adicionar Amigo

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

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

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



Nota

Você pode selecionar um remetente ou quantos você quiser.

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



Nota

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



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

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



Importante

Syntax: nome@domínio.com.

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



Importante

Syntax:

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

Para importar endereços de e-mail de **Livro de Endereços do Windows/Pastas do Outlook Express** para o **Microsoft Outlook/Outlook Express / Windows Mail**



selecione a opção apropriada do menu expansível **Importar endereços de e-mail de**.

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

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

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

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

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

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

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



Nota

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



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

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



Importante

Syntax: nome@domínio.com.

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



Importante

Syntax:

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



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

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

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

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

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

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



Nota

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

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

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



Opções

As seguintes opções estão disponíveis:

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

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

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

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



Nota

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



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

5.7.2. Assistente de Configuração Antispam

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



Nota

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

Passo 1/6 - Janela de Boas-vindas

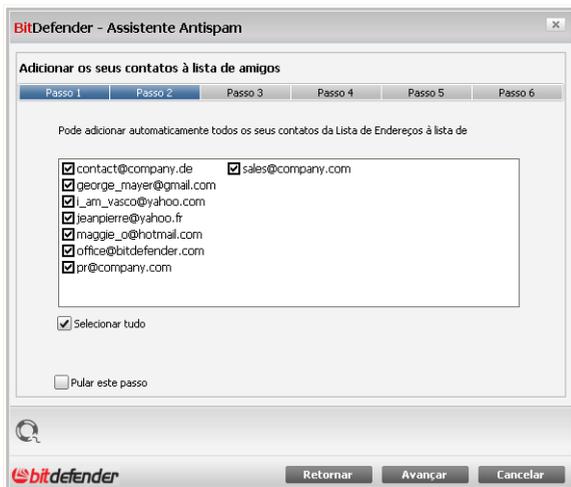


Janela de Boas-Vindas

Clique em **Próximo**.



Passo 2/6 - Preencher a Lista de Amigos



Preencher a Lista de Amigos

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

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

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



Passo 3/6 - Apagar a Base de Dados Bayesiana



Apagar a Base de Dados Bayesiana

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

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

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

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



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



Treine o filtro Bayesiano com e-mails legítimos

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

Existem duas opções avançadas por debaixo da lista de directórios:

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

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



Passo 5/6 - Treine o filtro Bayesiano com SPAM



Treine o filtro Bayesiano com SPAM

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



Importante

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

Existem duas opções avançadas por debaixo da lista de directórios:

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

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



Passo 6/6 - Conclusão



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

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

5.8. Integração com Exploradores web

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

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

- Internet Explorer
- Mozilla Firefox



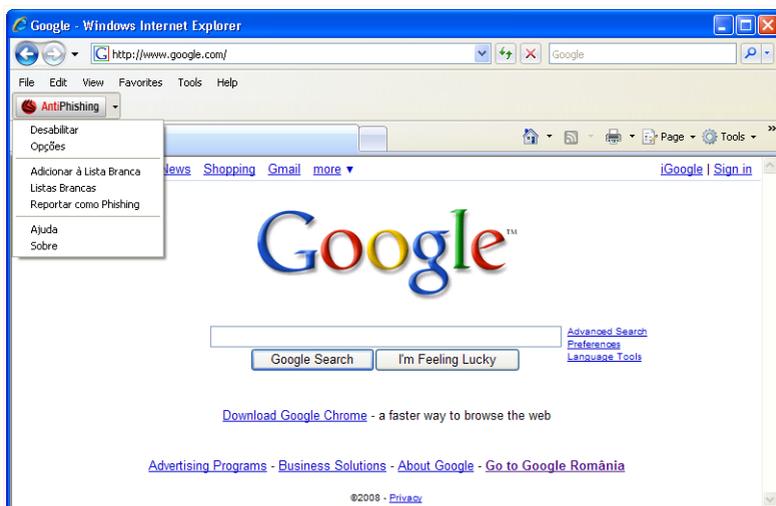
Pode de forma fácil e eficiente gerir a protecção antiphishing e a Lista Branca usando a barra de ferramentas do BitDefender Antiphishing que está integrada num dos exploradores da internet acima.

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



Nota

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



Barra de Ferramentas do Antiphishing

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

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



Nota

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



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

As seguintes opções estão disponíveis:

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



Nota

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

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

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

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

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

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

5.9. Integração com Messenger

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

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

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



Importante

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

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

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

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



Opções da Cifragem das Mensagens Instantâneas

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



6. Painel

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

The screenshot shows the BitDefender Internet Security 2009 - Trial interface. At the top, there is a red banner indicating "ESTADO: Existe 1 incidência pendente" with a "REPARAR" button. Below this are five main status tiles: "PAINEL", "SEGURANÇA AVISO CRÍTICO", "CONTROLE DOS PAIS PROTEGIDO", "COFRE DE ARQUIVOS SEGURO", and "REDE". The "Status" section displays "O estado geral do meu computador: AVISO CRÍTICO" and "Existe 1 incidência que afeta a segurança do seu sistema." with a "REPARAR" button. The "Tarefas" section lists "Atualizar agora", "Análise Completa", and "Análise Minuciosa". The "Visão Geral" section provides registration details: "Registro: Trial", "Última atualização: 30/12/2008 14:07", "Expira em: 30 dias", "Última análise: Nunca", and "Próxima Análise: 31/12/2008 02:00". A footer note explains that the dashboard shows product statistics and registration status with links for tasks. The BitDefender logo and navigation links (Comprar/Renovar, Minha Conta, Registo, Ajuda, Suporte, Histórico) are also visible.

Painel

6.1. Sumário

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

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



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

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

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

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



Nota

Os dados que nos fornecer serão mantidos confidenciais.

Para registar o BitDefender Internet Security 2009, siga estes passos.

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

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

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



6.2. Tarefas

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

Estão disponíveis os seguintes botões:

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

6.2.1. A analisar com BitDefender

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

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



Nota

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

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

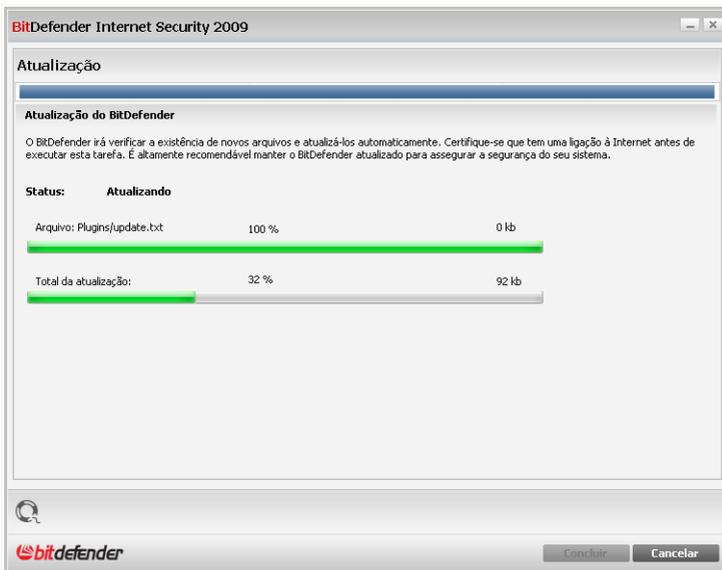
Siga o processo guiado de três passos para completar o processo de análise.



6.2.2. Actualizar o BitDefender

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

Por defeito, quando liga o computador o BitDefender verifica se há actualizações e depois disso fá-lo a cada **hora** . No entanto, se deseja actualizar o BitDefender, clique em **Actualizar Agora**. O processo de actualização irá ser iniciado e a seguinte janela irá aparecer imediatamente:



Actualizar o BitDefender

Nesta janela poderá ver o estado do processo de actualização.

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

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



Nota

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

Reinicie o computador se necessário. No caso de uma actualização importante, ser-lhe-á solicitado que reinicie o seu computador:

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

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



7. Segurança

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

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

Componentes Monitorados	Monitorar	Status
Segurança local		
A proteção em Tempo-real está habilitada	<input checked="" type="checkbox"/> Sim	OK
Nunca analisou o seu computador em busca de malware	<input checked="" type="checkbox"/> Sim	Reparar
Atualizado hoje	<input checked="" type="checkbox"/> Sim	OK
Firewall ativado	<input checked="" type="checkbox"/> Sim	OK
Segurança online		
Analisar Vulnerabilidade		OK

O módulo de segurança é composto de duas secções:

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

7.1. Componentes Monitorizados

Os componentes monitorizados estão agrupados em diversas categorias:



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

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

7.1.1. Segurança Local

Sabemos que é importante ser avisado sempre que haja um problema que afecte a segurança do seu computador. Ao monitorizar cada módulo de segurança, o BitDefender Internet Security 2009 avisá-lo-á não só quando você configura as definições que poderão afectar a segurança do seu computador, mas também quando se esquece de fazer tarefas importantes.

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

Incidência	Descrição
Proteção de arquivos em Tempo-real está activada	Assegura que todos os arquivos serão analisados, à medida que eles forem acedidos por si ou por uma aplicação do seu sistema.
Você analisou o seu computador em busca de malware hoje	É altamente recomendável que leve a cabo uma análise a-pedido tão depressa quanto possível para verificar que os arquivos armazenados no seu computador estão livres de malware.



<i>Incidência</i>	<i>Descrição</i>
Actualização automática está activada	Por favor mantenha a actualização automática activada para assegurar que as assinaturas de malware do seu produto BitDefender são actualizadas numa base regular.
Actualizar Agora	A actualização do produto e das assinaturas de malware está a ser levada a cabo.
Firewall activada	Protege o seu computador contra os hackers e os ataques maliciosos vindos do exterior.

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

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

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

7.1.2. Segurança On-line

As incidências que dizem respeito à segurança on-line são descritas em frases bem explícitas. Ao mesmo tempo que a frase, se existe algo que possa ameaçar a segurança do seu computador, verá um botão de estado vermelho denominado **Reparar**. De outra forma, um botão verde de estado a dizer **OK** é mostrado.

<i>Incidência</i>	<i>Descrição</i>
Antispam activado	Asegura que os seus e-mails são analisados em busca de malware e filtrados de spam.
Controle de Identidade ativado	Ajuda-o a manter os seus dados confidenciais seguros ao analisar o tráfego web e de e-mail em busca de palavras-chave. É recomendável que mantenha o Controle de Identidade ativado, para evitar que a sua informação confidencial (endereço de e-mail, IDs de usuário, palavras-passe, números de cartões de crédito, etc) seja roubada.



<i>Incidência</i>	<i>Descrição</i>
A protecção antiphishing Firefox está activada	BitDefender protege-o contra as tentativas de phishing quando está a navegar na Internet.
A protecção antiphishing Internet Explorer está activada	BitDefender protege-o contra as tentativas de phishing quando está a navegar na Internet.

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

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

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

7.1.3. Analisar Vulnerabilidades

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

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



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

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

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

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

7.2. Tarefas

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

Estão disponíveis os seguintes botões:

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



7.2.1. A analisar com BitDefender

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

Tarefa	Descrição
Análise Completa do Sistema	Analisa todo o sistema, excepto arquivos. Na configuração por defeito, faz uma análise em busca de todo o tipo de malware que ameace a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.
Análise Minuciosa do Sistema	Analisa todo o sistema. Na configuração por defeito, faz uma análise em busca de todo o tipo de malware que ameace a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.
Analisar Os Meus Documentos	Use esta tarefa para analisar pastas de usuários atuais: Os Meus Documentos, Ambiente de Trabalho e StartUp. Isto assegurará a segurança dos seus documentos, um espaço de trabalho seguro e aplicações limpas que se executam durante o iniciar do windows.



Nota

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

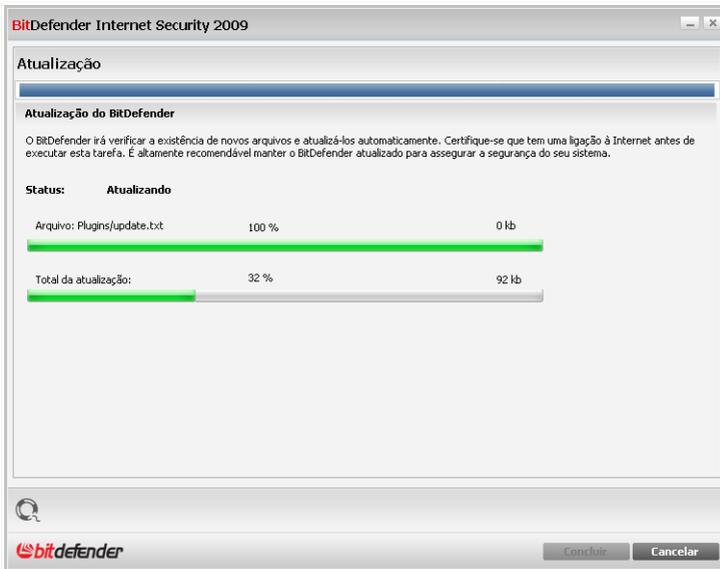
Quando dá início a um processo de análise a-pedido, quer seja uma análise rápida ou completa, o Analisador BitDefender surgirá. Siga o processo guiado de três passos para completar o processo de análise.

7.2.2. Actualizar o BitDefender

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



Por defeito, quando liga o computador o BitDefender verifica se há actualizações e depois disso fá-lo a cada **hora** . No entanto, se deseja actualizar o BitDefender, clique em **Actualizar Agora**. O processo de actualização irá ser iniciado e a seguinte janela irá aparecer imediatamente:



Actualizar o BitDefender

Nesta janela poderá ver o estado do processo de actualização.

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

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



Nota

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



Reinicie o computador se necessário. No caso de uma actualização importante, ser-lhe-á solicitado que reinicie o seu computador:

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

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

7.2.3. Procurar Vulnerabilidades

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

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



Passo 1/6 - Seleccionar Vulnerabilidades a Verificar

BitDefender 2009

Assistente de Vulnerabilidade BitDefender

Passo 1 | Passo 2 | Passo 3 | Passo 4 | Passo 5 | Passo 6

Selecionar Tarefas

Este assistente irá guiá-lo através das ações necessárias para identificar aplicações desatualizadas e as contas do Windows que têm uma senha fraca. Por favor seleccione da lista abaixo que itens deseja ver analisados em busca de vulnerabilidades.

- Verificar Atualizações Críticas Windows
- Verificar Atualizações Opcionais Windows
- Verificar a existência de duplicados de atualização
- Verificar as Senhas das suas Contas Windows

Selecionar as ações que o módulo de vulnerabilidade deve considerar ao analisar o seu sistema.

bitdefender Avançar Cancelar

Vulnerabilidades

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



Passo 2/6 - Analisar em Busca de Vulnerabilidades



Espere que o BitDefender termine a análise de vulnerabilidades.



Passo 3/6 - Alterar Palavras-passe Fracas

Nome do Usuário	Forte	Status
Administrator	Forte	Ok
cosmin	Fracas	Reparar

Esta é a lista das senhas definidas no seu computador e o nível de proteção que elas oferecem. Clique no botão "Reparar" para modificar as senhas fracas.

bitdefender Avançar Cancelar

Senhas do usuário

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

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

BitDefender

Como prefere resolver esta incidência?

Obrigado o usuário a mudar a senha durante o próximo logon

Mude a senha você mesmo agora

Digite a senha:

Confirme a Senha:

OK Fechar

Mudar a senha



Selecione o método para reparar esta incidência:

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



Nota

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

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

Clique em **Próximo**.



Passo 4/6 - Actualizar Aplicações

Nome da Aplicação	Versão Instalada	Última Versão	Status
Yahoo! Messenger	8.1.0.421	8.1.0.241	Atualizado
Winamp	5,5,3,1938	5,5,4	Página Principal
Firefox	3.0.4 (en-US)	3.0.1 (en-US)	Atualizado

Esta é a lista das aplicações suportadas pelo BitDefender e das atualizações disponíveis, se as houver.

Aplicações

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

Clique em **Próximo**.



Passo 5/6 - Actualizar Windows

The screenshot shows the BitDefender 2009 Assistant de Vulnerabilidade window. The title bar reads "BitDefender 2009" and the main title is "Assistente de Vulnerabilidade BitDefender". The progress bar indicates "Passo 5" is active. The main content area is titled "Atualizações do Windows" and contains two sections: "Verificar Atualizações Críticas Windows" and "Verificar Atualizações Opcionais Windows".

Verificar Atualizações Críticas Windows

- Windows Genuine Advantage Validation Tool (KB892130)
- Security Update for Microsoft XML Core Services 4.0 Service Pack 2 (KB954430)
- Windows XP Service Pack 3 (KB936929)

Verificar Atualizações Opcionais Windows

- Windows Search 4.0 For Windows XP (KB940157)
- Microsoft Silverlight (KB957938)
- Group Policy Preference Client Side Extensions for Windows XP (KB943729)
- Root Certificates Update

At the bottom of the list, there is a button labeled "Instalar todas atualizações do Sistema". Below this, a search icon and text state: "Esta é a listas das atualizações críticas e não-críticas das aplicações do Windows". The BitDefender logo is in the bottom left, and "Avançar" and "Cancelar" buttons are in the bottom right.

Atualizações Windows

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

Clique em **Próximo**.



Passo 6/6 - Ver Resultados

BitDefender 2009

Assistente de Vulnerabilidade BitDefender

Passo 1 | Passo 2 | Passo 3 | Passo 4 | Passo 5 | **Passo 6**

! A análise de vulnerabilidades está terminada, mas nenhuma atualizações foram instaladas. É fortemente recomendado que mantenha o seu computador atualizado.

A análise de vulnerabilidades está terminada, mas nenhuma atualizações foram instaladas. É fortemente recomendado que mantenha o seu computador atualizado.

bitdefender

Fechar

Resultados

Clique em **Fechar**.



8. Parental

BitDefender traz consigo um módulo Parental que o ajuda a manter
Para entrar no módulo Parental, clique na barra **Parental**.

The screenshot shows the BitDefender Internet Security 2009 interface. At the top, there's a status bar with a red warning: "ESTADO: Existe 1 incidência pendente" and a "REPARAR" button. Below this are five main navigation buttons: "PAINEL", "SEGURANÇA AVISO CRÍTICO", "CONTROLE DOS PAIS PROTEGIDO", "COFRE DE ARQUIVOS SEGURO", and "REDE". The "CONTROLE DOS PAIS" button is highlighted in blue. Below the navigation bar, the "Componentes Monitorados" section is expanded, showing a table with columns for "Monitorar" and "Status". The table lists three users: "cosmin (Administrador)", "Administrator (Administrador)", and "vdanciu (Administrador)", all with "Não" selected in the "Monitorar" column and "Não monitorado" in the "Status" column. To the right of the table is a "Tarefas" section with links for "Atualizar agora", "Análise Completa", and "Análise Minuciosa". At the bottom of the interface, there's a footer with the BitDefender logo and links for "Comprar/Renovar", "Minha Conta", "Registro", "Ajuda", "Suporte", and "Histórico".

Componentes Monitorados	Monitorar	Status
<input type="checkbox"/> Controle dos Pais foi configurado para os seguintes «0» usuários	<input type="checkbox"/> Não	Não monitorado
cosmin (Administrador)	<input type="checkbox"/> Não	Não monitorado
Administrator (Administrador)	<input type="checkbox"/> Não	Não monitorado
vdanciu (Administrador)	<input type="checkbox"/> Não	Não monitorado

O módulo Parental é composto de duas secções:

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

8.1. Componentes Monitorizados

Os componentes monitorizados são os seguintes:



<i>Categoria</i>	<i>Descrição</i>
Controle dos Pais	Aqui é onde pode verificar o estado do Controle dos Pais que lhe permite restringir o acesso das crianças à internet e a determinadas aplicações.

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

8.1.1. Controle dos Pais

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

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

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

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

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

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



8.2. Tarefas

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

Estão disponíveis os seguintes botões:

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

8.2.1. A analisar com BitDefender

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

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



Nota

Um vez que as tarefas **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.

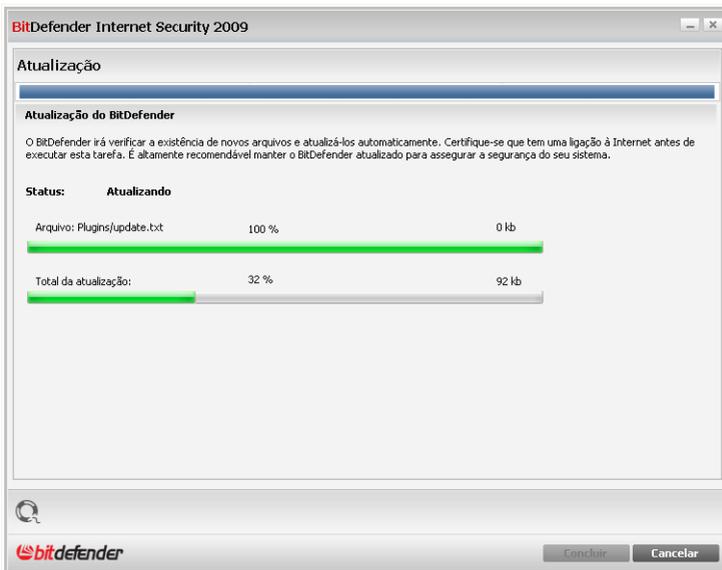
Siga o processo guiado de três passos para completar o processo de análise.



8.2.2. Actualizar o BitDefender

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

Por defeito, quando liga o computador o BitDefender verifica se há actualizações e depois disso fá-lo a cada **hora** . No entanto, se deseja actualizar o BitDefender, clique em **Actualizar Agora**. O processo de actualização irá ser iniciado e a seguinte janela irá aparecer imediatamente:



Actualizar o BitDefender

Nesta janela poderá ver o estado do processo de actualização.

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

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



Nota

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

Reinicie o computador se necessário. No caso de uma actualização importante, ser-lhe-á solicitado que reinicie o seu computador:

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

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



9. Cofre de arquivos

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

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

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

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

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



Cofre de arquivos

- **Componentes Monitorizados** - Permite-lhe ver a lista completa dos componentes monitorizados para cada módulo. Pode escolher quais os módulos a serem monitorizados. É recomendável activar a monitorização de todos os componentes.

9.1. Componentes Monitorizados

Os componentes monitorizados são os seguintes:

Categoria	Descrição
Cofre de arquivos	O cofre de arquivos é um espaço de armazenamento seguro de informação pessoal ou de arquivos considerados sensíveis. É mantido localmente, no seu computador. Como se encontra encriptado, os dados contidos no mesmo são invulneráveis ao roubo ou a uma quebra de segurança.

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



9.1.1. Cofre de arquivos

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

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

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

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

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

9.2. Tarefas

Estão disponíveis os seguintes botões:

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



9.2.1. Adicionar arquivos ao Cofre

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

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

Passo 1/6 - Seleccionar Alvo

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



Alvo

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



Nota

Pode seleccionar um ou vários locais.



Clique em **Próximo**.

Passo 2/6 - Seleccionar cofre

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

Seleccionar cofre **Selecione portas**

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

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

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

Clique em **Próximo**.



Passo 3/6 - Criar Cofre

Aqui é onde pode especificar informação do novo cofre.

BitDefender 2009

Cofre - Adicionar ao Cofre

Passo 1 | Passo 2 | **Passo 3** | Passo 4 | Passo 5 | Passo 6

Criar Cofre

Por favor especifique uma nova senha para o cofre e configure onde deve de ser armazenado e a sua capacidade.

Inserir caminho para o Cofre de Arquivos: **Procurar**

Letra da drive: J: ▾

Insira a senha para o Cofre de Arquivos: A senha deve conter no mínimo 8 caracteres.

Confirmar Senha para o Cofre de Arquivos:

Insira Tamanho do Cofre (MB): 50 O tamanho deve de conter pelo menos dois digitos.

Especifica a letra da drive para abrir o Cofre de Arquivos.

Retornar **Avançar** **Cancelar**

Criar Cofre

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

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



Nota

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

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



Nota

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



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



Nota

A senha deve ter pelo menos oito caracteres em tamanho.

4. Confirmar senha

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



Nota

O tamanho deve de conter apenas dígitos.

Clique em **Próximo**.

Irá para o passo 5.

Passo 4/6 - Senha

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



BitDefender 2009

Cofre - Adicionar ao Cofre

Passo 1 | Passo 2 | Passo 3 | **Passo 4** | Passo 5 | Passo 6

Solicitar Senha do Cofre

Por favor insira a senha para o cofre selecionado:

Senha: A senha deve conter no mínimo 8 caracteres.

Avançar para o passo seguinte do assistente.

 **Retornar** **Avançar** **Cancelar**

Confirmar senha

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

Passo 5/6 - Resumo

Aqui é onde pode rever as operações escolhidas.



BitDefender 2009

Cofre - Adicionar ao Cofre

Passo 1 | Passo 2 | Passo 3 | Passo 4 | **Passo 5** | Passo 6

Concluir

Operação	Adicionar 1 Arquivos/Pastas ao novo Cofre
Nome	fvtest2
Localização	H:\Dade.K\TSELECT12\Testbed\FileVault\fvtest2.bvd
Status	Fechado

Por favor reveja as operações escolhidas e clique **Avançar** se deseja continuar.
Pode clicar em **Retornar** se deseja alterar alguma coisa.

Avançar para o passo seguinte do assistente.

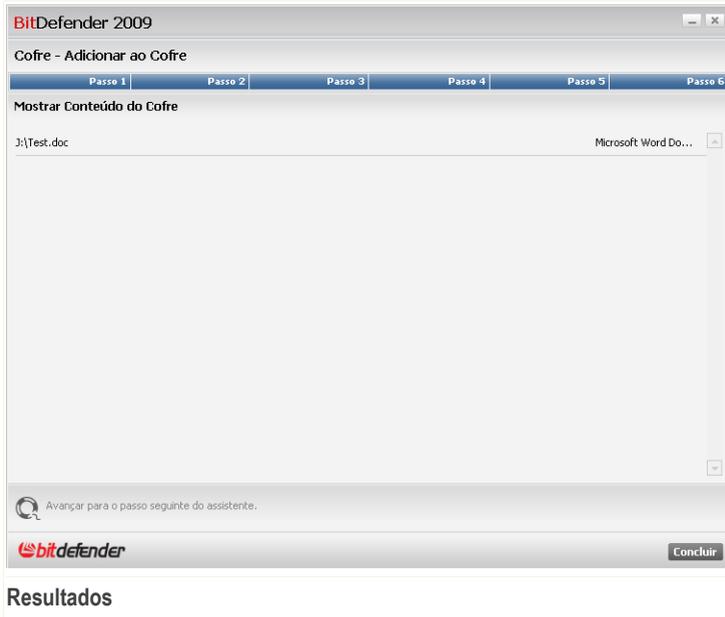
Retornar **Avançar** **Cancelar**

Sumário

Clique em **Próximo**.

Passo 6/6 - Resultados

Aqui é onde pode ver o conteúdo do cofre.



Clique em **Finalizar**.

9.2.2. Remover arquivos do Cofre

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

Passo 1/5 - Seleccionar Cofre

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



Seleccionar cofreSelecione portas

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

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

Clique em **Próximo**.

Passo 2/5 - Senha

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



BitDefender 2009

Cofre - Remover do Cofre

Passo 1 | **Passo 2** | Passo 3 | Passo 4 | Passo 5

Solicitar Senha do Cofre

Por favor insira a senha para o cofre selecionado:

Senha: A senha deve conter no mínimo 8 caracteres.

Avançar para o passo seguinte do assistente.

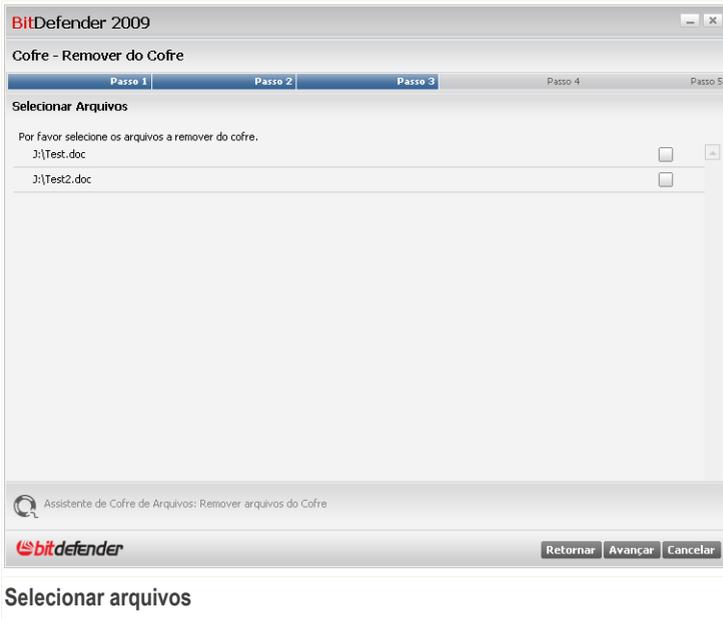
 **Retornar** **Avançar** **Cancelar**

Confirmar senha

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

Passo 3/5 - Seleccionar arquivos

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



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

Passo 4/5 - Sumário

Aqui é onde pode rever as operações escolhidas.



BitDefender 2009

Cofre - Remover do Cofre

Passo 1 | Passo 2 | Passo 3 | Passo 4 | Passo 5

Concluir

Operação	Remover 0 arquivos do Cofre
Nome	fvtest2
Localização	H:\Dade.K\TSELECT12\Testbed\FileVault\fvtest2.bvd
Status	Aberto em J:

Por favor reveja as operações escolhidas e clique **Avançar** se deseja continuar.
Pode clicar em **Retornar** se deseja alterar alguma coisa.

Avançar para o passo seguinte do assistente.

Retornar Avançar Cancelar

Sumário

Clique em **Próximo**.

Passo 5/5 - Resultados

Aqui é onde poder ver o resultado da operação.



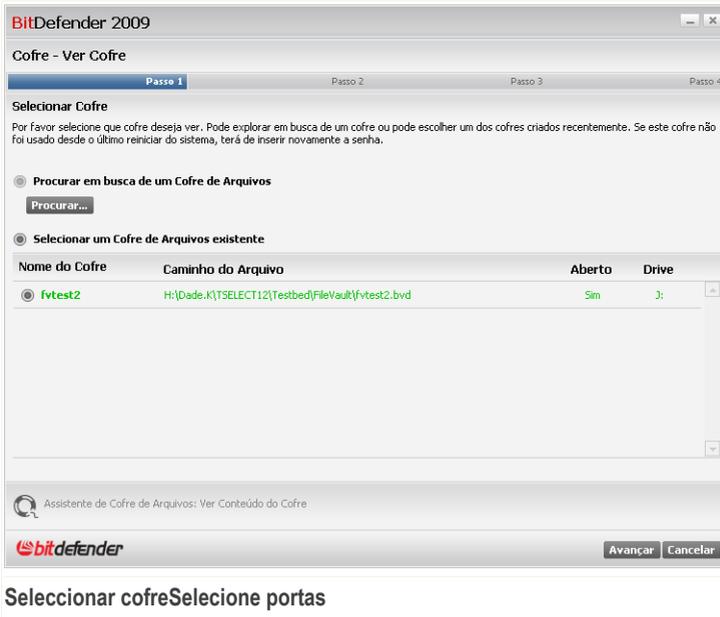
Clique em **Finalizar**.

9.2.3. Ver arquivos do Cofre

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

Passo 1/4 - Seleccionar Cofre

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



Seleccionar cofreSelecione portas

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

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

Clique em **Próximo**.

Passo 2/4 - Senha

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



BitDefender 2009

Cofre - Ver Cofre

Passo 1 Passo 2 Passo 3 Passo 4

Solicitar Senha do Cofre

Por favor insira a senha para o cofre selecionado:

Senha: A senha deve conter no mínimo 8 caracteres.

Especifica a senha para acessar ao Cofre.

 Retornar Avançar Cancelar

Confirmar senha

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

Passo 3/4 - Sumário

Aqui é onde pode rever as operações escolhidas.



BitDefender 2009

Cofre - Ver Cofre

Passo 1 | Passo 2 | **Passo 3** | Passo 4

Concluir

Operação	Ver conteúdo do Cofre
Nome	fvtest2
Localização	H:\Dade.K\TSELECT12\Testbed\FileVault\fvtest2.bvd
Status	Fechado

Por favor reveja as operações escolhidas e clique **Avançar** se deseja continuar.
Pode clicar em **Retornar** se deseja alterar alguma coisa.

Avançar para o passo seguinte do assistente.

Retornar **Avançar** **Cancelar**

Sumário

Clique em **Próximo**.

Passo 4/4 - Resultados

Aqui é onde pode ver os arquivos do cofre.



Clique em **Finalizar**.

9.2.4. Fechar o Cofre

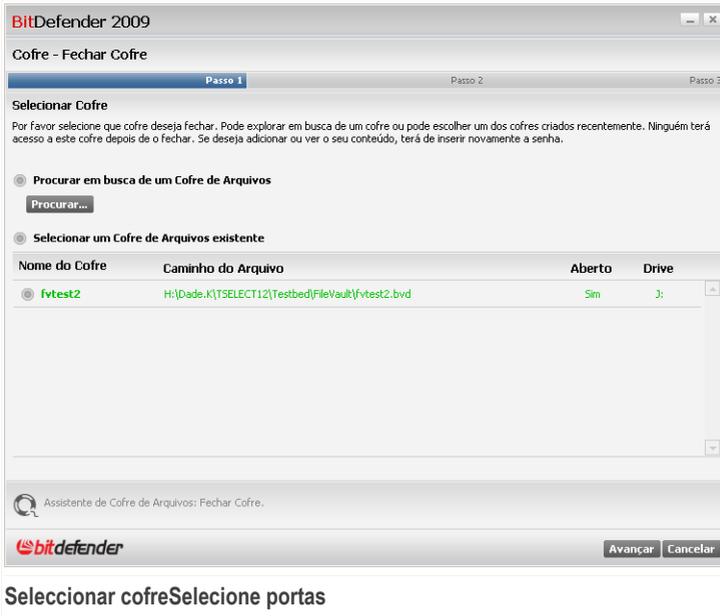
Como já sabe, um cofre é um arquivo encriptado com extensão `bvd` que está no seu computador. O cofre pode ser aberto (montado) ou fechado (desmontado).

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

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

Passo 1/3 - Seleccionar Cofre

Aqui é onde pode especificar o cofre a fechar.



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

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

Clique em **Próximo**.

Passo 2/3 - Sumário

Aqui é onde pode rever as operações escolhidas.



BitDefender 2009

Cofre - Fechar Cofre

Passo 1 | Passo 2 | Passo 3

Concluir

Operação	Fechar Cofre
Nome	fvtest2
Localização	H:\Dade.K\TSELECT12\Testbed\FileVault\fvtest2.bvd
Status	Aberto em J:

Por favor reveja as operações escolhidas e clique **Avançar** se deseja continuar.
Pode clicar em **Retornar** se deseja alterar alguma coisa.

Avançar para o passo seguinte do assistente.

Retornar **Avançar** **Cancelar**

Sumário

Clique em **Próximo**.

Passo 3/3 - Resultados

Aqui é onde poder ver o resultado da operação.



BitDefender 2009

Cofre - Fechar Cofre

Passo 1 | Passo 2 | Passo 3

Mostrar Resultado da Operação

Operação	Fechar Cofre
Nome	fvtest2
Localização	H:\Dade.K\TSELECT12\Testbed\FileVault\fvtest2.bvd
Resultado	A operação foi completada com sucesso.
Código de Erro	
Informação	Fecho do cofre de arquivos bem-sucedido.

Avançar para o passo seguinte do assistente.

Concluir

Resultados

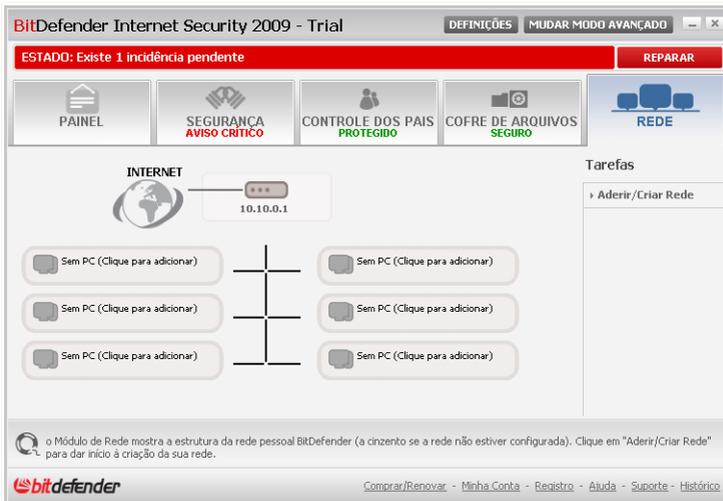
Clique em **Finalizar**.



10. Rede

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

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



Rede

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

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

10.1. Tarefas

Inicialmente só um botão está disponível.



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

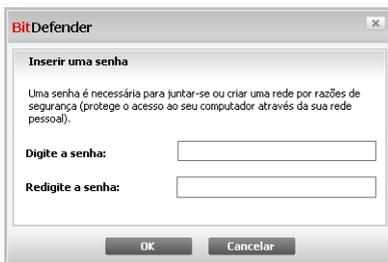
Após aderir à rede, mais botões irão surgir.

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

10.1.1. Aderir à Rede BitDefender

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

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



Configurar senha

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

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

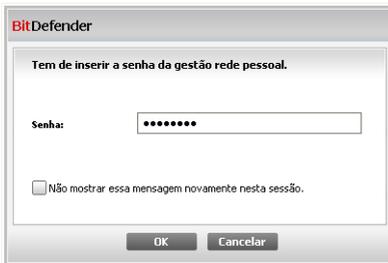


10.1.2. Adicionar Computadores à Rede BitDefender

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

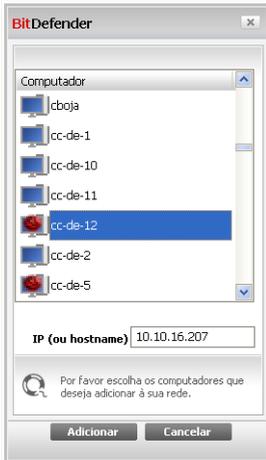
Para adicionar um computador à rede pessoal BitDefender, siga os seguintes passos:

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



Inserir senha

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



Adicionar Computador

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

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

3. Faça uma das coisas seguintes:

- Seleccione da lista o nome do computador a adicionar.
- Insira o endereço IP ou o nome do computador a adicionar no campo correspondente.

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



BitDefender

Tem de inserir a senha da gestão rede pessoal.

Senha:

Não mostrar essa mensagem novamente nesta sessão.

OK Cancelar

Autenticar

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



Nota

Podem adicionar até cinco computadores neste mapa de rede.

10.1.3. Gerir a Rede BitDefender

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



Mapa de Rede

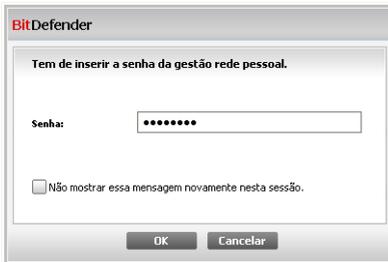
Se mover o curso do seu mouse sobre um computador do mapa de rede, pode ver alguma informação acerca dele (nome, endereço IP, número de incidências que estão a afetar a segurança do sistema, o estado de registo do BitDefender).

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

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



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



Inserir senha

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



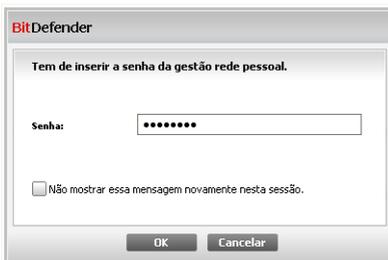
Nota

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

10.1.4. Analisar Todos os Computadores

Para analisar todos os computadores geridos, siga estes passos:

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

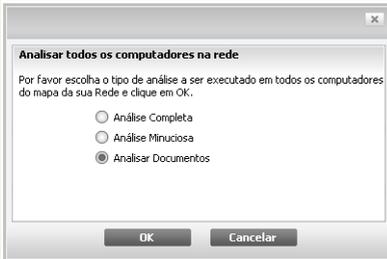


Inserir senha



2. Selecciono o tipo de análise.

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



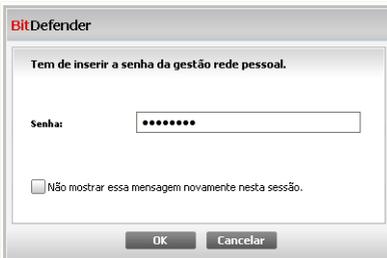
Seleccionar o Tipo de Análise

3. Clique em **OK**.

10.1.5. Actualizar Todos os Computadores

Para actualizar todos os computadores, siga estes passos:

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



Inserir senha

2. Clique em **OK**.



10.1.6. Registrar Todos os Computadores

Para registrar todos os computadores geridos, siga estes passos:

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

BitDefender

Tem de inserir a senha da gestão rede pessoal.

Senha:

Não mostrar essa mensagem novamente nesta sessão.

OK Cancelar

Inserir senha

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

Registrar o computador

Insira a chave que deseja registrar com

Insira a chave de licença:

OK Cancelar

Registrar Todos

3. Clique em **OK**.



11. Definições Básicas

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

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



Os módulos de segurança disponíveis estão agrupados em diversas categorias.

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



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

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

11.1. Segurança Local

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

Módulo de Segurança	Descrição
Protecção Antivirus & Antispyware de Arquivos em Tempo-Real	A protecção de arquivos em tempo-real assegura que todos os arquivos acedidos por si ou por uma aplicação são analisados.
Actualização Automática	A actualização automática assegura que os produtos e as assinaturas mais recentes são descarregados da Internet e instalados automaticamente numa base regular.
Verificação Automática de Vulnerabilidades	A Verificação Automática de Vulnerabilidades assegura que o software crucial no seu PC está actualizado.

11.2. Segurança On-line

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

Módulo de Segurança	Descrição
Antivirus em Tempo-Rea, Antispam &	A protecção em Tempo-real assegura que os seus e-mails são filtrados de spam e analisados em busca de tentativas de phishing.



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

11.3. Definições do Controle dos Pais

Aqui é onde pode ativar / desativar o módulo do Controle dos Pais com um só click.
O Controle dos Pais pode bloquear o acesso a páginas web inapropriadas, à internet durante determinados períodos de tempo e pode filtrar o tráfego de e-mail, IM e web baseado em determinadas palavras-chave.

11.4. Definições de rede

Aqui é onde pode activar / desactivar o módulo da Firewall com um só click.
A Firewall protege o seu computador contra os hackers e os ataques maliciosos externos.

11.5. Definições do Cofre de arquivos

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



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

11.6. Configurações Gerais

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

Item	Descrição
Modo de Jogo	O Modo de Jogo modifica temporariamente as definições da protecção de forma a minimizar o seu impacto no desempenho do sistema durante os jogos.
Modo de Portátil	O Modo de Portátil modifica temporariamente as definições da protecção de forma a minimizar o seu impacto no tempo de vida da bateria do seu portátil.
Senha de Configuração	Isto assegura que as definições do BitDefender só podem ser modificadas pela pessoa que conhece esta senha.
Senha do Controle dos Pais	Ao ativar esta opção, a protecção das definições fica a cargo do módulo do Controle dos Pais. Isto assegura que as definições do Controle dos Pais BitDefender apenas podem ser alteradas por alguém que saiba esta senha.
Notícias BitDefender	Ao activar esta opção, irá receber notícias importantes sobre a empresa BitDefender, sobre as actualizações do produto ou sobre novas ameaças de segurança.
Notificações de Alerta de Produtos	Ao activar esta opção, irá receber alertas de informação.
Barra de Actividade de Análise	A Barra de Actividade de Análise é uma pequena e transparente barra que indica o progresso da actividade de análise do BitDefender. As linhas verdes fluidas mostram a actividade da análise no seu sistema local. As linhas vermelhas fluidas mostram a actividade da análise na sua ligação à Internet.
Carregar o BitDefender ao iniciar o Windows	Ao ativar esta opção o interface BitDefender do usuário é carregado no iniciar o sistema. Esta opção não afeta o nível de protecção.
Enviar Relatórios de Vírus	Ao activar esta opção, os relatórios das análises são enviados para o Laboratório BitDefender para análise. Estes relatórios não contêm qualquer informação considerada pessoal e



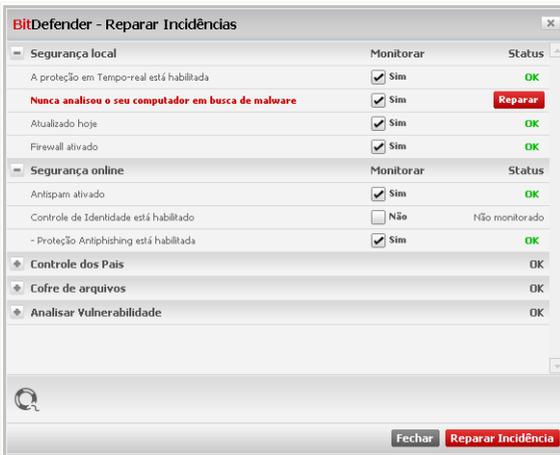
Item	Descrição
	confidencial (tal como o nome, endereço IP, etc) e não serão usados para qualquer propósito comercial.
Detecção de Surtos	Ao activar esta opção, os relatórios relativos a potenciais surtos de vírus são enviados para o Laboratório BitDefender para análise. Estes relatórios não contém qualquer informação considerada pessoal e confidencial (tal como o nome, endereço IP, etc) e não serão usados para qualquer propósito comercial.



12. Barra de Estado

Como pode rapidamente notar, na parte superior da janela do BitDefender Internet Security 2009 existe uma barra de estado que mostra o número de incidências pendentes. Clique no botão **Reparar Todas** para facilmente remover quaisquer ameaças à segurança do seu computador. Uma janela de estado de segurança irá aparecer.

O estado de segurança mostra uma lista facilmente gerida e sistematicamente organizada das vulnerabilidades de segurança do seu computador. O BitDefender Internet Security 2009 irá informá-lo sempre que surja um problema que possa afectar a segurança do seu computador.



Barra de Estado

12.1. Segurança Local

Sabemos que é importante ser avisado sempre que haja um problema que afecte a segurança do seu computador. Ao monitorizar cada módulo de segurança, o BitDefender Internet Security 2009 avisá-lo-á não só quando você configura as definições que poderão afectar a segurança do seu computador, mas também quando se esquece de fazer tarefas importantes.



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

<i>Incidência</i>	<i>Descrição</i>
Protecção de arquivos em Tempo-real está activada	Assegura que todos os arquivos serão analisados, à medida que eles forem acedidos por si ou por uma aplicação do seu sistema.
Você analisou o seu computador em busca de malware hoje	É altamente recomendável que leve a cabo uma análise a-pedido tão depressa quanto possível para verificar que os arquivos armazenados no seu computador estão livres de malware.
Actualização automática está activada	Por favor mantenha a actualização automática activada para assegurar que as assinaturas de malware do seu produto BitDefender são actualizadas numa base regular.
Actualizar Agora	A actualização do produto e das assinaturas de malware está a ser levada a cabo.
Firewall activada	Protege o seu computador contra os hackers e os ataques maliciosos vindos do exterior.

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

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

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

12.2. Segurança On-line

As incidências que dizem respeito à segurança on-line são descritas em frases bem explícitas. Ao mesmo tempo que a frase, se existe algo que possa ameaçar a



segurança do seu computador, verá um botão de estado vermelho denominado **Reparar**. De outra forma, um botão verde de estado a dizer **OK** é mostrado.

<i>Incidência</i>	<i>Descrição</i>
Antispam activado	Asegura que os seus e-mails são analisados em busca de malware e filtrados de spam.
Controle de Identidade activado	Ajuda-o a manter os seus dados confidenciais seguros ao analisar o tráfego web e de e-mail em busca de palavras-chave. É recomendável que mantenha o Controle de Identidade ativado, para evitar que a sua informação confidencial (endereço de e-mail, IDs de usuário, palavras-passe, números de cartões de crédito, etc) seja roubada.
A protecção antiphishing Firefox está activada	BitDefender protege-o contra as tentativas de phishing quando está a navegar na Internet.
A protecção antiphishing Internet Explorer está activada	BitDefender protege-o contra as tentativas de phishing quando está a navegar na Internet.

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

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

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

12.3. Cofre de arquivos

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



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

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

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

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

12.4. Analisar Vulnerabilidades

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

<i>Incidência</i>	<i>Descrição</i>
A verificação de Vulnerabilidades está activada	Monitoriza as actualizações do Microsoft Windows, do Microsoft Windows Office e as palavras-passe das contas Microsoft Windows para assegurar que o seu SO está actualizado e não se encontra vulnerável à quebra de palavras-passe.
Actualizações Críticas da Microsoft	Instala Actualizações Críticas da Microsoft que estejam disponíveis.
Outras Actualizações da Microsoft	Instala Actualizações não-críticas da Microsoft que estejam disponíveis.
A Actualização Automática do	Instala novas actualizações de segurança do Windows assim que estejam disponíveis.



<i>Incidência</i>	<i>Descrição</i>
Windows está activada	
Admin (senha forte)	Indica a força de cada senha de usuários específicos

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

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

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



13. Registro

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

13.1. Passo 1/1 - Registar BitDefender Internet Security 2009

The screenshot shows the 'Assistente de Registro' (Registration Assistant) window for BitDefender Internet Security 2009. The window title is 'BitDefender Internet Security 2009'. The main content area is titled 'Assistente de Registro' and contains the following information:

- Instructions: 'Por favor siga as instruções abaixo para registrar o seu produto BitDefender.'
- Current license status: 'O estado atual da licença do seu BitDefender é: **Trial**'
- Current license key: 'A sua chave de licença BitDefender atual é: **BE1B409B7E067AD03090**'
- Expiration: 'Esta chave de licença irá expirar em: **30 dias**'

There are three main sections on the left side of the window:

- Opções de Licença**: 'Se deseja manter a chave atual, por favor selecione a primeira opção. Se deseja adicionar uma nova chave, por favor selecione a segunda opção e insira a chave na caixa abaixo.'
 - Continuar a usar a chave atual
 - Quero registrar o produto com uma nova chave
- Compre uma Chave de Licença**: 'Para adquirir uma chave de licença, clique no link abaixo.'
 - [Renove a sua chave de licença do seu BitDefender](#)

On the right side, there is a section titled 'Aqui é onde pode encontrar a sua Chave de Licença:' with three options:

- 1) Etiqueta do CD-Rom (with an image of a CD-ROM)
- 2) Cartão de registo do produto (with an image of a registration card)
- 3) E-mail da compra online (with an image of an email interface)

At the bottom of the window, there is a search icon, the BitDefender logo, and two buttons: 'Concluir' and 'Cancelar'.

Registro

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

Para registar BitDefender Internet Security 2009:

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



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



Nota

Pode encontrar a sua chave de licença:

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

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

Clique em **Finalizar**.



14. Histórico

O link **Histórico** no fundo da janela do Centro de Segurança BitDefender abre uma outra janela com o histórico & dos eventos. Esta janela oferece uma visão geral dos eventos relacionados com a segurança. Por exemplo, pode 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.

Nome da ação	Ação tomada	Data e hora
Atualização com Sucesso	O produto foi atualizado...	12/30/2008 2:15:39 PM
Atualização com Sucesso	O produto foi atualizado...	12/30/2008 2:07:19 PM
Atualização com Sucesso	O produto foi atualizado...	12/30/2008 2:06:03 PM
Arquivos Downloaded	Os arquivos da atualizaç...	12/30/2008 2:06:03 PM
Atualização com Sucesso	O produto foi atualizado...	12/30/2008 2:06:03 PM
Atualização com Sucesso	O produto foi atualizado...	12/30/2008 2:00:10 PM
Arquivos Downloaded	Os arquivos da atualizaç...	12/30/2008 2:00:10 PM
Atualização com Sucesso	O produto foi atualizado...	12/30/2008 2:00:10 PM

Eventos

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

- **Antivírus**
- **Firewall**
- **Antispam**
- **Controle Privacidade**
- **Controle dos Pais**
- **Actualização**



- **Rede**
- **Cofre de arquivos**

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

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



Administração Avançada



15. Geral

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

15.1. Painel

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

BitDefender Internet Security 2009 - Trial MUDAR MODO BÁSICO

ESTADO: Existe 1 incidência pendente REPARAR

Geral Painel Opções Info Sistema

Antivirus

Antispam

Controle dos Pais

Privacidade

Firewall

Vulnerabilidade

Criptografia

Modo Jogo/Laptop

Rede

Atualização

Registo

Estatísticas

Arquivos analisados: 2722

Arquivos desinfetados: 0

Arquivo infectado detectado: 0

Última análise: Nunca

Próxima análise: 31/12/2008 02:00

Atividade Local

Visão Geral

Última atualização: 30/12/2008 14:15

Minha Conta: Sem Conta

Registo: Trial

Expira em: 30 dias

Atividade de rede

Para descobrir mais sobre cada opção apresentada na Interface do Usuário BitDefender, por favor mova o seu cursor sobre a janela. Um texto de ajuda relevante será apresentado nessa área.

bitdefender Comprar/Renovar - Minha Conta - Registo - Ajuda - Suporte - Histórico

Painel

O painel é composto de várias secções:

- **Estatísticas** - Mostra informação importante com respeito à actividade do BitDefender.



- **Visão Geral** - Mostra o estado da actualização, o estado da sua conta, e informação do seu registo e licença.
- **Zona PC** - Indica a evolução do número de objectos analisados pelo BitDefender Antimalware. A altura da barra indica a intensidade do tráfego durante esse intervalo de tempo.
- **Zona Net** - Indica a evolução do tráfego de rede, filtrado pela Firewall do BitDefender. A altura da barra indica a intensidade do tráfego durante esse intervalo de tempo.

15.1.1. Estatísticas

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

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

15.1.2. Sumário

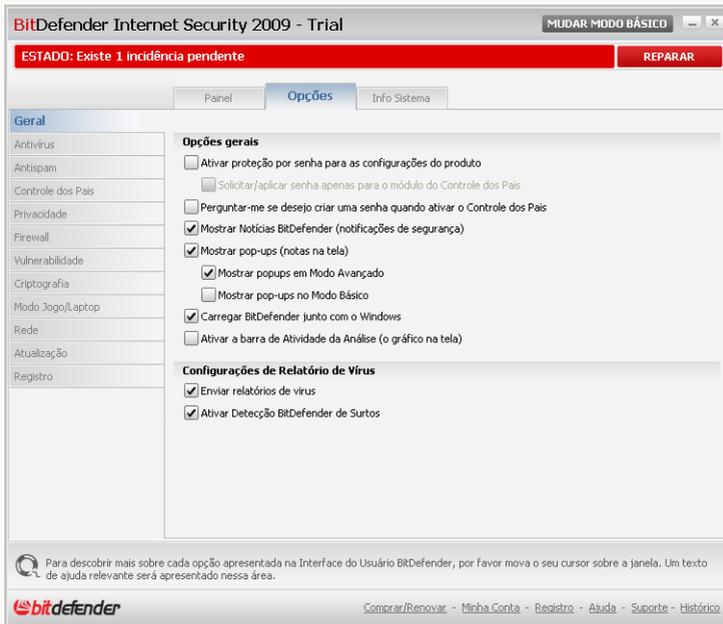
Aqui pode ver um resumo das estatísticas respeitantes ao estado da actualização, ao estado da sua conta, registo e informação de licença.



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

15.2. Opções

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



Configurações Gerais

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

15.2.1. Configurações Gerais

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



Nota

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

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



BitDefender

Deve inserir uma senha e re-inseri-la para confirmar.

A senha deve conter no mínimo 8 caracteres.

Senha

Redigite a senha

OK Cancelar

Confirmar senha

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

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

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



Importante

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

- **Solicitar senha quando activar o Controle dos Pais** - se esta opção estiver activada e nenhuma senha estiver definida, ser-lhe-á solicitado que a defina quando activar o Controle dos Pais. Ao definir uma senha, irá prevenir que outros usuários com direitos administrativos possam mudar as suas definições do Controle dos Pais que configurou para um determinado usuário.
- **Receber Notícias BitDefender (notificações de segurança)** - de tempos em tempos recebe notificações de segurança com relação a novas epidemias de vírus, enviadas pelo servidor BitDefender.
- **Mostrar pop-ups (notas na tela)** - mostrar janelas pop-up a respeito do status do produto. Você pode configurar para mostrar pop-ups somente quando usar o Modo Básico ou o Modo Avançado.
- **Carregar BitDefender junto com o Windows** - inicia automaticamente o BitDefender na inicialização do sistema. Nós recomendamos que você mantenha esta opção seleccionada.
- **Permitir que a barra de Análise de Atividades (na tela gráfica de atividade do produto)** - mostra a **Barra de Análise de Atividade** sempre que você se logar ao



Windows. Limpe esta caixa se deseja que a barra de Actividade da Análise não seja mostrada daí em diante.



Nota

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

15.2.2. Configurações do Relatório de Vírus

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

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

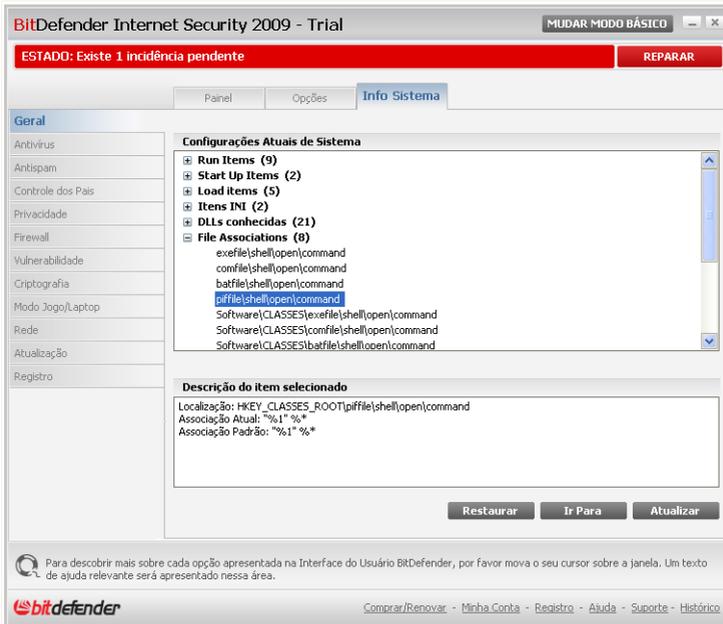
- **Activar Detecção de Epidemias BitDefender** - envia relatórios para os Laboratórios do BitDefender com respeito a potenciais epidemias de vírus.

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

15.3. Informação do Sistema

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

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



Informação do Sistema

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

Três botões estão disponíveis:

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



Nota

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

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



16. Antivírus

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

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



Nota

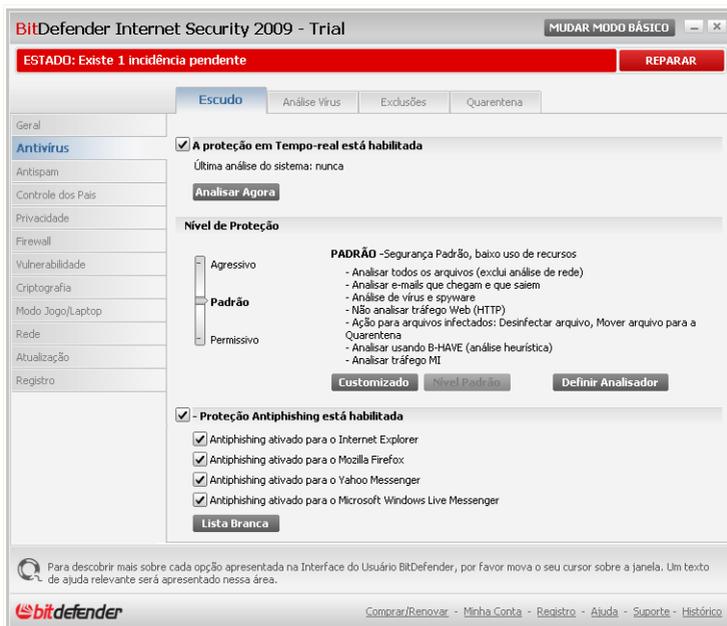
A protecção em Tempo-real, também referida como análise no acesso - os arquivos são analisados à medida que os usuários lhes acessem.

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

16.1. Protecção em Tempo-real

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

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



Protecção em Tempo-real

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



Importante

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

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

16.1.1. Configurar Nível de Protecção

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

Existem 3 níveis de protecção:



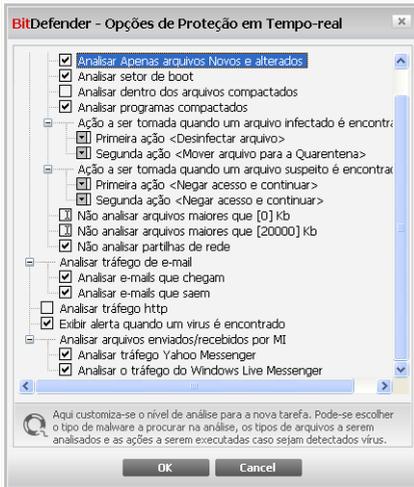
Nível de Protecção	Descrição
Permissivo	<p>Cobre necessidades básicas de segurança. O nível de consumo de recursos é muito baixo.</p> <p>Programas e mensagens de e-mail de entrada são apenas analisados em busca de vírus. Para além da tradicional análise baseada em assinaturas, a análise heurística também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

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

16.1.2. Personalizando Nível de Protecção

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

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



Configurações do Escudo

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



Nota

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

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

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



Opção	Descrição
	<p>Verificar apenas os arquivos de programas</p> <p>Apenas arquivos de programas serão verificados. Isso significa apenas os arquivos com as seguintes extensões: .exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml e .nws.</p>
	<p>Verificar as extensões definidas pelo usuário</p> <p>Apenas os arquivos com as extensões especificadas pelo usuário serão verificados. Essas extensões devem ser separadas por ";".</p>
	<p>Analisar em busca de riskware</p> <p>Analisar em busca de riskware. Os arquivos detectados serão tratados como arquivos infectados. O software que inclua componentes de adware poderá deixar de funcionar se esta opção estiver activa.</p> <p>Selecione Excluir da análise dialers e aplicações se deseja excluir este tipo de arquivos da análise.</p>
Analisar o sector de arranque	Para verificar o setor de boot do sistema.
Verificar dentro dos arquivos compactados	Arquivos de backup acessados também serão verificados. Com essa opção ativada, o computador ficará lento.
Verificar programas compactados	Todos os programas compactados serão verificados.
Primeira Acção.	Seleccionar do menu drop-down a primeira acção a levar a cabo sobre um arquivo infectado ou suspeito.
	<p>Negar acesso e continuar</p> <p>Caso um arquivo infectado seja detectado, o acesso a ele será negado.</p>



Opção	Descrição
Limpar arquivo	Desinfecta os arquivos infectados.
Apagar arquivo	Apaga o arquivo infectado imediatamente, sem avisar.
Mover o arquivo para a quarentena	Move os arquivos infectados para a quarentena.
Segunda Ação	Selecione através do menu a segunda ação a ser tomada em arquivos infectados, caso a primeira ação falhe.
Negar acesso e continuar	Caso um arquivo infectado seja detectado, o acesso a ele será negado.
Apagar arquivo	Apaga o arquivo infectado imediatamente, sem avisar.
Mover o arquivo para a quarentena	Move os arquivos infectados para a quarentena.
Não analisar arquivos maiores do que [x] Kb	Digite o tamanho máximo dos arquivos a serem verificados. Se o tamanho for 0Kb, todos os arquivos serão verificados.
Não analisar arquivos maiores do que [20000] Kb	Insira o tamanho máximo dos arquivos comprimidos a serem analisados em kilobytes (KB). Se deseja analisar todos os arquivos, independentemente do seu tamanho, insira 0.
Não analisar partilhas de redes	Se esta opção estiver ativada, BitDefender não irá analisar as partilhas de rede, permitindo um acesso de rede mais rápido. Recomendamos que ative esta opção apenas se a rede de que faz parte estiver protegida por uma solução antivírus.

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

As seguintes opções estão disponíveis:



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

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

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

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

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

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

16.1.3. Configurar o Analisador Comportamental

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

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



Alerta do Analisador Comportamental

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

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

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



Configurações do Analisador Comportamental

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



Importante

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

Configurar Nível de Protecção

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



Nota

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

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

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

Gerir Aplicações Excluídas

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

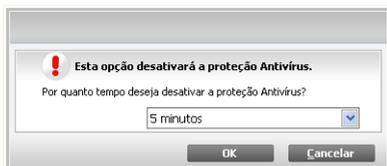
Para gerir as aplicações excluídas, pode usar os botões colocados no topo da tabela:

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



16.1.4. Desactivando a Protecção em Tempo-real

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



Desactivar Protecção em Tempo-real

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



Atenção

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

16.1.5. Configurar Protecção Antiphishing

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

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

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

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



Lista Branca do AntiPhishing

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

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



Nota

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

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

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

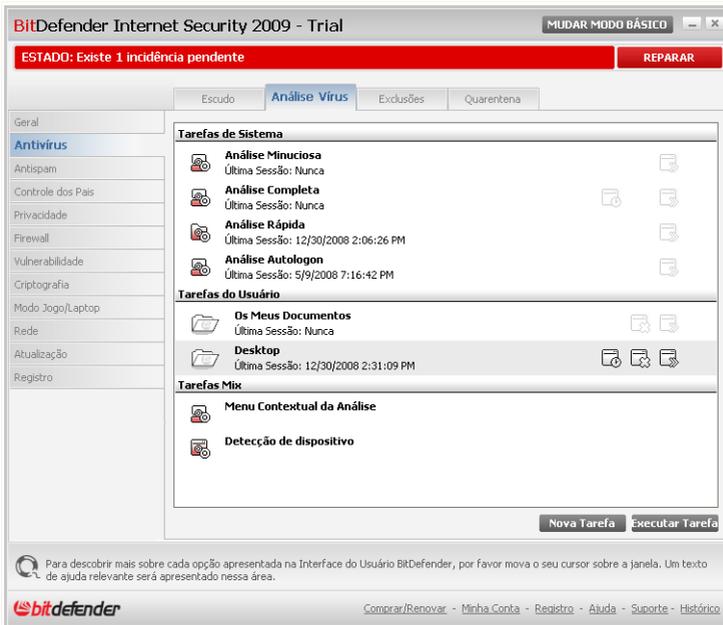
16.2. Análise A-pedido

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



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

Para configurar e iniciar uma análise a-pedido, clique **Antivírus>Análise** no Modo Avançado.



Tarefas de Análise

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



16.2.1. Tarefas de Análise

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

Cada tarefa tem uma janela de **Propriedades** que o permite configurar a tarefa e ver os resultados da análise. Para mais informação, consulte "*Configurar Tarefas de Análise*" (p. 146).

Existem três categorias de tarefas de análise:

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

Tarefa Padrão	Descrição
Análise Minuciosa do Sistema	Analisa todo o sistema. Na configuração por defeito, faz uma análise em busca de todo o tipo de malware que ameace 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 análise em busca de todo o tipo de malware que ameace a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.
Análise Rápida do Sistema	Analisa as pastas <code>Windows</code> , <code>Programas</code> e <code>All Users</code> . Na configuração padrão, analisa em busca de todo o tipo de malware, excepto rootkits, mas não analisa a memória, o registo ou os cookies.
Análise Autologon	Analisar os itens que são executados quando o usuário entra no Windows. Por default, a análise de autologon está desabilitada. Se você deseja usar esta tarefa, clique com o botão direito do mouse nela, selecione Agendar e programe a tarefa para rodar quando o sistema iniciar . Você poderá especificar em quanto tempo, após o início, a tarefa deverá começar a rodar (em minutos).



Nota

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

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

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

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

Três botões estão disponíveis à direita de cada tarefa:

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



Nota

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

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

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

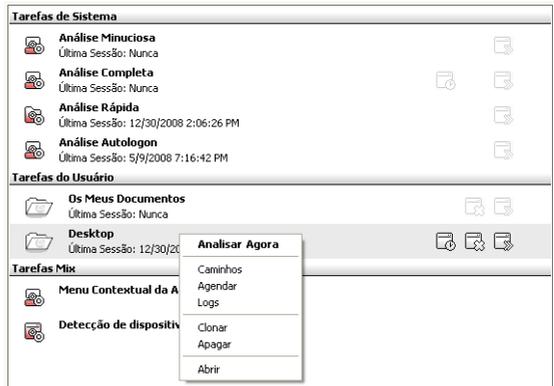


16.2.2. Usando o Menú de Atalho

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

Os seguintes comandos estão disponíveis no menu de atalho:

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



Menú de Atalho



Nota

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

- **Agenda** - abre a janela **Propriedades**, Aba **Agenda**, onde você poderá agendar a tarefa seleccionada.
- **Logs** - abre a janela **Propriedades**, Aba **Logs**, onde você pode ver os relatórios gerados após as tarefas seleccionadas serem executadas.
- **Duplicar** - duplica a tarefa seleccionada. Isto é útil na criação de novas tarefas, pois pode modificar as definições da tarefa duplicada.
- **Apagar** - apaga a tarefa seleccionada.



Nota

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

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



Nota

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

16.2.3. Criando Tarefas de Análise

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

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

16.2.4. Configurar Tarefas de Análise

Cada tarefa de análise tem a 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. 165).

Configurar Definições da Análise

Para configurar as opções de análise de uma específica tarefa de análise, faça clique-botão direito e seleccione **Propriedades**. A seguinte análise irá aparecer:



Sumário

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

Escolher Nível de Análise

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

Existem 3 níveis de análise:

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



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

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

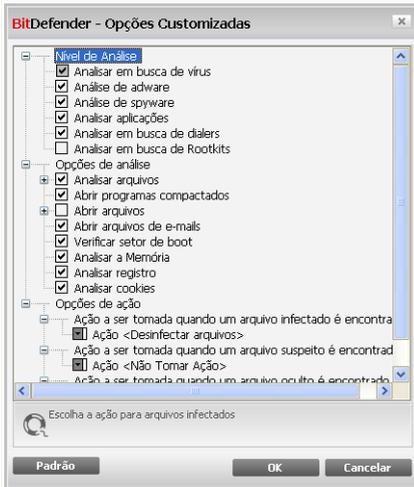
- **Executar a análise com Baixa prioridade.** Diminui a prioridade do processo de verificação. Você permitirá outros programas a executarem mais rapidamente e aumentar o tempo de verificação.
- **Minimizar a janela de análise no início para a barra de tarefas.** Minimiza a janela de verificação para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

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

Personalizar o Nível de Análise

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

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



Opções de Análise

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

As opções de análise são agrupadas em 3 categorias:

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

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



Opção	Descrição
Analisar em busca de spyware	Analisa em busca de ameaças de spyware. Estes arquivos serão tratados como arquivos infectados.
Analisar aplicações	Analisar aplicações legítimas que podem ser usadas como ferramenta de espionagem, para ocultar aplicações maliciosas ou outras intenções maliciosas.
Analisa em busca de dialers	Procura aplicações de ligação para números de valor acrescentado. Estes arquivos serão tratados como arquivos infectados. O software que inclua componentes de ligação deste tipo poderá deixar de funcionar se esta opção estiver activa.
Analisar em busca de Rootkits	Analisa em busca de objectos ocultos (arquivos e processos), conhecidos por rootkits.

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

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



Opção	Descrição
Abrir programas compactados	Arquivos de backup acessados também serão verificados.
Abrir arquivos	Todos os arquivos compactados serão verificados. Analisar arquivos comprimidos aumenta o tempo da análise e requer mais recursos do sistema. Pode clicar em Limite de tamanho dos arquivos e inserir o tamanho máximo em kilobytes (KB) dos arquivos a serem analisados.
Abrir arquivos de e-mails	Para verificar dentro de arquivos de e-mails.
Verificar setores de boot	Para verificar o setor de boot do sistema.
Verificar Memória	Analisa a memória em busca de vírus e outro malware.
Verificar registo	Analisa entradas de registo.
Verificar cookies	Analisa os arquivos cookie.

- **Opções de ação.** Especifique a acção a tomar sobre cada categoria de arquivos detectados usando as opções da categoria **Opções de acção**.



Nota

Para definir uma nova acção, faça clique na actual acção e seleccione a opção desejada no menu.

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

Ação	Descrição
Nenhum (objetos de log)	Nenhuma ação será tomada em arquivos infectados. Esses arquivos aparecerão no arquivo de relatório.
Desinfetar arquivos	Remover o código de malware dos arquivos infectados detectados.



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

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

Ação	Descrição
Nenhum (objetos de log)	Nenhuma acção será levada a cabo sobre os arquivos suspeitos. Estes arquivos aparecerão no arquivo de relatório.
Apagar arquivos	Apaga imediatamente e sem qualquer aviso, os arquivos suspeitos.
Mover arquivos para a quarentena	Move os arquivos suspeitos para a quarentena. O arquivos em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.



Nota

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

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

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



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

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

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

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



Ação	Descrição
Não Tomar Acção	Apenas manter registo dos arquivos comprimidos suspeitos no relatório da análise. Após a análise terminar, pode abrir o relatório da análise para ver informação sobre esses arquivos.
Apagar arquivos	Apaga imediatamente e sem qualquer aviso, os arquivos suspeitos.
Mover arquivos para a quarentena	Move os arquivos suspeitos para a quarentena. Os arquivos em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.

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

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



Nota

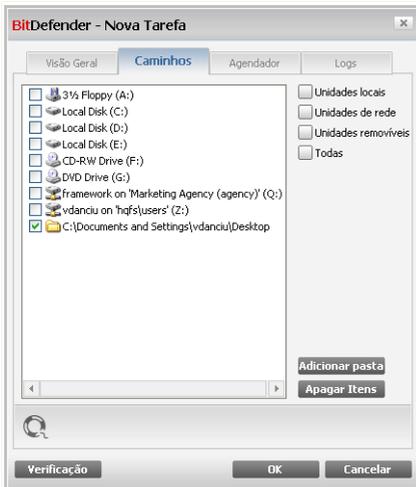
Se escolher ignorar os arquivos detectados ou se a ação escolhida falhar, terá de escolher uma ação no assistente de análise.

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



Definir Alvo da Análise

Para ver o alvo da análise de uma determinada tarefa de análise do sistema de um usuário específico, faça clique com o botão direito do mouse sobre a tarefa seleccione **Mostrar Caminho da Tarefa**. A seguinte análise irá aparecer:



Alvo da Análise

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

Essa seção contém os seguintes botões:

- **Adicionar Itens** - abre uma janela onde você pode seleccionar o(s) arquivo(s) / pasta (s) que deseja verificar.



Nota

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

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



Nota

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

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

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



Nota

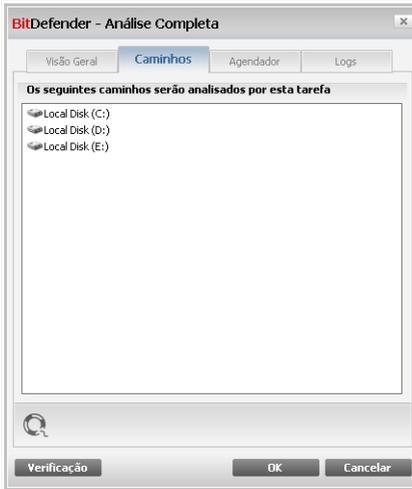
Se você quer verificar todo o seu computador contra vírus selecione a caixa correspondente a **Todas**.

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

Ver o Alvo da Análise das Tarefas de Sistema

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

Para ver o alvo da análise de uma determinada tarefa de análise do sistema, faça clique com o botão direito do mouse sobre a tarefa selecione **Mostrar Caminho da Tarefa**. Por exemplo, para **Análise Completa do Sistema**, a seguinte janela irá aparecer:



Alvo da Análise da Análise Completa do Sistema

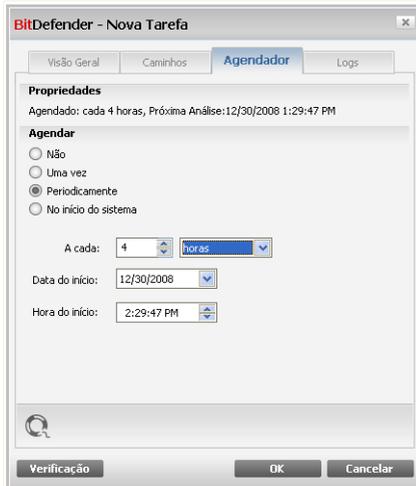
Análise Completa do Sistema e **Análise Minuciosa do Sistema** analisarão todas as drives locais, enquanto **Análise Rápida do Sistema** apenas analisará as pastas Windows e Programas .

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

Agendar Tarefas de Análise

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

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



Agendador

Se houver, pode ver a tarefa agendada.

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

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

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

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

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



16.2.5. Analisar objectos

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



Nota

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

Métodos de Análise

O BitDefender permite quatro tipos de verificação solicitada:

- **Análise imediata** - executa uma tarefa de análise das tarefas do sistema/usuário.
- **Verificação contextual** - clique com o botão direito em um arquivo ou pasta e escolha BitDefender Antivirus 2009.
- **Verificação Arraste & Solte** - arraste e solte um arquivo ou pasta sobre a **Barra de Atividade**;
- **Análise manual** - Use a Análise Manual do BitDefender para seleccionar directamente os arquivos ou pastas a serem analisados.

Verificação imediata

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

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

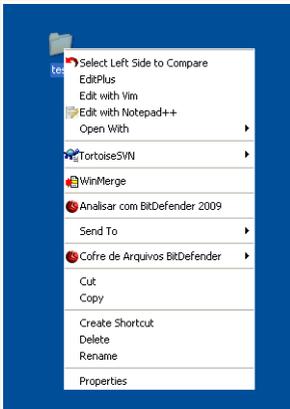
- faça duplo-clique com o rato sobre a tarefa desejada da lista.
- clique no botão  **Analisar agora** da correspondente tarefa.
- seleccione a tarefa e depois clique em **Executar Tarefa**.

O Analisador BitDefender aparecerá e a análise será iniciada. Para mais informação, por favor consulte a seção "**Analisador BitDefender**" (p. 161).



Verificação contextual

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



Verificação Contextual

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

O Analisador BitDefender aparecerá e a análise será iniciada. Para mais informação, por favor consulte a seção *"Analisador BitDefender"* (p. 161).

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

Verificação Arraste & Solte

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



Arraste o arquivo



Solte o arquivo



O Analisador BitDefender aparecerá e a análise será iniciada. Para mais informação, por favor consulte a seção *“Analisador BitDefender”* (p. 161).

Verificação Manual

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



Nota

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

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



Verificação Manual

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

O Analisador BitDefender aparecerá e a análise será iniciada. Para mais informação, por favor consulte a seção *“Analisador BitDefender”* (p. 161).

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.



BitDefender 2009 - Desktop

Análise Antivírus - Passo 1 de 3

Passo 1 | Passo 2 | Passo 3

Status da Análise

Item atual analisado =>HKEY_LOCAL_MACHINE\SOFTWARE\CLA... 7.0\PDFMAKER\MAIL\OUTLOOK\PDFMOUTLOOK.DLL

Tempo Decorrido: 00:00:56

Arq/seg: 7

Estatísticas da Análise

Itens analisados: 422

Itens não analisados: 0

Itens infectados: 0

Itens Suspeitos: 0

Itens Ocultos: 0

Processos Ocultos: 0

Análise antivírus em progresso. A seção acima indica o progresso e a seção abaixo as estatísticas do processo. Por padrão, o BitDefender tentará desinfetar os itens detectados como infectados.

bitdefender Pausar Parar Cancelar

Analisar

Pode ver o estado da análise e as estatísticas (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.

Espreze 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.



The screenshot shows the BitDefender 2009 Desktop interface. The window title is "BitDefender 2009 - Desktop". The main content area is titled "Análise Antivírus - Passo 2 de 3". Below this, there are three tabs: "Passo 1", "Passo 2" (selected), and "Passo 3". The "Resumo de Resultados" section indicates "1 ameaça(s) que afetaram 1objeto(s) requerem a sua atenção". A table lists one threat: "EICAR-Test-File (not a virus)" with a "falha 1 incidência (Falhou a desinfecção)". A "Mover para a quarentena" button is visible next to the threat. Below the table, it says "Incidências Resolvidas: 0". A table with columns "Caminho de arquivo", "Nome da Ameaça", and "Resultado da Ação" is present but empty. At the bottom, there is a message: "o BitDefender detectou e bloqueou vírus no seu computador! Esta é a lista das ameaças. Por favor clique no nome do vírus para ver a lista dos correspondentes itens infectados." and a "Continuar" button.

Ações

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

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

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

As seguintes opções podem aparecer no menu:

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



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

Passo 3/3 - Ver Resultados

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

	Passo1	Passo2	Passo3
Resumo de Resultados			
Itens resolvidos:	1		
Itens não resolvidos:	0		
Itens Protegidos por senha:	0		
Itens Ignorados:	0		
Itens Falhados:	0		

1 ameaça foi removida.

o BitDefender detectou e bloqueou vírus no seu computador! Esta é a lista das ameaças. Por favor clique no nome do vírus para ver a lista dos correspondentes itens infectados.

Mostrar Log **Fechar**

Sumário

Pode ver o sumário dos resultados. Clicar **Mostrar Relatório** para ver o relatório da análise.



Importante

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

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

BitDefender Não Pode Resolver Algumas Incidências

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



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

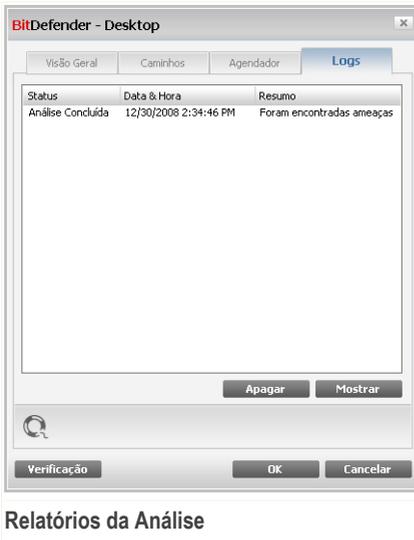
BitDefender Detectou Arquivos Suspeitos

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

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

16.2.6. Ver os Relatórios da Análise

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



Aqui pode ver os relatórios gerados cada vez que uma tarefa foi executada. Cada arquivo no relatório contém informação sobre o estado do processo de análise



registado, a data e hora quando a análise foi feita e um resumo dos resultados da análise.

Dois botões estão disponíveis:

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



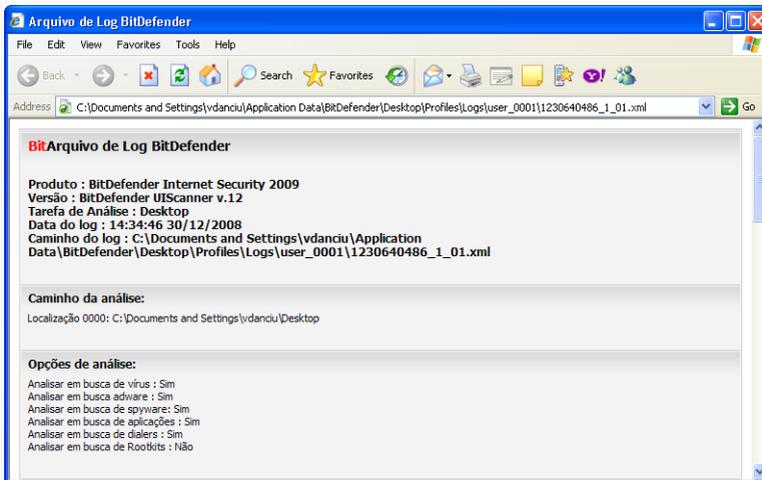
Nota

Também, para ver ou apagar um arquivo, faça duplo-clique com o rato sobre o arquivo e seleccione a opção correspondente do menu de atalho.

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

Exemplo de Relatório da Análise

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



Exemplo de Relatório da Análise

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



16.3. Objectos a Excluir da Análise

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

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

Dois tipos de objectos podem ser excluídos da análise:

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



Nota

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

Para ver os objectos excluídos da análise, vá para **Antivírus>Excepções** no Modo Avançado.



Excluir objetos da análise	Ao acessar	Ao solicitar
Arquivos e pastas		
c:\documents and settings\vdanciu\desktop\excar_test\	Sim	Não
Extensões		
*.jpg (Bitmap graphics (Joint Photography Experts Group))	Não	Sim
*.png	Não	Sim
*.txt (Arquivo de texto)	Não	Sim

Exceções

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



Nota

As exceções definidas aqui NÃO serão aplicada à análise contextual.

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

Para editar uma entrada da lista, seleccione-a e clique no botão **Editar**. Aparecerá uma nova janela onde poderá alterar a extensão ou o caminho a ser excluído e o tipo de análise da qual quer que eles sejam excluídos. Faça as alteração necessárias e clique **OK**.



Nota

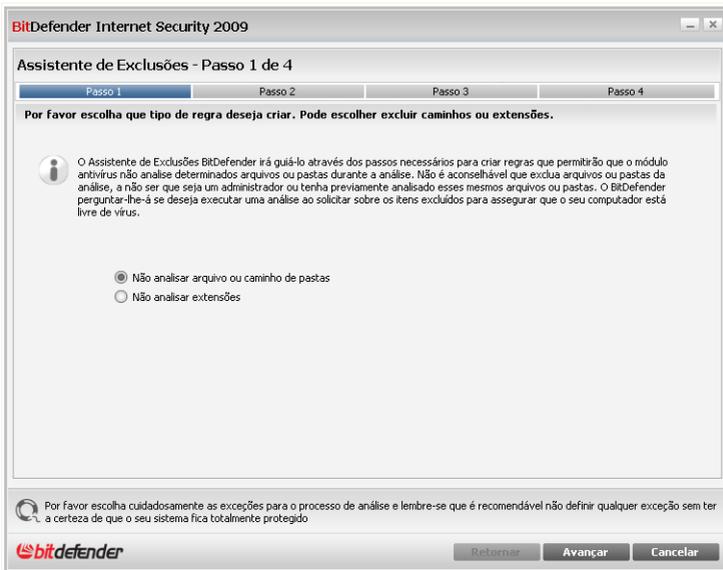
Podem também clicar no objecto usando o botão direito do mouse e utilizar as opções que aparecem no menu de atalho para o editar ou apagar.

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

16.3.1. Excluir Caminhos da Análise

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

Passo 1/4 - Seleccionar o Tipo de Objecto



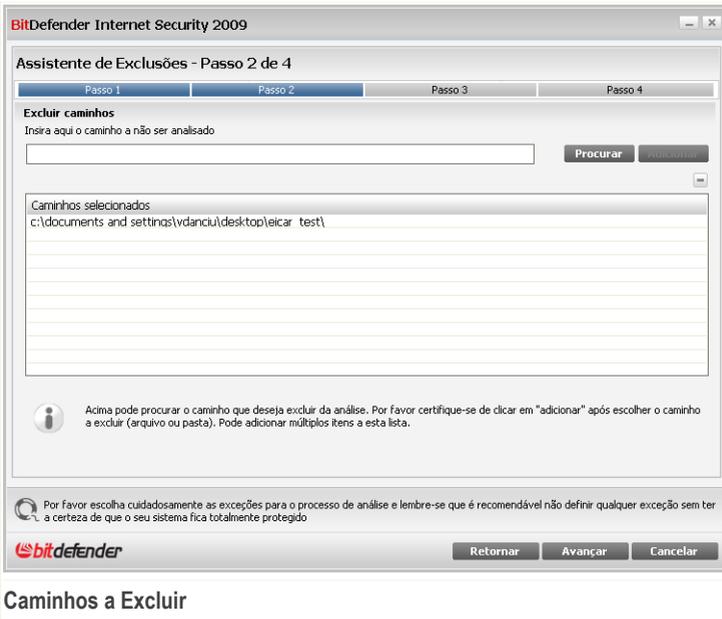
Tipo de Objecto

Selecione a opção de excluir um caminho da análise.

Clique em **Próximo**.



Passo 2/4 - Especificar Os Caminhos a Excluir



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

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



Nota

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

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

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

Clique em **Próximo**.



Passo 4/4 - Analisar arquivos Excluidos



Analisar arquivos Excluidos

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

Clique em **Finalizar**.

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

16.3.2. Excluir Extensões da Análise

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



Passo 1/4 - Seleccionar o Tipo de Objecto



Tipo de Objecto

Selecione a opção de excluir uma extensão da análise.

Clique em **Próximo**.



Passo 2/4 – Especificar Extensões a Excluir



Extensões a Excluir

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

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



Nota

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

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

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

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



Passo 4/4 - Seleccionar o Tipo de Análise



Tipo de Análise

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

Clique em **Finalizar**.

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

16.4. Área de Quarentena

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

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



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

16.4.2. Configurar opções da Quarentena

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



Opções da quarentena

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

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



Nota

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



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



Nota

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

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



Nota

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

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

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



17. Antispam

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

17.1. Compreender o Antispam

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

17.1.1. Filtros Anti-spam

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



Nota

Pode activar/desactivar cada um destes filtros na secção da [Configuração](#) no módulo de **Antispam**.

Lista de Spammers / Amigos

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

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



Nota

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

Filtro de Caracteres

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

Filtro de Imagem

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

Filtro de URL

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

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

Filtro NeuNet (Heurístico)

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

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



Nota

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

Filtro Bayesiano

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

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

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



Importante

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



Nota

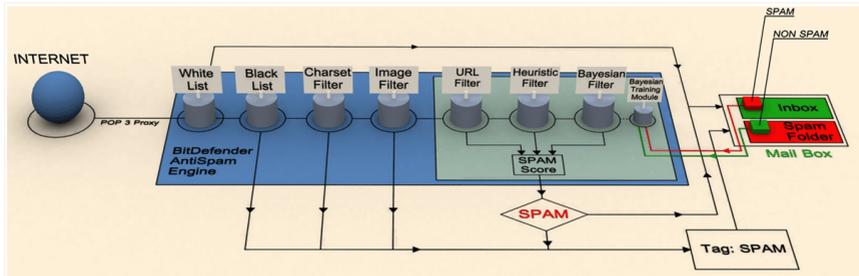
Cada vez que executa uma actualização:

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

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

17.1.2. Operação Antispam

O esquema a seguir mostra como o BitDefender funciona.



Operação Antispam

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

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

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

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

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

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

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



Nota

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

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

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

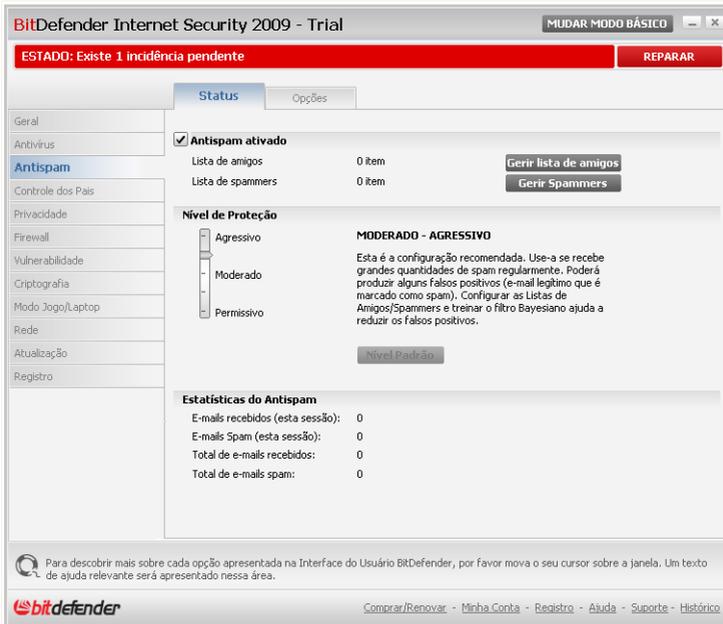


Importante

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

17.2. Status

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



Status do Antispam

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



Importante

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

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

17.2.1. Definir Nível de Protecção

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



Existem 5 níveis de protecção:

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

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



17.2.2. Configurar a Lista de Amigos

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



Nota

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

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



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

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



Importante

Syntax: nome@domínio.com.



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



Importante

Syntax:

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

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

Use os botões **Salvar**/ **Carregar** para salvar / carregar a **Lista de amigos** num local desejado. O arquivo terá a extensão `.bw1`.

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



Nota

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

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

17.2.3. Configurar a lista de Spammers

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



Nota

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

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



Lista de Spammers

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

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



Importante

Syntax: nome@domínio.com.

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



Importante

Syntax:

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



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

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

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

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

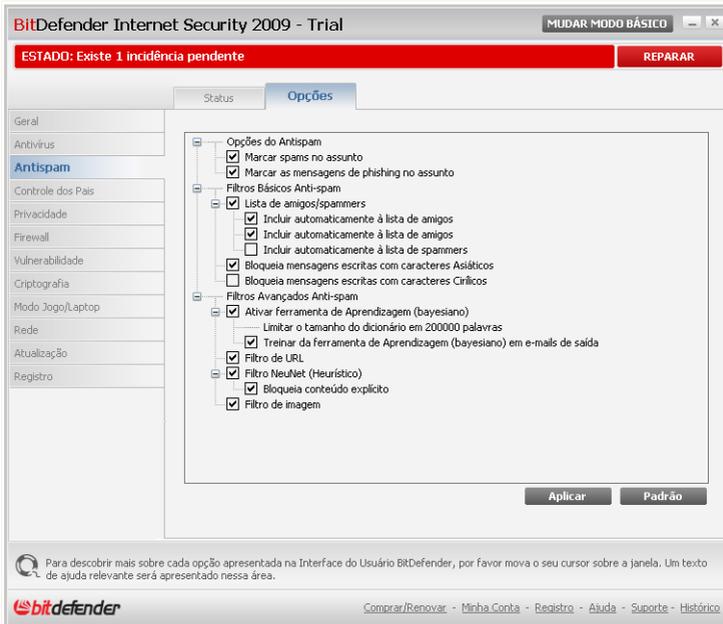


Importante

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

17.3. Opções

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



Configurações de Antispam

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



Nota

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

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

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

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



17.3.1. Configurações de Antispam

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

17.3.2. Filtros Antispam Básicos

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



Nota

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

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

17.3.3. Filtros Antispam Avançados

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



Nota

O tamanho recomendado é 200.000 palavras.



- **Treinar Motor de Aprendizagem (bayesiano) nos e-mails de saída** - treina o Motor de Aprendizagem (bayesiano) nos e-mails de saída.
- **Filtro de URL** - ativa/desativa o **Filtro de URL**;
- **Filtro NeuNet (Heurístico)** - activa/desactiva o **Filtro NeuNet (Heurístico)**;
 - **Bloqueia conteúdo explícito** - ativa/desativa a detecção de mensagens com SEXUALMENTE EXPLÍCITO no campo assunto.
- **Filtro de Imagem** - ativa/desativa o **Filtro de Imagem**.



18. Controle dos Pais

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

Pode configurar o Controle dos Pais para bloquear:

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



Importante

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

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

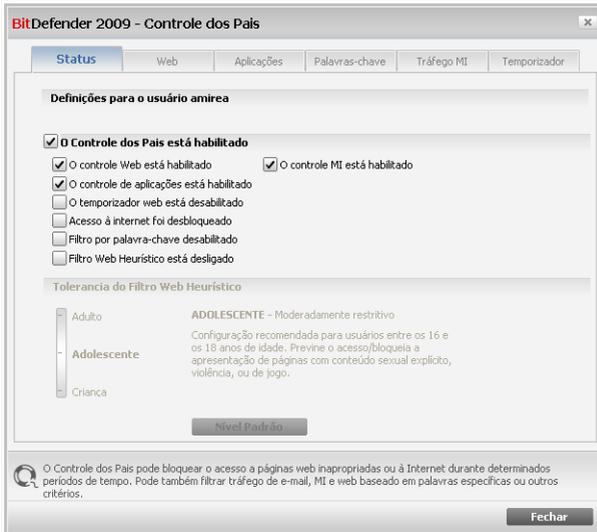
1. Criar uma conta do Windows limitada (standard) para a sua criança usar.



Nota

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

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



Estado do Controle dos Pais

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

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



Importante

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

2. Definir senha para proteger as Definições do Controle dos Pais. Para mais informação, por favor consulte o *"Proteger as Definições do Controle dos Pais"* (p. 197).
3. Marque as caixas correspondentes aos controles de proteção que deseja usar:
 - **Controle Web** - para filtrar a navegação na Internet de acordo com as regras definidas por si na secção **Web**.
 - **Controle de Aplicações** - para bloquear o acesso às aplicações no seu computador de acordo com as regras definidas por si na secção **Aplicações**.



- **Controle Mensagens Instântaneas** - permitir ou bloquear o chat IM de acordo com as regras definidas por si na secção **Tráfego IM** .
 - **Temporizador Web** - para permitir o acesso à web de acordo com a tabela de horário definida por si na secção **Temporizador** .
 - **Acesso Web** - para bloquear o acesso a todos os websites (não só apenas aqueles definidos na secção **Web**).
 - **Filtragem Palavra-chave** - para filtrar o acesso à web, ao correio electrónico e às mensagens instântaneas de acordo com as regras definidas por si na secção **Palavra-chave** .
 - **Filtro web Heurístico** - para filtrar o acesso à web de acordo com regras pré-estabelecidas baseadas em categorias de idade.
4. De forma a tirar o máximo benefício das características oferecidas pelo Controle dos Pais, deve de configurar os controles seleccionados. Para aprender como configurá-los, por favor consulte os seguintes tópicos deste capítulo.

18.1.1. Proteger as Definições do Controle dos Pais

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

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



Controle dos Pais BitDefender - Senha

Para assegurar que é o único que pode alterar as definições do Controle dos Pais, recomendamos que proteja este módulo com uma senha. Por padrão, esta apenas protegerá o módulo do Controle dos Pais mas pode alterar esta opção acessando à janela da Configuração Avançada

Deseja definir agora uma senha?

Senha

Redigite a senha

A senha deve conter no mínimo 8 caracteres.

Não solicitar uma senha quando ativar o Controle dos Pais



Definir Protecção por senha

Para definir protecção por senha, faça o seguinte:

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

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



Nota

A senha não protege quaisquer outras definições do BitDefender.

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

18.1.2. Configurar Filtro Web Heurístico

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



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

Existem 3 níveis de tolerância:

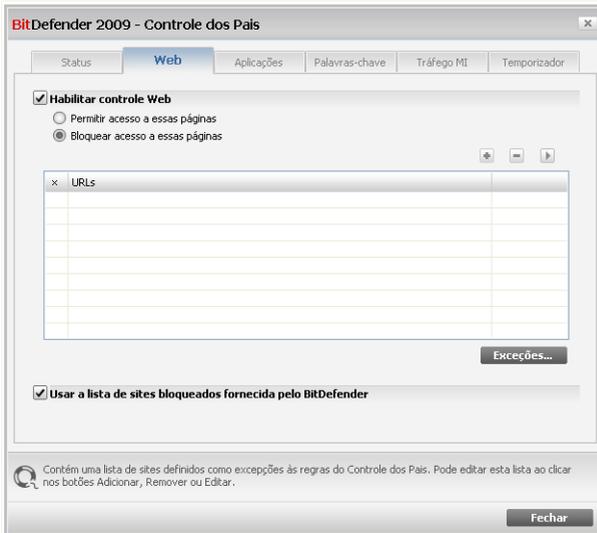
Nível de Tolerância	Descrição
Criança	Oferece um acesso restrito à web, de acordo com as configurações recomendadas para usuários menores de 14. São bloqueadas as páginas web com um potencial conteúdo prejudicial para as crianças (porno, sexualidade, drogas, hacking, etc.).
Adolescente	Oferece um acesso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

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

18.2. Controle Web

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

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



Controle Web

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

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

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

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

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

18.2.1. Assistente de Configuração

O assistente de configuração é um procedimento de um passo.



Passo 1/1 - Especifique as páginas web

Especifique as páginas web

Introduza o site web para o qual a regra será aplicada e clique em **Terminar**.



Importante

Syntax:

- *.xxx.com - a acção da regra será aplicada a todos os sites web que terminam em .xxx.com;
- *porn* - a acção da regra será aplicada a todos os sites web que contenham porn no endereço do site web;
- www.*.com - a acção da regra será aplicada a todos os sites web que tenham o sufixo de domínio com;
- www.xxx.* - a acção da regra será aplicada a todos os sites web que comecem por www.xxx. sem importar o sufixo do domínio.

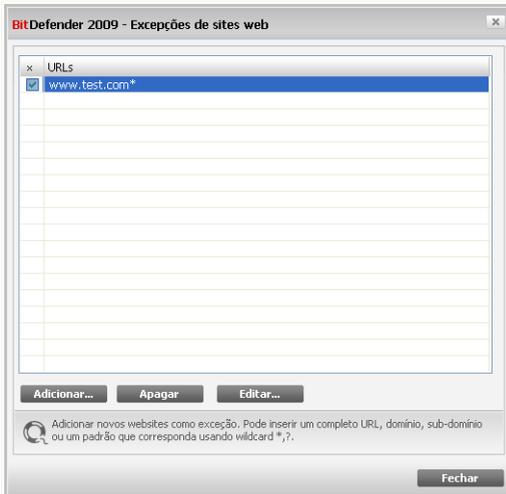
18.2.2. Especifique as exceções

Por vezes necessita de especificar exceções para uma regra em particular. Por exemplo, define uma regra que bloqueia sites que contêm a palavra "hard" no endereço (syntaxe: *hard*). Também está consciente da existência de um site denominado hard-rock onde os visitantes podem ouvir música on-line. Para abrir uma exceção



à regra previamente criada, aceda à janela **Excepções** e defina uma excepção para a regra.

Clique em **Excepções...** A seguinte janela irá aparecer:



Especificando as excepções

Clique em **Adicionar...** para especificar excepções. O **assistente de configuração** aparecerá. Complete o assistente de forma a definir a excepção.

Para apagar uma regra, apenas seleccione-a e clique em **Apagar**. Para modificar uma regra seleccione-a e clique em **Editar...** ou faça um duplo-clique nela. Para desactivar temporariamente uma regra sem a apagar, desmarque a respectiva caixa de selecção.

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

18.2.3. Lista Negra Web BitDefender

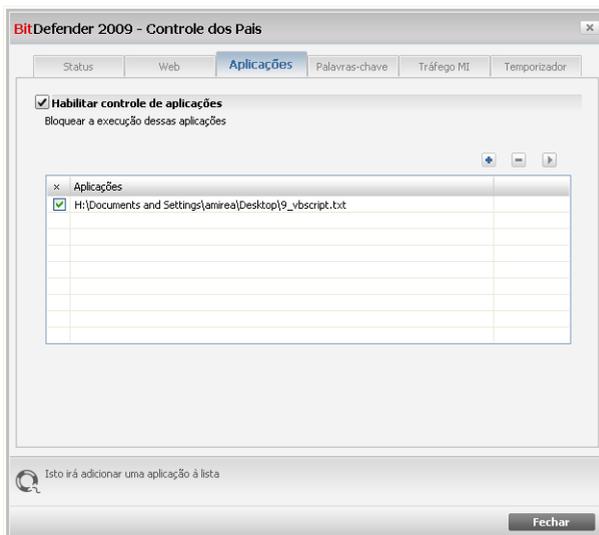
De forma a proteger as suas crianças, o BitDefender dá-lhe um lista negra de sites web com conteúdo inapropriado ou possivelmente perigoso. Para bloquear os sites que aparecem nesta lista seleccione **Usar a lista dos sites bloqueados fornecidos por BitDefender**.



18.3. Controle de Aplicações

O **Controle de aplicações** ajuda você a bloquear qualquer aplicação contra execução. Jogos, mídia e software de mensagens, assim como outras categorias de software e malware podem ser bloqueadas desta maneira. Aplicações bloqueadas desta forma também são bloqueadas contra modificação, e não podem ser copiadas ou movidas.

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



Controle de Aplicações

Para habilitar esta proteção selecione a caixa correspondente a **Habilitar Controle de Aplicações**.

As regras devem ser inseridas manualmente. Clique no botão **Adicionar...** para dar início ao assistente de configuração.

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



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

18.3.1. Assistente de Configuração

O assistente de configuração é um procedimento de um passo.

Passo 1/1 - Selecionar a aplicação a ser bloqueada



Selecione a aplicação a ser bloqueada

Clique em **Explorar**, seleccione a aplicação a ser bloqueada e clique em **Terminar**.

18.4. Filtragem Palavra-chave

A Filtragem por Palavra-chave ajuda-o a bloquear o acesso dos usuários a mensagens de e-mail, páginas web e mensagens instantâneas que contenham determinadas palavras. Ao usar a Filtragem por Palavra-chave, pode evitar que as crianças vejam palavras ou frases inapropriadas quando estão on-line.



Nota

A Filtragem por Palavra-chave das mensagens instantâneas só está disponível para o Yahoo Messenger e o Windows Live (MSN) Messenger.



Para configurar Filtragem por Palavra-chave para um determinado usuário, faça duplo clique no respectivo usuário e clique na barra **Palavras-chave**.

BitDefender 2009 - Controle dos Pais

Status Web Aplicações **Palavras-chave** Tráfego IM Temporizador

Activar Filtragem por Palavra-chave
Bloquear páginas web e mensagens de e-mail que contenham estas palavras.

Palavra	HTTP	POP3	IM	Igualar todas as pal...
test	Sim	Não	Não	Sim

Esta lista mostra todas as palavras-chave que são usadas para bloquear as páginas web e os e-mails que as contêm.

Fechar

Filtragem Palavra-chave

Marque a caixa **Activar Filtragem Palavra-chave** se pretende usar esta opção de controle.

Tem de adicionar regras para especificar as palavras-chave a serem bloqueadas. Para adicionar uma regra, clique no botão **Adicionar** e configure os parâmetros da regra na janela de configuração.

Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**. Para editar uma regra existente faça duplo clique na regra ou clique no botão **Editar** e faça as alterações desejadas na janela de configuração.

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

18.4.1. Janela de configuração

Quando adiciona ou edita regras, a janela de configuração irá aparecer.



BitDefender 2009 - Assistente de Palavras-chave

Adicionar nova palavra-chave

test

Selecionar opção

HTTP

POP3

Mensagens Instantâneas

Igualar todas as palavras

 Por favor adicione a palavra que deseja impedir que seja mostrada (mensagens de e-mail e páginas web completas serão bloqueadas).

 Adicione palavras a esta lista de forma a bloquear o acesso a páginas web ou a e-mails que as contenham

Concluir **Cancelar**

Inserir senha

Deve definir os seguintes parâmetros:

- **Palavra-chave** - insira no campo de edição a palavra ou frase que deseja bloquear.
- **Protocolo** - escolha o protocolo que o BitDefender deve analisar para a palavra especificada.

Opção	Descrição
POP3	As mensagens de e-mail que contenham a palavra-chave são bloqueadas.
HTTP	As páginas web que contenham a palavra-chave são bloqueadas.
Mensagens Instantâneas	As mensagens instantâneas que contenham a palavra-chave são bloqueadas.

Clique em **Terminar** para adicionar a regra.



18.5. Controle de Mensagens Instantâneas (IM)

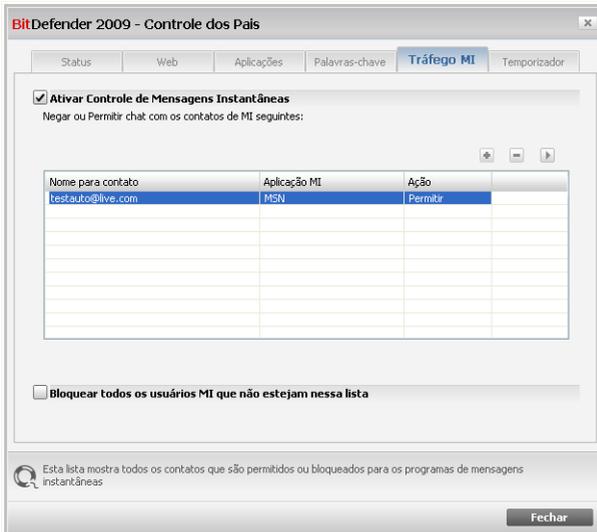
O Controle de Mensagens Instantâneas (IM) permite-lhe especificar os contactos IM com os quais a sua criança pode fazer chat.



Nota

O Controle de Mensagens Instantâneas (IM) só está disponível para o Yahoo Messenger e o Windows Live (MSN) Messenger.

Para configurar O Controle de Mensagens Instantâneas (IM) para um determinado usuário, faça duplo clique sobre o mesmo e clique na barra **Tráfego IM**.



Controle de Mensagens Instantâneas

Marque a caixa **Ativar Controle de Mensagens Instantâneas** se deseja utilizar esta opção de controle.

Tem de adicionar regras para especificar que contatos IM o usuário está ou não autorizado a fazer chat. Para adicionar uma regra, clique no botão **Adicionar** e configure os parâmetros da regra na janela de configuração.



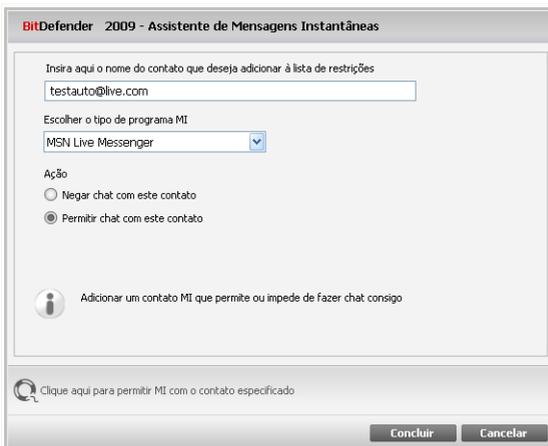
Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**. Para editar uma regra existente faça duplo clique na regra ou clique no botão **Editar** e faça as alterações desejadas na janela de configuração.

Se definiu todos os contatos IM que o usuário está permitido a fazer chat com, seleccione **Bloquear todos os contatos IM que não estão nesta lista**. Desta forma, somente os contatos explicitamente autorizados podem enviar mensagens instantâneas ao usuário.

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

18.5.1. Janela de configuração

Quando adiciona ou edita regras, a janela de configuração irá aparecer.



Adicionar contacto IM

Proceder da seguinte forma:

1. Inserir nome de usuário (ID) do contacto IM.
2. Escolher o program de IM com o qual o contacto se associa.
3. Seleccionar a acção da regra:
 - **Bloquear chat com este contacto**
 - **Permitir chat com este contacto**



4. Clique em **Terminar** para adicionar a regra.

18.6. Limitador de Horário Web

O **Limitador de Horário Web** ajuda você a permitir ou bloquear o acesso web para usuários e aplicações durante intervalos específicos de tempo.



Nota

O BitDefender irá executar atualizações de hora em hora não importando as configurações do **Limitador de Horário Web**.

O BitDefender efectuará a actualização de hora-a-hora independentemente da configuração do **Temporizador Web**.

The screenshot shows the 'Temporizador' (Timer) tab in the BitDefender 2009 - Controle dos Pais interface. The 'Habilitar Temporizador Web' checkbox is checked. Below it, a grid allows users to configure web access intervals for each day of the week (D, S, T, Q, Q, S, S). The grid shows intervals from 00:00 to 12:00. A legend indicates that white cells mean 'permitted' and grey cells mean 'blocked'. Buttons for 'Marcar Todos', 'Remover Todos', and 'Aplicar' are visible. A 'Fechar' button is at the bottom right.

Intervalos	D.	S.	T.	Q.	Q.	S.	S.
00:00 - 01:00							
01:00 - 02:00							
02:00 - 03:00							
03:00 - 04:00							
04:00 - 05:00							
05:00 - 06:00							
06:00 - 07:00							
07:00 - 08:00							
08:00 - 09:00							
09:00 - 10:00							
10:00 - 11:00							
11:00 - 12:00							

Limitador de Horário Web

Para habilitar esta proteção selecione a caixa correspondente a **Limitador de Horário Web**.

Selecione os intervalos de tempo em que todas as ligações à Internet estarão bloqueadas. Pode clicar em células individuais ou pode clicar e arrastar o ponteiro de forma a cobrir longos períodos de tempo. Também pode clicar em **Marcar Todas**



para seleccionar todas as células, implicitamente, bloqueando todo o acesso à web. Se clicar em **Desmarcar Todas**, as ligações de internet serão sempre permitidas.



Importante

As caixas em cinza representam intervalos em que todas as conexões com a Internet estão bloqueadas.

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



19. Controle Privacidade

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

19.1. Estado do Controle de Privacidade

Para configurar o Controle de Privacidade e ver informação quanto à sua atividade, vá para **Controle de Privacidade>Estado** no Modo Avançado.

BitDefender Internet Security 2009 - Trial

ESTADO: Existe 1 incidência pendente

REPARAR

Status

Identidade Registro Cookies Scripts

Controle de Privacidade está habilitado

Controle de Identidade está configurado

Nível de Proteção

Agressivo

Padrão

Permissivo

PADRÃO

- Identidade O controle está habilitado
- Registro O controle está desabilitado
- Cookies O controle está desabilitado
- Scripts O controle está desabilitado

Customizado Nível Padrão

Estadísticas do Controle de Privacidade

Info de Identidade bloqueada:	0
Registros bloqueados:	0
Cookies bloqueados:	0
Scripts bloqueados:	0

Para descobrir mais sobre cada opção apresentada na Interface do Usuário BitDefender, por favor mova o seu cursor sobre a janela. Um texto de ajuda relevante será apresentado nessa área.

Comprar/Renovar - Minha Conta - Registro - Ajuda - Suporte - Histórico

Estado do Controle de Privacidade

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



Importante

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

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

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

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

19.1.1. Configurar Nível de Protecção

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

Existem 3 níveis de protecção:

Nível de Protecção	Descrição
Permissivo	Apenas o Controle de Registo está ativo.
Por Defeito	O Controle de Registo e o Controle de Identidade estão ativos.
Agressivo	O Controle de Registo , o Controle de Identidade e o Controle de Script estão ativos.

Pode personalizar o nível de protecção clicando em **Nível Pessoal**. Na janela que lhe irá aparecer, escolha o controles de protecção que deseja ativar e clique em **OK**.

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



19.2. Controle de Identidade

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

Quer seja o seu e-mail o seu número de cartão de crédito, quando eles caem em mãos erradas essa informação poderá causar-lhe danos: poderá encontrar-se afogado em mensagens spam ou poderá ser surpreendido ao aceder à sua conta e verificar que está vazia.

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

Pode criar regras para proteger cada peça de informação que possa considerar pessoal ou confidencial, desde o seu número de telefone ou endereço de e-mail até à sua informação bancária. Suporte multi-usuário é fornecido de forma a que os usuários de diferentes contas do Windows possam configurar e usar as suas próprias regras de identidade. As regras que criou são aplicadas e podem ser acedidas apenas quando entrou com a sua conta no Windows.

Porquê usar o Controle de Identidade?

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

Supondo que tal aplicação funciona de forma a evitar a detecção antivírus, a mesma não pode enviar os dados roubados por e-mail, web ou mensagens instantâneas se tiver criado as regras de protecção de identidade adequadas.

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

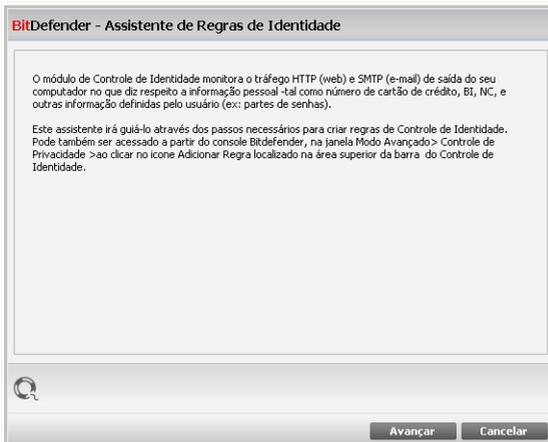


1. Selecione a caixa **Controle de Identidade**.
2. Criar regras para proteger a sua informação sensível. Para mais informação, por favor consulte o **“Criar Regras de Identidade”** (p. 215).
3. Se necessário, defina excepções específicas para as regras que criou. Para mais informação, por favor consulte o **“Definir Excepções”** (p. 218).

19.2.1. Criar Regras de Identidade

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

Passo 1/4 - Janela de Boas-vindas



Janela de Boas-Vindas

Clique em **Próximo**.



Passo 2/4 - Definir Tipo de Regra e Dados

BitDefender - Assistente de Regras de Identidade

Nome de regra

Tipo de regra

Dados da Regra

A informação pessoal é encriptada e não pode ser usada por mais ninguém que não você. Como medida de segurança adicional, insira apenas parte da informação que deseja proteger (ex: se deseja filtrar tráfego do seguinte endereço de e-mail: jonas@exemplo.com, deve inserir apenas "jonas").

Definir Tipo de Regra e Dados

Deve definir os seguintes parâmetros:

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



Nota

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

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

Clique em **Próximo**.



Passo 3/4 - Seleccionar Tráfego



Seleccionar Tráfego

Selecione o tráfego que quer que o BitDefender analise. As seguintes opções estão disponíveis:

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

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

Clique em **Próximo**.



Passo 4/4 - Descrever Regra

BitDefender - Assistente de Regras de Identidade

Descrição de regra

Insira uma descrição para esta regra. A descrição deverá ajudá-lo a si ou aos outros administradores a identificar facilmente que informação está a ser bloqueada.

Retornar Concluir Cancelar

Descrever Regra

Insira uma breve descrição da regra no campo de edição. Uma vez que os dados bloqueados (string de caracteres) não são mostrados em pleno texto quando se acede à regra, a descrição deverá ajudá-lo a identificá-la facilmente.

Clique em **Finalizar**. A regra aparecerá na tabela.

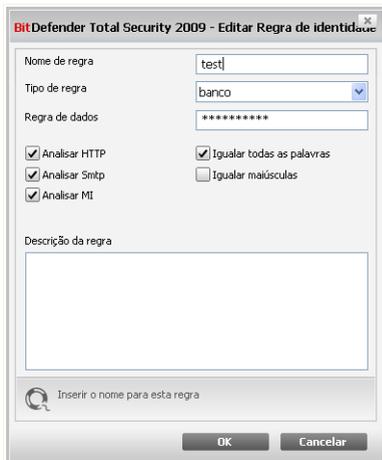
19.2.2. Definir Exceções

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

Para abrir a janela onde pode gerir as exceções, clique em **Exceções**.



Para editar uma regra, selecione-a e clique no botão **Editar** ou faça duplo-clique sobre ela. Uma nova janela irá aparecer.



Aqui pode mudar o nome, descrição e parâmetros da regra (tipo, dados e tráfego). Clique em **OK** para guardar as alterações.

Editar Regra

19.3. Controle de Registro

Uma parte muito importante do sistema operacional Windows é chamada de **Registro**. É aqui que o Windows mantém suas configurações, programas instalados, informações de usuário e informações do gênero.

O **Registro** é também usado para definir quais programas deverão ser iniciados automaticamente quando o Windows inicia. Vírus costumam usar isso para serem executados automaticamente quando o usuário reinicia seu computador.

O **Controle de Registro** fica de olho no Registro do Windows – Isso é útil também para detectar Trojans. Você será alertado sempre que um programa tentar modificar uma entrada de registro para ser executado na inicialização do Windows.



Alerta do Registro

Poderá ver o programa que está a tentar alterar o registo do Windows.

Se não reconhece o programa e lhe parecer suspeito, clique em **Bloquear** para evitar que ele modifique o registo do Windows. De outra forma, clique em **Permitir** para permitir a modificação.

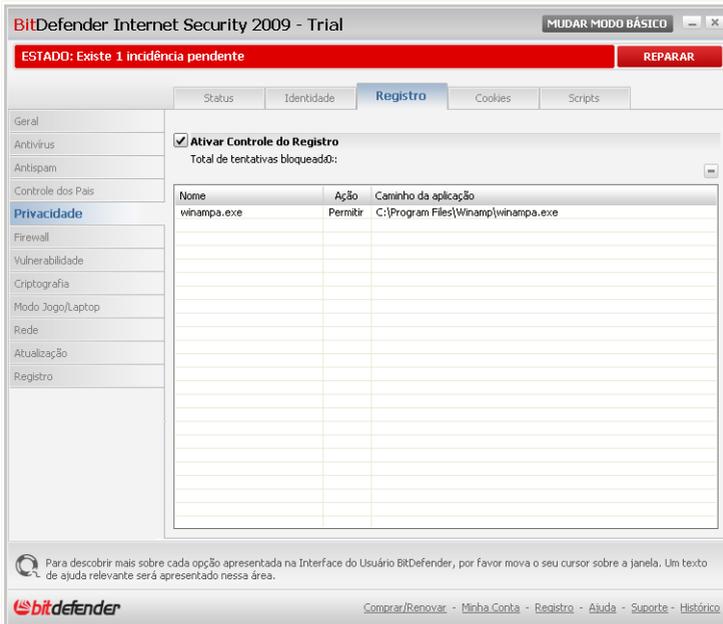
Baseado na sua resposta, a regra é criada e listada na tabela de regras. A mesma acção será aplicada sempre que este programa tentar modificar uma entrada no registo.



Nota

O BitDefender normalmente irá alertá-lo quando você instalar novos programas que precisam rodar após a próxima inicialização de seu computador. Na maioria dos casos, esses programas são legítimos e podem ser confiados.

Para configurar o Controle de Registro, clique em **Controle Privacidade>Registro** no Modo Avançado.



Controle de Registro

Pode ver as regras criadas até agora listadas na tabela.

Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**.

19.4. Controle de Cookie

Cookies são uma ocorrência muito comum na Internet. Eles são pequenos arquivos gravados em seu computador. Websites criam esses cookies para manter controle de informações específicas sobre você.

Cookies normalmente são usados para tornar sua vida mais fácil. Por exemplo, eles podem ajudar o site a lembrar de seu nome e preferências, para que você não tenha que inseri-los a cada visita.

Mas os cookies podem também ser usados para comprometer sua privacidade, vigiando seus padrões de navegação.



É aí que o **Controle de Cookie** ajuda. Quando ativado, o **Controle de Cookie** pedirá sua permissão sempre que um novo site tentar colocar um cookie:



Alerta de cookie

Você pode ver o nome do aplicativo que está tentando enviar o cookie.

Marque a caixa **Lembrar dessa resposta** e clique em **Sim** ou **Não** e uma regra será criada, aplicada e listada na tabela de regras. Você não será mais notificado quando se conectar a esse site.

Isso ajudará você a escolher quais sites tem ou não sua confiança.



Nota

Por causa do grande número de cookies usados hoje na Internet, o **Controle de Cookie** pode ser bem chato no início. No início, ele fará várias perguntas sobre sites tentando colocar cookies em seu computador. Conforme você adicionar seus sites comuns à lista de regras, surfar na Internet será tão fácil quanto antes.

Para configurar o Controle de Cookies, clique em **Controlo Privacidade>Cookie** no Modo Avançado.



BitDefender Internet Security 2009 - Trial MUDAR MODO BÁSICO

ESTADO: Existe 1 incidência pendente REPARAR

Status Identidade Registro **Cookies** Scripts

Ativar Controle de Cookies
Total Cookies bloqueados: 0

Domínio	Direção	Ação
www.bitdefender.com	Ambos	Permitir
download.bitdefender.com	Saída	Permitir
metrics.bitdefender.com	Saída	Permitir
ssl-hints.netflame.cc	Entrada	Permitir
en-us.feedds.mozilla.com	Saída	Permitir
newrss.bbc.co.uk	Saída	Permitir

A lista das cookies ativadas no seu web browser. Pode alterar esta lista ao clicar nos botões Adicionar, Remover ou Editar.

[Comprar/Renovar](#) - [Minha Conta](#) - [Registro](#) - [Ajuda](#) - [Suporte](#) - [Histórico](#)

Controle de Cookie

Pode ver as regras criadas até agora listadas na tabela.



Importante

A prioridade das regras é de baixo para cima, ou seja, a última regra tem a maior prioridade. Arraste & solte regras para mudar a prioridade.

Para apagar uma regra, apenas selecione-a e clique no botão **Apagar**. Para modificar os parâmetros da regra, faça duplo clique sobre a regra e faça as modificações desejadas na janela de configuração.

Para adicionar manualmente uma regra, clique no botão **Adicionar** e configure os parâmetros da regra na janela de configuração.

19.4.1. Janela de configuração

Quando edita ou adiciona manualmente uma regra, a janela de configuração irá aparecer.



BitDefender - Assistente Regras de Cookie

Digite domínio

Qualquer

Digite domínio

Selecionar ação

Permitir

Negar

Selecionar direção

Saída

Entrada

Ambos

Seleccione os sites e domínios de quem você deseja aceitar ou rejeitar cookies. Cookies são usados para traçar comportamento de navegação e outras informações. Note que alguns sites não funcionarão corretamente sem cookies.

Concluir **Cancelar**

Selecione endereço, ação e direção

Você pode configurar parâmetros:

- **Domínio** - digite o domínio em que você quer aplicar a regra.
- **Ação** - selecione a ação da regra.

Ação	Descrição
Permitir	Os cookies daquele domínio serão executados.
Negar	Os cookies daquele domínio não serão executados.

- **Direção** - selecione a direção do tráfego.

Tipo	Descrição
Saída	A regra será aplicada apenas para os cookies que forem devolvidos para o site conectado.
Entrada	A regra será aplicada apenas para os cookies que forem recebidos do site conectado.
Ambos	As regras valem para as duas direções.



Nota

Você pode aceitar cookies mas nunca devolvê-los definindo a ação como **Negar** e a direção como **Saída**.

Clique em **Finalizar**.

19.5. Controle de Scripts

Scripts e outros códigos tais como **Controles ActiveX** e **Java applets**, que são usados para criar páginas da web interativas, podem ter efeitos danosos. Elementos ActiveX, por exemplo, podem ganhar acesso total a seus dados e eles podem ler dados de seu computador, apagar informações, capturar senhas e interceptar mensagens enquanto você esta on-line. Você pode apenas aceitar conteúdo ativo de sites de sua total confiança.

O BitDefender deixa você escolher entre executar estes elementos ou bloquear a execução.

Com o **Controle de Scripts** você será responsável por quais websites você confia ou não. O BitDefender pedra sua permissão sempre que um site tentar ativar um script ou outro conteúdo ativo:



Alerta de script

Você pode ver o nome do recurso.

Marque a caixa **Lembrar dessa resposta** e clique em **Sim** ou **Não** e uma regra será criada, aplicada e listada na tabela de regras. Você não será mais notificado quando esse site tentar lhe enviar conteúdo ativo.

Para configurar o Controle de Script, clique em **Controle Privacidade>Script** no Modo Avançado.



BitDefender Internet Security 2009 - Trial

ESTADO: Existe 1 incidência pendente

MUDAR MODO BÁSICO

REPARAR

Status Identidade Registro Cookies **Scripts**

Ativar Controle de Script
Total de scripts bloqueadas: 0

Domínio	Ação
www.bitdefender.com	Permitir

A lista dos scripts ativados no seu web browser. Pode alterar esta lista ao clicar nos botões Adicionar, Remover ou Editar.

Comprar/Remover - Minha Conta - Registro - Ajuda - Suporte - Histórico

Controle de Scripts

Pode ver as regras criadas até agora listadas na tabela.



Importante

A prioridade das regras é de baixo para cima, ou seja, a última regra tem a maior prioridade. Arraste & solte regras para mudar a prioridade.

Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**. Para modificar os parâmetros da regra, faça duplo clique sobre a regra e faça as modificações desejadas na janela de configuração.

Para adicionar manualmente uma regra, clique no botão **Adicionar** e configure os parâmetros da regra na janela de configuração.

19.5.1. Janela de configuração

Quando edita ou adiciona manualmente uma regra, a janela de configuração irá aparecer.



BitDefender - Assistente de Regras Script

Digite domínio

Selecionar ação

Permitir

Negar

 Escolha o(s) domínio(s) específico(s) de quem você deseja permitir ou bloquear scripts. Normalmente, você deve usar esse assistente para especificar os domínios de quem você deseja permitir scripts. É recomendado que você bloqueie scripts de todos os domínios em que você não confia.



Selecione endereço e ação

Você pode configurar parâmetros:

- **Domínio** - digite o domínio em que você quer aplicar a regra.
- **Ação** - selecione a ação da regra.

Ação	Descrição
Permitir	Os scripts daquele domínio serão executados.
Negar	Os scripts daquele domínio não serão executados.

Clique em **Finalizar**.



20. Firewall

A Firewall protege o seu computador de tentativas de ligações internas e externas não-autorizadas. É bastante semelhante a um guarda que está à sua porta – irá manter um olhar atento na sua ligação à Internet e rastrear a quem permitir e a quem bloquear o acesso à mesma.



Nota

Um firewall é essencial se você estiver usando uma conexão banda-larga ou DSL.

Em Modo Stealth o seu computador fica “escondido” do software maligno e dos hackers. O módulo da firewall é capaz de detectar e proteger automaticamente o seu computador contra os scans de portas (conjunto de pacotes enviados para uma máquina de forma a encontrar "pontos de acesso", frequentemente como modo de preparação para um ataque).

20.1. Opções

Para configurar a protecção firewall, clique em **Firewall>Definições** no Modo Avançado.



Definições da Firewall

Aqui é onde pode ver se a Firewall BitDefender se encontra activada ou desactivada. Se deseja alterar o estado da firewall, limpe ou seleccione a caixa correspondente.



Importante

Para estar protegido contra ataques de Internet mantenha o **Firewall** habilitado.

Existem duas categorias de informação:

- **Configuração de Rede Breve.** Pode ver o nome do seu computador, o seu endereço IP e a sua gateway por defeito. Se tem mais do que um adaptador de rede (significando que está ligado a mais do que uma rede), verá o endereço IP e a gateway configurada para cada adaptador de rede.
- **Estatísticas.** Pode ver as várias estatísticas com respeito à actividade da firewall:
 - número de bytes enviados.



- número de bytes recebidos.
- número de scans de portas detectados e bloqueados pelo BitDefender. Os scans de portas são frequentemente usados pelos hackers para descobrir portas abertas no seu computador com o objectivo de as explorar.
- número de pacotes deixados cair.
- número de portas abertas.
- número de ligações de entrada activas.
- número de ligações de saída activas.

Para ver as ligações activas e as portas abertas, vá até à barra **Actividade**.

Ao fundo e ao lado desta secção pode ver as estatísticas do BitDefender com respeito ao tráfego de entrada e de saída. O gráfico mostra-lhe o volume de tráfego da Internet durante os últimos dois minutos.



Nota

O gráfico aparece mesmo que o **Firewall** esteja desabilitado.

20.1.1. Definir a Acção por Defeito

Por defeito o BitDefender permite automaticamente que todos os programas conhecidos da sua lista branca acedam aos serviços da rede e à Internet. Para todos os outros programas o BitDefender consulta-o através de uma janela de alerta para que decida a acção a tomar. A acção que determinar será aplicada cada vez que a respectiva aplicação solicite o acesso à rede/internet.

Arraste o marcador ao longo da escala para definir a acção a ser levada a cabo para as aplicações que solicitem acesso à rede/Internet. Estão disponíveis as seguintes acções por defeito:

Acção por Defeito	Descrição
Permitir Todos	Aplica as regras actuais e permite as tentativas de tráfego que não correspondem com nenhuma das regras actuais sem o consultar. Esta política é muito desaconselhada, mas poderá ser útil para administradores de redes e jogadores.
Permitir Programas Conhecidos	Aplica as regras actuais e permite todas as tentativas de ligação de saída dos programas que BitDefender



Acção por Defeito	Descrição
	<p>considera como legítimos (lista branca) sem o consultar. Para as restantes tentativas de ligação, Bitdefender solicitará a sua permissão.</p> <p>Programas da Lista Branca são as aplicações mais usadas e comuns a nível mundial. Incluem os mais conhecidos browsers de internet, audio&video players, programas de chat e filesharing, como também as aplicações de cliente servidor e do sistema operacional.</p>
Relatório	Aplica as regras actuais e consulta-o acerca das tentativas de tráfego que não correspondem com nenhuma das regras actuais.
Bloquear Todos	Aplica as regras actuais e bloqueia todas as tentativas de tráfego que não correspondem com nenhuma das regras actuais.

20.1.2. Configuração Avançada da Firewall

Clique em **Avançada** para configurar as definições avançadas da firewall.



Configuração Avançada da Firewall

As seguintes opções estão disponíveis:

- **Activar Suporte de Internet Connection Sharing (ICS)** - activa o suporte para Internet Connection Sharing (ICS).



Nota

Esta opção não ativa automaticamente o ICS no seu sistema, mas apenas permite este tipo de ligação em caso de a ativar no seu sistema operacional.

O Internet Connection Sharing (ICS) permite que elementos da sua rede de área local se liguem à Internet através do seu computador. Isto é útil quando beneficia de uma ligação à Internet especial/particular (ex:- ligação wireless) e a quer partilhar com outros membros da sua rede.

Partilhar a sua ligação à Internet com membros da sua rede de área local leva a um elevado consumo de recursos e pode envolver algum risco. Também lhe retira algumas portas (aquelas abertas pelos membros que estão a usar a sua ligação à Internet).

- **Monitorizar mudanças em arquivos de programas que igualam as regras da firewall** - Verifica cada tentativa de ligação à Internet das aplicações para ver se elas mudaram desde que a regra que controla o seu acesso foi criada. Se a aplicação foi alterada, um aviso de alerta surgirá para que permita ou bloqueie o acesso da aplicação à Internet.

Normalmente as aplicações são alteradas pelas actualizações. Mas, existe um risco que elas sejam alteradas por aplicações malware, com o propósito de infectar o seu computador e outros computadores na rede.



Nota

Recomendamos que mantenha esta opção seleccionada e permita acesso apenas àquelas aplicações que espera que tenham mudado após a regra que controla o seu acesso ter sido criada.

Aplicações assinadas são suposta serem fiáveis e de um alto nível de segurança. Pode escolher **Ignorar mudanças em processos assinados** de forma a permitir que aplicações assinadas que se alteraram se liguem à Internet sem ser alertado acerca deste evento.

- **Activar notificações wireless** - se estiver ligado a uma rede wireless, mostra janelas informativas com respeito aos eventos de rede (por exemplo, quando um novo computador foi ligado à rede).
- **Bloquear scans de portas** - detecta e bloqueia todas as tentativas de descobrir que portas se encontram abertas.

Os scans de portas são frequentemente usados pelos hackers para descobrir que portas se encontram abertas no seu computador. Então eles poderão entrar no seu computador se descobrirem uma porta menos segura ou vulnerável.



- **Regras automáticas estritas** - cria regras estritas usando a janela de alerta da firewall. Com esta opção seleccionada, o BitDefender consulta-lo-á para tomar uma acção e criar regras para cada diferente processo que abre a aplicação que está a solicitar o acesso à rede ou à Internet.
- **Sistema de detecção de Intrusão (IDS)** - activa a monitorização heurística das aplicações que estão a tentar aceder aos serviços de rede ou à Internet.

20.2. Rede

Para configurar a protecção firewall, clique em **Firewall>Rede** no Modo Avançado.

Configuração de Rede:

Adaptador	Nível de Confiança	Modo Invi...	Gené...	Endereços	Gateways
Local Area Connection	Confiável Lo...	Remoto	Não	10.10.17.51/16	10.10.0.1

Zonas:

Adptador / Zonas	Confiança
Local Area Connection	
10.10.10.37	Negar

Para descobrir mais sobre cada opção apresentada na Interface do Utilizador BitDefender, por favor mova o seu cursor sobre a janela. Um texto de ajuda relevante será apresentado nessa área.

bitdefender Comprar/Renovar - Minha Conta - Registo - Ajuda - Suporte - Histórico

Rede

As colunas na tabela de **Configuração de Rede** dão-lhe informação detalhada da rede à qual se encontra ligado:



- **Adaptador** - o adaptador de rede que o seu computador usa para se ligar à rede ou à Internet.
- **Tipo** - o nível de confiança atribuído ao adaptador de rede. Dependendo da configuração do dispositivo de rede, o BitDefender pode automaticamente atribuir ao dispositivo um nível de confiança ou solicitar-lhe mais informação.
- **Stealth** - para não ser detectado por outros computadores.
- **Prima Genérico** - se regras genéricas são aplicadas a esta ligação.
- **Endereços** - o endereço IP configurado no dispositivo.
- **Gateways** - O endereço IP que o seu computador usa para se ligar à Internet.

20.2.1. Alterar o Nível de Confiança

BitDefender atribui a cada dispositivo de rede um nível de confiança. O nível de confiança atribuído ao adaptador indica quão fiável a respectiva rede é.

Baseado no nível de confiança, determinadas regras são criadas para o adaptador independentemente de como os processo do sistema e do BitDefender acedem à rede ou à Internet.

Pode ver o nível de confiança configurado para cada adaptador na tabela de **Configuração de Rede** debaixo da coluna **Tipo** . Para alterar o nível de confiança, clique na seta da coluna **Tipo** e escolha o nível desejado.

Nível de Confiança	Descrição
Confiança Total	desactiva a firewall para o respectivo dispositivo.
Local Fiável	Permite o tráfego entre o seu computador e os computadores na rede local.
Segura	Permite partilhar recursos entre computadores numa rede local. Este nível é automaticamente definido para redes locais (casa ou escritório).
Insegura	Impede que os computadores de rede ou da Internet se liguem ao seu. Este nível é automaticamente definido para redes públicas (se recebe um endereço IP de um ISP (Internet Service Provider)).
Bloquear Local	Bloqueia todo o tráfego entre o seu computador e os computadores na rede local, enquanto mantém o acesso à



Nível de Confiança	Descrição
	Internet. Este nível de confiança é automaticamente definido para redes wireless inseguras (abertas).
Bloqueado	Bloqueia completamente o tráfego de rede e de Internet através do respectivo adaptador.

20.2.2. Configurar o Modo Stealth

O Modo Stealth torna o seu computador invisível na rede ou na internet ao software malicioso e aos hackers. Para configurar o Modo Stealth, clique na seta ▼ da coluna **Stealth** e seleccione a opção desejada.

Opção Stealth	Descrição
Ligado.	O Modo Stealth está ligado. O seu computador deixa de ser visível a partir da rede local e da Internet.
Desligado	O Modo Stealth está desligado. Qualquer pessoa da rede local ou da Internet pode fazer ping e detectar o seu computador.
Remoto	O seu computador não pode ser detectado da Internet. As redes locais podem fazer ping e detectar o seu computador.

20.2.3. Configurar Definições Gerais

Se o endereço IP de um adaptador é alterado, o BitDefender modifica o nível de confiança de acordo com a alteração. Se deseja manter o mesmo nível de confiança, clique na seta ▼ da coluna **Genérico** e seleccione **Sim**.

20.2.4. Zonas de Rede

Pode adicionar computadores autorizados ou bloqueados a uma determinado adaptador.

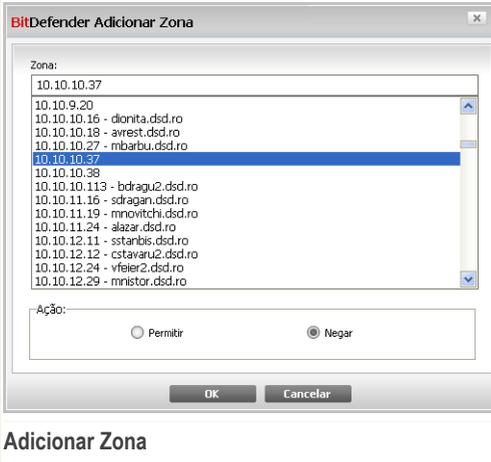
Uma zona fiável é um computador em que confia totalmente. Todo o tráfego entre o seu computador e o computador fiável é permitido. Para partilhar recursos com determinados computadores numa rede wireless insegura, adicione-os como computadores autorizados.



Uma zona bloqueada é um computador que você não quer de forma alguma que comunique com o seu.

A tabela **Zonas** mostra as actuais zonas de rede por dispositivo.

Para adicionar uma zona, clique no botão  **Adicionar** .



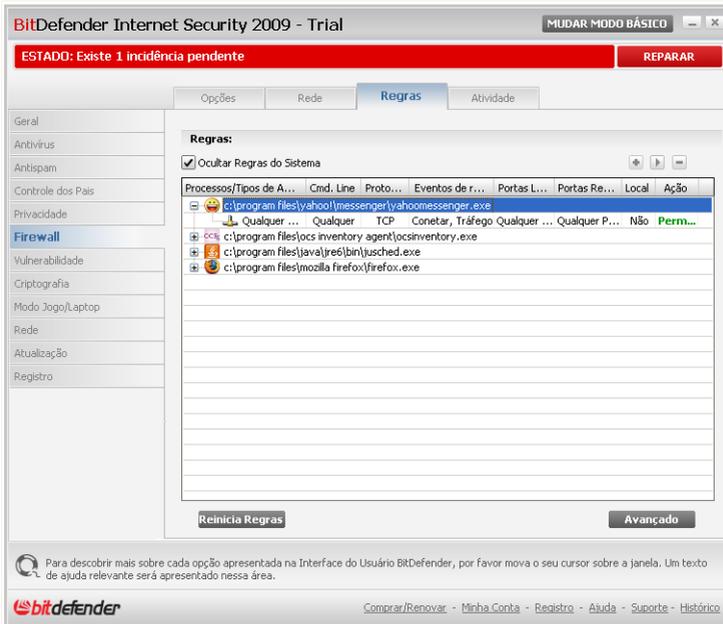
Adicionar Zona

Proceder da seguinte forma:

1. Selecciono o endereço IP do computador que pretende adicionar.
2. Seleccionar a acção:
 - **Permitir** - para autorizar o tráfego entre o seu computador e o computador seleccionado.
 - **Negar** - para bloquear o tráfego entre o seu computador e o computador seleccionado.
3. Clique em **OK**.

20.3. Regras

Para gerir as regras da firewall que controlam o acesso das aplicações aos recursos de rede e à Internet, clique em **Firewall>Regras** no Modo Avançado.



Regras da Firewall

Pode ver as aplicações (processos) para os quais as regras de firewall foram criadas. Limpe a caixa de selecção correspondente a **Ocultar processos de sistema** para poder ver as regras que dizem respeito aos processos de sistema e do BitDefender.

Para ver as regras criadas para uma aplicação específica, clique na caixa + ao pé da respectiva aplicação. Pode aprender info detalhada sobre cada regra, como indicada na tabela de colunas:

- **Processo/Tipos Adaptador** - o processo e os tipos de adaptador de rede aos quais a regra se aplica. As regras são automaticamente criadas para filtrar o acesso à rede ou à Internet através de qualquer adaptador. Pode criar manualmente as regras ou editar as regras existentes para filtrar o acesso à rede ou à Internet de uma aplicação através de um determinado adaptador (por exemplo, um adaptador de rede wireless).
- **Linha de comando** - o comando (**cmd**) usado para iniciar o processo no interface de linha de comando do Windows.



- **Protocolo** - o protocolo IP aos quais as regras se aplicam. Pode ver um dos seguintes:

Protocolo	Descrição
Todas	Inclui todos os protocolos IP.
TCP	Transmission Control Protocol - TCP possibilita dois computadores a estabelecer uma conexão e trocar dados. O TCP garante a entrega de dados e também que pacotes serão entregues na mesma ordem que foram enviados.
UDP	User Datagram Protocol - UDP é um transporte baseado em IP concebido para alta performance. Jogos e outros aplicativos baseados em vídeo usam UDP.
Um número	Representa um protocolo IP específico (outro que não TCP e UDP). Pode encontrar a lista completa de números IP atribuídos em www.iana.org/assignments/protocol-numbers .

- **Eventos de Rede** - os eventos de rede aos quais a regra se aplica. Os seguintes eventos podem ser tidos em consideração:

Evento	Descrição
Ligar	Intercâmbio preliminar de mensagens standard usado pelos protocolos orientados para a ligação (tais como TCP) para estabelecer a mesma. Com protocolos orientados para a ligação, o tráfego de dados entre dois computadores ocorre apenas após a ligação ser estabelecida.
Tráfego	Fluxo de dados entre dois computadores.
Escutar	Estado em que uma aplicação monitoriza a rede à espera de estabelecer uma ligação ou de receber informação de uma aplicação peer.

- **Portas Locais** - as portas no seu computador em que a regra se aplica.
- **Portas Remotas** - as portas nos computadores remotos em que a regra se aplica.
- **Local** - se a regra só se aplica a computadores na rede local.
- **Acção** - se à aplicação será permitido ou negado o acesso à rede ou Internet nas circunstâncias determinadas.



20.3.1. Adicionar Regras Automaticamente

Com a **Firewall** activada, o BitDefender pedirá a sua permissão sempre que uma tentativa de ligação à Internet seja feita:



Alerta da Firewall

Pode ver o seguinte: a aplicação que se está a tentar ligar à internet, o caminho do arquivo da aplicação, o destino, o protocolo usado e a **porta** na qual a aplicação se está a tentar ligar.

Clique **Permitir** para permitir o tráfego (entrada e saída) gerado por esta aplicação a partir do local host para qualquer destino, no respectivo protocolo IP protocol e em todas as portas. Se clicar em **Bloquear**, será negado completamente o acesso à Internet por parte da aplicação no respectivo protocolo IP.

Baseado na sua resposta, uma regra será criada, aplicada e listada na tabela. A próxima vez que a aplicação se tentar ligar, esta regra será aplicada por defeito.



Importante

Permitir tentativas de ligação de entrada apenas de IP's ou domínios em que confia totalmente.

20.3.2. Apagar Regras

Para apagar uma regra, seleccione-a e clique no botão **Apagar Regra**. Pode seleccionar e apagar várias regras de uma só vez.

Para eliminar todas as regras criadas para uma especifica aplicação, seleccione-a da lista e clique no botão **Remover regra**.

20.3.3. Criar e Modificar Regras

Criar novas regras manualmente e modificar as regras existentes consiste em configurar os parâmetros da regra na janela de configuração.

Criar regras. Para criar regras manualmente, siga estes passos:

1. Clique no botão **Adicionar Regra** . A janela de configuração irá aparecer.



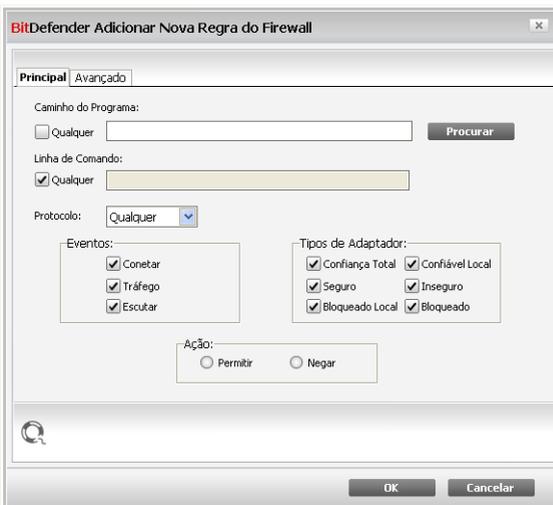
2. Configure os parâmetros principais e avançados quanto seja necessário.
3. Clique em **OK** para adicionar a nova regra.

Modificar regras. Para modificar uma regra existente, siga os seguintes passos:

1. Clique no botão **Editar Regra** ou faça duplo-clique sobre ela. A janela de configuração irá aparecer.
2. Configure os parâmetros principais e avançados quanto seja necessário.
3. Clique em **OK** para salvar as alterações.

Configurar os Parâmetros Principais

A barra **Principal** da janela de configuração permite configurar os principais parâmetros da regra.



Parâmetros Principais

Pode configurar os seguintes parâmetros:

- **Caminho do Programa.** Clique em **Explorar** para seleccionar a aplicação à qual a regra se aplica. Se deseja que a regra se aplique a todas as aplicações, apenas seleccione **Todas**.



- **Linha de comando.** Se deseja que a regra se aplique apenas quando a aplicação é aberta com um comando específico na linha de comandos do Windows, limpe a caixa **Todas** e insira o respectivo comando no campo de edição.
- **Protocolo.** Seleccione do menu o protocolo IP ao qual a regra se aplica.
 - Se deseja que a regra se aplique a todos os protocolos, seleccione **Todos**.
 - Se deseja que a regra se aplique a um determinado protocolo, seleccione **Outro**. Um campo de edição irá aparecer. Insira no campo de edição o número atribuído ao protocolo que deseja filtrar.



Nota

Os números dos protocolos IP são atribuídos pelo Internet Assigned Numbers Authority (IANA). Pode encontrar a lista completa de números IP atribuídos em www.iana.org/assignments/protocol-numbers.

- **Eventos.** Dependendo do protocolo seleccionado, escolha os eventos de rede aos quais a regra se aplica. Os seguintes eventos podem ser tidos em consideração:

<i>Evento</i>	<i>Descrição</i>
Ligar	Intercâmbio preliminar de mensagens standard usado pelos protocolos orientados para a ligação (tais como TCP) para estabelecer a mesma. Com protocolos orientados para a ligação, o tráfego de dados entre dois computadores ocorre apenas após a ligação ser estabelecida.
Tráfego	Fluxo de dados entre dois computadores.
Escutar	Estado em que uma aplicação monitoriza a rede à espera de estabelecer uma ligação ou de receber informação de uma aplicação peer.

- **Nível de Confiança.** Seleccione os níveis de confiança aos quais a regra se aplica.
- **Ação.** Seleccione uma das seguintes acções disponíveis:

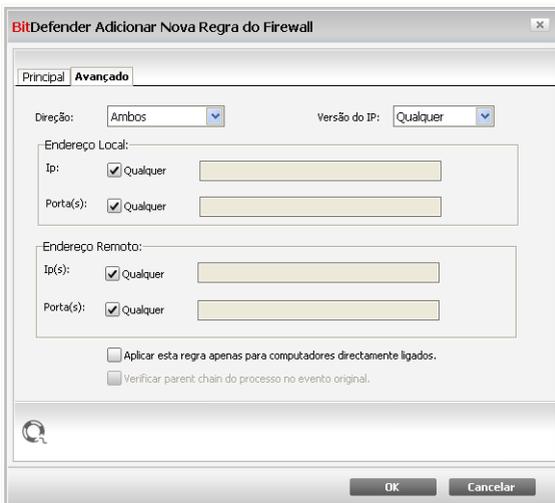
<i>Ação</i>	<i>Descrição</i>
Permitir	À aplicação especificada será permitido o acesso à rede / Internet nas circunstâncias determinadas.



Ação	Descrição
Negar	À aplicação especificada será negado o acesso à rede / Internet nas circunstâncias determinadas.

Configurar Parâmetros Avançados

A barra **Avançada** da janela de configuração permite-lhe configurar parâmetros avançados da regra.



Parâmetros Avançados

Pode configurar os seguintes parâmetros avançados:

- **Direcção.** Seleccione do menu a direcção do tráfego ao qual a regra se aplica.

Direcção	Descrição
Saída	As regras valem apenas para tráfego de saída.
Entrada	As regras valem apenas entrada.
Ambos	As regras valem para as duas direcções.



- **versão IP.** Seleccione do menu a versão do IP (IPv4, IPv6 ou qualquer) ao qual a regra se aplica.
- **Endereço Local.** Especifique o endereço IP local e a porta aos quais a regra se aplica da seguinte forma:
 - Se tem mais de um adaptador de rede, pode limpar a caixa **Todos** e inserir um endereço IP específico.
 - Se escolheu TCP ou UDP como protocolo pode definir uma porta específica ou um range entre 0 e 65535. Se deseja que a regra se aplique a todas as portas seleccione **Todas**.
- **Endereço Remoto.** Especifique o endereço IP remoto e a porta aos quais a regra se aplica da seguinte forma:
 - Para filtrar o tráfego entre o seu computador e um determinado computador, limpe a caixa **Todos** e insira o endereço IP do outro computador.
 - Se escolheu TCP ou UDP como protocolo pode definir uma porta específica ou um range entre 0 e 65535. Se deseja que a regra se aplique a todas as portas seleccione **Todas**.
- **Aplicar esta regra apenas a computadores ligados directamente.** Seleccione esta opção quando deseja que a regra se aplique apenas às tentativas de tráfego locais.
- **Verificar o processo parent chain pelo evento original.** Apenas pode alterar este parâmetro se tiver seleccionado **Regras estritamente automáticas** (vá para a barra **Definições** e clique **Configuração Avançada**). Regras estritas significa que o BitDefender consulta-o para que tome uma acção quando a aplicação requer acesso à rede/Internet de cada vez que o processo parent é diferente.

20.3.4. Gestão Avançada de Regras

Se necessita de controle avançado sobre as regras da firewall, clique em **Avançadas**. Uma nova janela irá aparecer.



BitDefender Editar Regras Avançadas do Firewall

Filtro ligado: Qualquer Adaptador

Ind....	Aplicação	Cmd. Line	Verifica...	Adaptador	Prob...	Endereço Local	Endereço Remoto	Versão...	Local	Direção	Eventos de r...	Ação
1	svchost.exe	Qualquer	Não	Qualquer A...	UDP	Qualquer IP : Client...	Qualquer IP : Serv...	Qualquer	Não	Ambos	All	Permitir
2	svchost.exe	Qualquer	Não	Qualquer A...	UDP	Qualquer IP : Servid...	Qualquer IP : Client...	Qualquer	Sim	Ambos	All	Permitir
3	svchost.exe	Qualquer	Não	Qualquer A...	UDP	Qualquer IP : 1024...	Qualquer IP : DNS	Qualquer	Não	Ambos	All	Permitir
4	svchost.exe	Qualquer	Não	Qualquer A...	TCP	Qualquer IP : 1024...	Qualquer IP : DNS	Qualquer	Não	Ambos	Conetar, Tráf...	Permitir
5	Qualquer	Qualquer	Não	Confiança T...	Qualquer	Qualquer IP : Qualq...	Qualquer IP : Qualq...	Qualquer	Não	Ambos	All	Permitir
6	Qualquer	Qualquer	Não	Confiável ...	Qualquer	Qualquer IP : Qualq...	Qualquer IP : Qualq...	Qualquer	Sim	Ambos	All	Permitir
7	Qualquer	Qualquer	Não	Bloqueado ...	Qualquer	Qualquer IP : Qualq...	Qualquer IP : Qualq...	Qualquer	Sim	Ambos	All	Negar
8	Qualquer	Qualquer	Não	Bloqueado	Qualquer	Qualquer IP : Qualq...	Qualquer IP : Qualq...	Qualquer	Não	Ambos	All	Negar
9	Qualquer	Qualquer	Não	Qualquer A...	IGMP	Qualquer IP : Qualq...	Qualquer IP : Qualq...	Qualquer	Não	Ambos	Tráfego	Permitir
10	Qualquer	Qualquer	Não	Qualquer A...	GRE	Qualquer IP : Qualq...	Qualquer IP : Qualq...	Qualquer	Não	Ambos	Tráfego	Permitir
11	Qualquer	Qualquer	Não	Qualquer A...	AH	Qualquer IP : Qualq...	Qualquer IP : Qualq...	Qualquer	Não	Ambos	Tráfego	Permitir
12	Qualquer	Qualquer	Não	Qualquer A...	ESP	Qualquer IP : Qualq...	Qualquer IP : Qualq...	Qualquer	Não	Ambos	Tráfego	Permitir
13	Qualquer	Qualquer	Não	Qualquer A...	ICMP	Qualquer IP : Qualq...	Qualquer IP : Qualq...	Qualquer	Não	Ambos	Tráfego	Permitir
14	Qualquer	Qualquer	Não	Qualquer A...	ICMP6	Qualquer IP : Qualq...	Qualquer IP : Qualq...	Qualquer	Não	Ambos	Tráfego	Permitir
15	Qualquer	Qualquer	Não	Qualquer A...	RRP	Qualquer IP : Qualq...	Qualquer IP : Qualq...	Qualquer	Não	Ambos	Tráfego	Permitir
16	svchost.exe	Qualquer	Não	Qualquer A...	UDP	Qualquer IP : DNS	Qualquer IP : 1024...	Qualquer	Sim	Ambos	All	Permitir
17	svchost.exe	Qualquer	Não	Qualquer A...	TCP	Qualquer IP : DNS	Qualquer IP : 1024...	Qualquer	Sim	Ambos	Tráfego, Escutar	Permitir
18	svchost.exe	Qualquer	Não	Qualquer A...	TCP	Qualquer IP : 1024...	Qualquer IP : RPC	Qualquer	Sim	Ambos	Conetar, Tráf...	Permitir
19	svchost.exe	Qualquer	Não	Qualquer A...	TCP	Qualquer IP : Qualq...	Qualquer IP : HTTP...	Qualquer	Não	Ambos	Conetar, Tráf...	Permitir
20	svchost.exe	Qualquer	Não	Qualquer A...	UDP	Qualquer IP : NTP...	Qualquer IP : NTP	Qualquer	Não	Ambos	All	Permitir
21	svchost.exe	Qualquer	Não	Seguro	TCP	Qualquer IP : RPC	Qualquer IP : Qualq...	Qualquer	Sim	Ambos	Tráfego, Escutar	Permitir
22	svchost.exe	Qualquer	Não	Seguro	UDP	Qualquer IP : 1900...	Qualquer IP : Qualq...	Qualquer	Sim	Ambos	All	Permitir
23	svchost.exe	Qualquer	Não	Seguro	TCP	Qualquer IP : 2177...	Qualquer IP : Qualq...	Qualquer	Sim	Ambos	All	Permitir
24	svchost.exe	Qualquer	Não	Qualquer A...	TCP	Qualquer IP : RDP	Qualquer IP : 1024...	Qualquer	Não	Ambos	Tráfego, Escutar	Permitir
25	svchost.exe	Qualquer	Não	Qualquer A...	Qualquer	Qualquer IP : Qualq...	Qualquer IP : Qualq...	Qualquer	Não	Ambos	All	Negar
26	System	Qualquer	Não	Qualquer A...	UDP	Qualquer IP : NetBI...	Qualquer IP : NetBI...	Qualquer	Sim	Ambos	All	Permitir
27	System	Qualquer	Não	Qualquer A...	TCP	Qualquer IP : Qualq...	Qualquer IP : NetBI...	Qualquer	Sim	Ambos	Conetar, Tráf...	Permitir
28	System	Qualquer	Não	Qualquer A...	UDP	Qualquer IP : L2TP...	Qualquer IP : 1024...	Qualquer	Sim	Ambos	All	Permitir
29	System	Qualquer	Não	Qualquer A...	TCP	Qualquer IP : PPTP	Qualquer IP : 1024...	Qualquer	Não	Ambos	Tráfego, Escutar	Permitir

Fechar

Gestão Avançada de Regras

Pode ver as regras da firewall listadas pela ordem em que são verificadas. A tabela de colunas dá-lhe uma informação completa sobre cada regra.



Nota

Quando uma tentativa de ligação é feita (seja de entrada ou saída), o BitDefender aplica a acção da primeira regra que corresponda a essa respectiva ligação. Logo, a ordem pela qual as regras são verificadas é muito importante.

Para apagar uma regra, seleccione-a e clique no botão **Apagar Regra**.

Para editar uma regra, seleccione-a e clique no botão **Editar Regra** ou faça duplo-clique sobre ela.

Pode aumentar ou diminuir a prioridade de uma regra. Clique no botão **Subir na Lista** para aumentar um nível a prioridade da regra seleccionada, ou clique no botão **Descer na Lista** para diminuir um nível a prioridade da regra seleccionada. Para atribuir a máxima prioridade a uma regra, clique no botão **Subir Topo**. Para atribuir a uma regra a mínima prioridade, clique no botão **Descer Fundo**.

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



20.4. Controle de Conexão

Para monitorizar a rede actual / actividade Internet (em TCP e UDP) por aplicação e abrir o log da Firewall BitDefender, clique em **Firewall>Actividade** no Modo Avançado.

Nome do Processo	PID/P...	Saída	Saída / s	Entrada	In / s	Idade
System	4	3.0 KB	0.0 B/s	296.1 KB	214.0 B/s	31m 47s
svchost.exe -k netsvc...	1652	2.0 KB	0.0 B/s	1.2 KB	0.0 B/s	31m 39s
svchost.exe -k locale...	200	0.0 B	0.0 B/s	10.7 KB	0.0 B/s	31m 36s
rapimg.exe -embedding	1844	0.0 B	0.0 B/s	0.0 B	0.0 B/s	31m 5s
firefox.exe	716	134.6 KB	0.0 B/s	125.6 KB	0.0 B/s	19m 6s
127.0.0.1:1162 =...	TCP	0.0 B	0.0 B/s	213.0 B	0.0 B/s	19m 1s
127.0.0.1:1160 =...	TCP	0.0 B	0.0 B/s	873.0 B	0.0 B/s	19m 5s
lsass.exe	1232	9.0 KB	0.0 B/s	35.1 KB	0.0 B/s	31m 41s
svchost.exe -k dcomla...	1412	0.0 B	0.0 B/s	0.0 B	0.0 B/s	31m 40s
yserv.exe /service	3028	1.1 KB	0.0 B/s	718.0 B	0.0 B/s	21m 49s
svchost.exe -k rpcss	1500	0.0 B	0.0 B/s	0.0 B	0.0 B/s	31m 39s

Controle de Conexão

Pode ver todo o tráfego por aplicação. Para cada aplicação, pode ver as ligações e as portas abertas, como também as estatísticas com respeito à velocidade de tráfego de saída & entrada e o montante total de dados enviados / recebidos.

Se deseja ver também os processos inactivos, limpe a caixa **Ocultar processos inactivos**.

O significado dos ícones é o seguinte:

- Indica uma ligação aberta no seu computador.
- Indica uma porta aberta no seu computador.



A janela apresenta em tempo-real a actividade da actual rede / Internet. À medida que as ligações e portas são fechadas, pode ver que as estatísticas correspondentes são diminuídas e que, eventualmente, desaparecerão. A mesma coisa acontece a todas as estatísticas correspondentes a uma aplicação que gera tráfego ou que tem portas abertas que você fecha.

Para obter uma lista mais completa de eventos com respeito ao uso do módulo da Firewall (ativar/desativar a firewall, bloquear tráfego, modificar configurações) ou gerado pelas actividades detectadas por ela (scan de portas, bloqueio de tentativas de ligação ou de tráfego de acordo com as regras) consulte o arquivo de relatório da Firewall do BitDefender que pode ser visualizado clicando em **Mostrar Relatório**. O arquivo está localizado na pasta de Arquivos Comuns do usuário atual do Windows, no caminho: `...BitDefender\BitDefender Firewall\bdfirewall.txt`.

Se deseja que o relatório contenha mais informação, seleccione **Aumentar verbosidade do relatório**.



21. Encriptação

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

21.1. Encriptação de Mensagens Instantâneas (IM)

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

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



Importante

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

Para configurar a encriptação de Mensagens Instantâneas, clique em **Encriptação>Encriptação IM** no Modo Avançado.



Nota

Pode configurar facilmente a cifragem das mensagens instantâneas usando a barra de ferramentas a partir da janela de chat. Para mais informação, por favor consulte a seção "*Integração com Messenger*" (p. 51).



Encriptação MI Cofre

A Encriptação MI está ativada.

- A Encriptação Yahoo Messenger Encryption está ativada.
- A Encriptação Windows Live (MSN) Messenger está ativada.

Exclusões de Encriptação

ID Usuário	Programa MI
yahoo_id	Yahoo Messenger

Ligações Atuais

ID Usuário	Programa MI	Estado da Encriptação

Esta é a lista de IDs com os quais você deseja fazer chat sem encriptação mesmo quando esta está ativada.

bitdefender Comprar/Renovar - Minha Conta - Registro - Ajuda - Suporte - Histórico

Encriptação de Mensagens Instantâneas

Por defeito, a Encriptação de Mensagens Instantâneas está activada para o Yahoo Messenger e o Windows Live (MSN) Messenger. Pode escolher desactivar a encriptação de Mensagens Instantâneas para apenas uma aplicação de chat ou para todas.

São mostradas duas tabelas:

- **Exclusões da Encriptação** - lista os IDs dos usuários e o programa de IM associado para os quais a encriptação está desativada. Para remover um contacto da lista, seleccione-o e clique no botão **Remover**.
- **Ligações Atuais** - lista as atuais ligações de mensagens (IDs dos usuários e o programa de IM associado) e se devem ou não ser encriptadas. Uma ligação poderá não ser encriptada pelas seguintes razões:
 - Desactivou explicitamente a encriptação para o respectivo contacto.

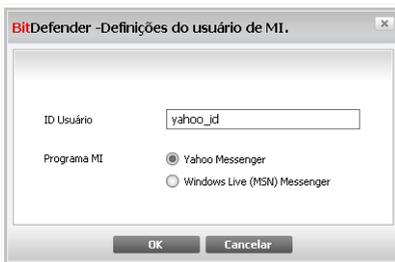


- O seu contacto não tem instalado uma versão do BitDefender que suporte a encriptação IM.

21.1.1. Desativar a Encriptação para usuários Específicos

Para desativar a encriptação para um determinado usuário, siga estes passos:

1. Clique no botão **Adicionar** para abrir a janela de configuração.



Adicionar Contactos

2. Insira no campo de edição o ID do usuário do seu contacto.
3. Seleccione a aplicação de mensagens instantâneas associada ao contacto.
4. Clique em **OK**.

21.2. Cofre de arquivos

O Cofre de arquivos BitDefender permite-lhe criar drives lógicas encriptadas, e protegidas por senha (cofres) no seu computador onde pode armazenar em segurança os seus documentos confidenciais e sensíveis. Os dados armazenados nos cofres apenas podem ser acessados pelos usuários que sabem a senha.

A senha permite-lhe abrir, armazenar dados no cofre e fechá-lo ao mesmo tempo que o mantém seguro. Quando um cofre é aberto, pode adicionar-lhe arquivos, aceder aos que lá estão ou alterá-los.

Fisicamente, o cofre é um arquivo armazenado no seu disco rígido local com a extensão `.bvd`. Apesar dos arquivos físicos que representam as drives de cofre poderem ser acessados a partir de um sistema operacional diferente (tal como Linux), a informação armazenada não pode ser lida por estar encriptada.



Para gerir os cofres no seu computador, clique em **Encriptação>Cofre arquivos** no Modo Avançado.

BitDefender Internet Security 2009 - Trial

ESTADO: Existe 1 incidência pendente

MUDAR MODO BÁSICO

REPARAR

Encriptação MI **Cofre**

Cofre de Arquivos está ativado

Cofres neste computador

Cofre	Status	Letra do drive	Caminho completo

Conteúdo do cofre

Caminho completo	Tipo de Arquivo

Para descobrir mais sobre cada opção apresentada na Interface do Usuário BitDefender, por favor mova o seu cursor sobre a janela. Um texto de ajuda relevante será apresentado nessa área.

Comprar/Renovar - Minha Conta - Registo - Ajuda - Suporte - Histórico

Cofre de arquivos

Para desativar Cofre de arquivos, limpe a caixa **Cofre de arquivos ativado** e clique em **Sim** para confirmar. Se desativar o Cofre de arquivos, todos os cofres de arquivos serão fechados e não será mais capaz de aceder aos arquivos que eles contêm.

A tabela no topo mostra os cofres de arquivos no seu computador. Pode ver o nome, o estado (aberto / fechado), a letra da drive e o caminho completo para o cofre. A tabela do fundo mostra o conteúdo dos cofre seleccionados.

21.2.1. Criar um Cofre

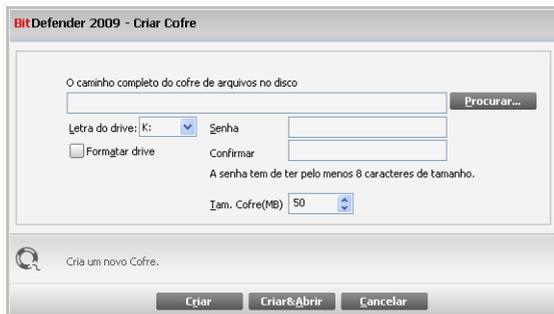
Para criar um cofre, use um dos seguintes métodos:

- Clique **Criar cofre**.



- Clique botão direito do mouse na tabela dos cofres e seleccionar **Criar**.
- Clique botão direito do mouse no seu Ambiente de Trabalho ou numa pasta do seu computador, apontar para **Cofre Arquivos BitDefender** e seleccionar **Criar**.

Uma nova janela irá aparecer.



Criar Cofre de arquivos

Proceder da seguinte forma:

1. Especificar a localização e o nome do cofre de arquivos.
 - Clique em **Explorar** para seleccionar a localização do cofre e guarde o cofre de arquivos sob o nome desejado.
 - Insira o caminho completo do cofre de arquivos no disco.
2. Escolha a letra da drive a partir do menu. Quando abre o cofre, um disco virtual com a letra seleccionada aparecerá em O Meu Computador.
3. Insira a palavra-passe do cofre no campo **Senha** . Qualquer pessoa que tente abrir o cofre e aceder aos seus arquivos tem de inserir a senha.
4. Selecciona **Formatar drive** para formatar a drive virtual atribuída ao cofre.
5. Se deseja mudar o tamanho por defeito (50 MB) do cofre, insira o valor desejado no campo **Tamanho Cofre** .
6. Clique em **Criar** se deseja criar o cofre na localização seleccionada. Para criar e mostrar o cofre como um disco virtual em O Meu Computador, clique em **Criar&Abrir**.



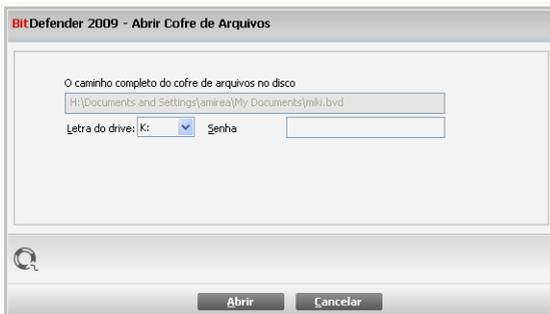
21.2.2. Abrir um Cofre

De forma a poder aceder e trabalhar com os arquivos armazenados no cofre, tem de o abrir. Quando abre o cofre, um disco virtual aparece em O Meu Computador. A drive tem a denominação da letra que atribuiu ao cofre.

Para abrir o cofre, use um dos seguintes métodos:

- Seleccione o cofre da tabela e clique **Abrir cofre**.
- Clique com o botão-direito na tabela e seleccione **Abrir**.
- Clique com o botão-direito no cofre de arquivos no seu computador, aponte para **Cofre arquivos BitDefender** e seleccione **Abrir**.

Uma nova janela irá aparecer.



Abrir Cofre de arquivos

Proceder da seguinte forma:

1. Escolha a letra da drive a partir do menu.
2. Insira a palavra-passe do cofre no campo **Senha**.
3. Clique em **Abrir**.

21.2.3. Fechar um Cofre

Quando terminou de trabalhar sobre um cofre de arquivos, deve de o fechar de forma a proteger os seus dados.

Para fechar um cofre, use um dos seguintes métodos:



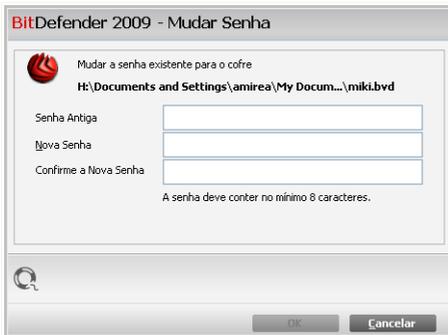
- Selecione o cofre na tabela e clique em **Fechar cofre**.
- Clique com o botão-direito do mouse no cofre da tabela e selecione **Fechar**.
- Clique com o botão direito do mouse no cofre de arquivos do seu computador, aponte para **Cofre Arquivos BitDefender** e selecione **Fechar**.
- Clique com o botão direito do mouse no correspondente disco virtual em Meu Computador, aponte para **Cofre arquivos BitDefender** e selecione **Fechar**.

21.2.4. Mudar senha do Cofre

Para mudar a senha do cofre, use um dos seguintes métodos:

- Selecione o cofre na tabela e clique em **Alterar senha**.
- Clique com o botão-direito do mouse no cofre da tabela e selecione **Alterar senha**.
- Clique com o botão-direito do mouse no cofre de arquivos do seu computador, aponte para **Cofre arquivos BitDefender** e selecione **Alterar senha do cofre**.

Uma nova janela irá aparecer.



Alterar senha do Cofre

Proceder da seguinte forma:

1. Insira a senha atual do cofre no campo **senha antiga** .
2. Insira a nova senha nos campos **Nova senha** e **Confirmar nova senha** .



Nota

A senha deve ter pelo menos oito caracteres em tamanho. Para obter uma senha forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, \$ ou @).

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

21.2.5. Adicionar arquivos ao Cofre

Para adicionar arquivos ao cofre, siga os seguintes passos:

1. Clique em **Adicionar arquivo**. Uma nova janela irá aparecer.
2. Selecione os arquivos / pastas que deseja adicionar ao cofre.
3. Clique em **OK** para copiar os objectos seleccionados para o cofre.



Nota

Não pode adicionar arquivos de sistema ou de aplicações ao cofre.

21.2.6. Remover arquivos do Cofre

Para remover arquivos do cofre, siga os seguintes passos:

1. Selecione da tabela de cofres o cofre que contém o arquivo a ser removido.
2. Selecione o arquivo a ser removido a partir da tabela que mostra o conteúdo do cofre.
3. Clique em **Remover arquivo**.



Nota

Se o cofre estiver aberto, pode remover diretamente os arquivos a partir da drive virtual atribuída ao cofre.



22. Vulnerabilidade

Um passo importante na proteção do seu computador contra as pessoas e aplicações maliciosas é manter atualizado o seu sistema operacional e as aplicações que usa regularmente. Mais ainda, para evitar acesso físico não-autorizado ao seu computador, senhas fortes (senhas que não são fáceis de adivinhar) devem de ser criadas para cada conta de usuário do Windows.

O BitDefender analisa regularmente o seu sistema em busca de vulnerabilidades e notifica-o das incidências existentes.

22.1. Status

Para configurar a análise automática de vulnerabilidades, ou levar a cabo uma, clique em **Vulnerabilidade>Estado** no Modo Avançado.

The screenshot shows the BitDefender Internet Security 2009 - Trial interface. At the top, a red banner indicates "ESTADO: Existe 1 incidência pendente" with a "REPARAR" button. Below this, the "Status" tab is selected, showing a checkbox for "A Verificação Automática de Vulnerabilidade está ativada" which is checked. A "Verificar" button is present. The main area displays the "Estado da Última Verificação de Vulnerabilidade" table.

Incidência	Status	Ação
Atualizações Microsoft Críticas	Instalar	Instalar
Outras Atualizações Microsoft	Instalar	Instalar
Status atualização automática	Habilitada	Nenhum
Yahoo! Messenger	Última	Nenhum
Winamp	Desatualizado	Mais informac...
Firefox	Última	Nenhum
cosmin	Senha Fraca	Reparar
Administrator	Senha Forte	Nenhum

At the bottom of the window, there is a help icon and text: "Para descobrir mais sobre cada opção apresentada na Interface do Usuário BitDefender, por favor mova o seu cursor sobre a janela. Um texto de ajuda relevante será apresentado nessa área." Below this is the BitDefender logo and a navigation bar with links: "Comprar/Renovar - Minha Conta - Registro - Ajuda - Suporte - Histórico".

Status de Vulnerabilidade



A tabela mostra os problemas cobertos na última análise de vulnerabilidade e o seu estatus. Você pode ver a ação que deve ser tomada para consertar cada situação de vulnerabilidade, caso esta exista. Se a ação é **Nenhuma**, então o ponto detectado não representa um ponto de vulnerabilidade.



Importante

Para ser automaticamente notificado acerca das vulnerabilidades do seu sistema e aplicações, mantenha a **Análise Automática de Vulnerabilidades** ativada.

22.1.1. Consertando pontos vulneráveis

Para consertar um ponto vulnerável, clique duas vezes com o mouse e, dependendo do problema, continue como definido a seguir:

- Se houverem atualizações disponíveis do Windows, clique **Instale todas as Atualizações do Sistema** para instalá-las.
- Se um aplicativo estiver desatualizado, use o link **Página Inicial** fornecido para efetuar o download e instalar a versão mais atualizada do aplicativo.
- Se uma conta de usuário do Windows possuir uma senha considerada vulnerável, faça o usuário mudar sua senha no próximo logon ou mude a senha você mesmo.

Você pode clicar **Verificar Agora** e seguir as instruções para consertar os pontos vulneráveis passo a passo.



Passo 1/6 - Seleccionar Vulnerabilidades a Verificar

BitDefender 2009

Assistente de Vulnerabilidade BitDefender

Passo 1 | Passo 2 | Passo 3 | Passo 4 | Passo 5 | Passo 6

Seleccionar Tarefas

Este assistente irá guiá-lo através das ações necessárias para identificar aplicações desatualizadas e as contas do Windows que têm uma senha fraca. Por favor seleccione da lista abaixo que itens deseja ver analisados em busca de vulnerabilidades.

- Verificar Atualizações Críticas Windows
- Verificar Atualizações Opcionais Windows
- Verificar a existência de duplicados de atualização
- Verificar as Senhas das suas Contas Windows

Seleccionar as ações que o módulo de vulnerabilidade deve considerar ao analisar o seu sistema.

bitdefender Avançar Cancelar

Vulnerabilidades

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



Passo 2/6 - Analisar em Busca de Vulnerabilidades



Espere que o BitDefender termine a análise de vulnerabilidades.



Passo 3/6 - Alterar Palavras-passe Fracas

Nome do Usuário	Forte	Status
Administrator	Forte	Ok
cosmin	Fracas	Reparar

Esta é a lista das senhas definidas no seu computador e o nível de proteção que elas oferecem. Clique no botão "Reparar" para modificar as senhas fracas.

Avançar **Cancelar**

Senhas do usuário

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

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

Como prefere resolver esta incidência?

Obrigado o usuário a mudar a senha durante o próximo logon

Mude a senha você mesmo agora

Digite a senha:

Confirme a Senha:

OK **Fechar**

Mudar a senha



Selecione o método para reparar esta incidência:

- **Forçar o usuário a mudar a senha no próximo login:** O BitDefender avisará o usuário que tem de alterar a senha da próxima vez que ele entrar no Windows.
- **Mudar a senha do usuário.** Deve inserir a nova senha nos campos editáveis.



Nota

Para obter uma senha forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, \$ ou @).

Clique em **OK** para alterar a senha.

Clique em **Próximo**.



Passo 4/6 - Actualizar Aplicações

Nome da Aplicação	Versão Instalada	Última Versão	Status
Yahoo! Messenger	8.1.0.421	8.1.0.241	Atualizado
Winamp	5,5,3,1938	5,5,4	Página Principal
Firefox	3.0.4 (en-US)	3.0.1 (en-US)	Atualizado

Esta é a lista das aplicações suportadas pelo BitDefender e das atualizações disponíveis, se as houver.

Aplicações

Pode ver a lista de todas as aplicações verificadas pelo BitDefender e se as mesmas estão ou não actualizadas. Se a aplicação não estiver actualizada, clique no link fornecido para descarregar a versão mais recente.

Clique em **Próximo**.



Passo 5/6 - Atualizar Windows

BitDefender 2009

Assistente de Vulnerabilidade BitDefender

Passo 1 | **Passo 2** | Passo 3 | Passo 4 | **Passo 5** | Passo 6

Atualizações do Windows

Verificar Atualizações Críticas Windows

- Windows Genuine Advantage Validation Tool (KB892130)
- Security Update for Microsoft XML Core Services 4.0 Service Pack 2 (KB954430)
- Windows XP Service Pack 3 (KB936929)

Verificar Atualizações Opcionais Windows

- Windows Search 4.0 For Windows XP (KB940157)
- Microsoft Silverlight (KB957938)
- Group Policy Preference Client Side Extensions for Windows XP (KB943729)
- Root Certificates Update

Instalar todas atualizações do Sistema

Esta é a listas das atualizações críticas e não-críticas das aplicações do Windows

bitdefender Avançar Cancelar

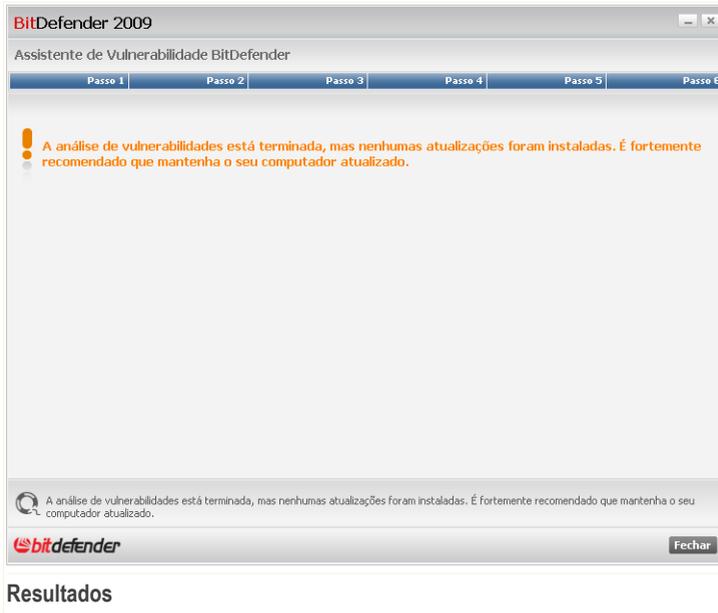
Atualizações Windows

Pode ver a lista das actualizações críticas e não-críticas do Windows que não se encontram actualmente instaladas no seu computador. Clique em **Instalar Todas Actualizações do Sistema** para instalar todas as actualizações disponíveis.

Clique em **Próximo**.



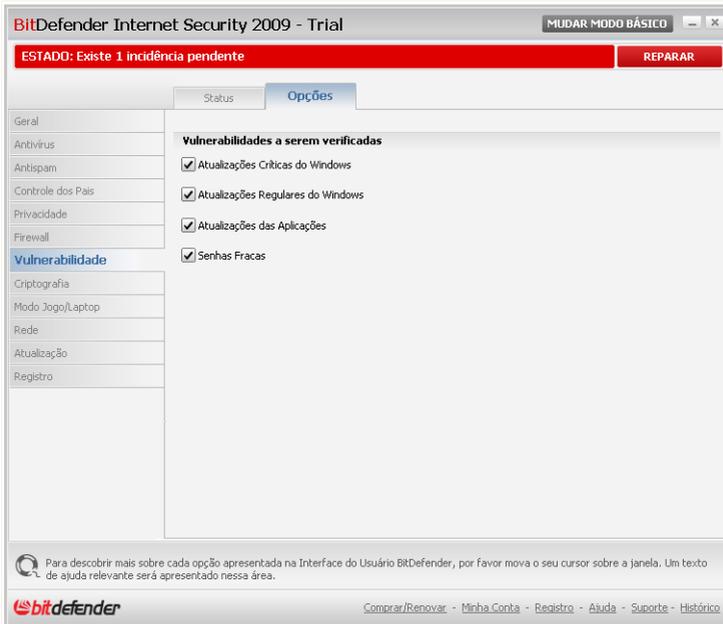
Passo 6/6 - Ver Resultados



Clique em **Fechar**.

22.2. Opções

Para configurar as definições da análise automática de vulnerabilidades, clique em **Vulnerabilidade>Configuração** no Modo Avançado.



Definições da Análise Automática de Vulnerabilidades

Selecione as caixas que correspondem às vulnerabilidades do sistema que deseja que sejam regularmente verificadas.

- **Atualizações Críticas do Windows**
- **Atualizações Regulares do Windows**
- **Palavras-passe Fracas .**
- **Atualizações de Aplicações**



Nota

Se limpar a a caixa correspondente a uma determinada vulnerabilidade, o BitDefender não o irá mais notificar acerca das incidências relacionadas.



23. Modo de Jogo / Portátil

O módulo do modo de Jogo / Portátil permite-lhe configurar os modos especiais de operação do BitDefender.

- O **Modo de Jogo** modifica temporariamente as definições da protecção de forma a minimizar o seu impacto no desempenho do sistema enquanto estiver a jogar.
- O **Modo de Portátil** evita que as atrefas agendadas sejam executadas quando o seu portátil esteja em modo de bateria de forma a economizar a mesma.

23.1. Modo de Jogo

O Modo de Jogo modifica temporariamente as definições da protecção de forma a minimizar o seu impacto no desempenho do sistema. Quando liga o Modo de Jogo, as seguintes definições são aplicadas:

- Todos os alertas e pop-ups do BitDefender são desactivados.
- O nível da protecção em tempo-real do BitDefender é definida como **Permissivo**.
- A Firewall BitDefender está definida para **Permitir todos**. Isto significa que todas as novas ligações (quer de entrada quer de saída) são automaticamente autorizadas, independentemente da porta e do protocolo utilizado.
- As actualizações não são executadas por defeito.



Nota

Para mudar esta configuração, vá para **Atualizar>Configurações** e limpe a **Não atualizar se o Modo Game (Jogo) estiver ativado** selecione a opção.

- As tarefas de análise agendadas são desactivadas por defeito.

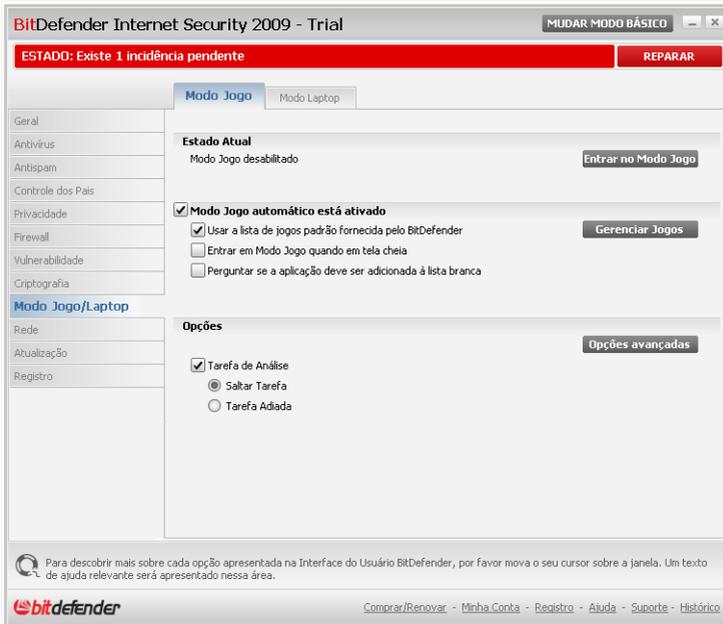
Por defeito, o BitDefender entra automaticamente em Modo de Jogo quando inicia um jogo da lista dos jogos conhecidos do BitDefender ou quando uma aplicação entra em Modo de ecrã inteiro. Pode entrar manualmente em Modo de Jogo usando a hotkey por defeito **Ctrl+Alt+Shift+G**. É fortemente recomendado que saia do Modo de Jogo quando acaba de jogar (Pode usar a mesma hotkey por defeito **Ctrl+Alt+Shift+G**).



Nota

Enquanto no Modo de Jogo, pode ver a letra G sobre o  ícone do BitDefender.

Para configurar o Modo Jogo, vá para **Modo Jogo/Laptop>Modo Jogo** no Modo Avançado



Modo de Jogo

No topo da secção, pode ver o estado do Modo de Jogo. Clique em **Entrar Modo de Jogo** ou **Sair Modo de Jogo** para alterar o estado actual.

23.1.1. Configurar Modo de Jogo Automático

O Modo de Jogo Automático permite que o BitDefender entre automaticamente em Modo de Jogo quando um jogo é detectado. Você pode configurar uma das seguintes opções:



- **Usar por defeito a lista de jogos do BitDefender** - para entrar automaticamente em Modo de Jogo quando inicia um jogo da lista dos jogos conhecidos do BitDefender. Para ver esta lista, clique em **Gerir Jogos** e depois em **Ver Jogos Permitidos**.
- **Entrar em Modo de Jogo quando em ecrã inteiro** - entra automaticamente em Modo de Jogo quando uma aplicação entra em modo de ecrã inteiro.
- **Adicionar a aplicação à lista de jogos?** - para ser notificado a adicionar a nova aplicação à lista de jogos quando deixar o modo de ecrã inteiro. Ao adicionar uma nova aplicação à lista de jogos, da próxima vez que o jogar o BitDefender entrará automaticamente em Modo de Jogo.

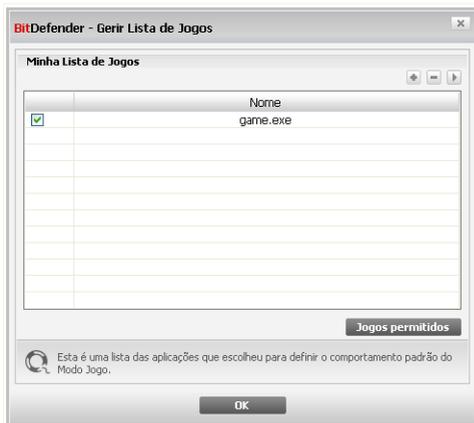


Nota

Se não deseja que o BitDefender entre automaticamente em Modo de Jogo, limpe a caixa de selecção **Modo de Jogo Automático**.

23.1.2. Gerir a Lista de Jogos

O BitDefender entra automaticamente em Modo de Jogo quando inicia uma aplicação que se encontra na lista de jogos. Para ver e gerir a lista de jogos, clique em **Gerir Jogos**. Uma nova janela irá aparecer.



Lista de Jogos

Novas aplicações são adicionadas automaticamente à lista quando:



- Inicia um jogo da lista de jogos conhecidos do BitDefender. Para ver esta lista, clique em **Ver Jogos Permitidos**.
- Após sair do modo de ecrã inteiro, pode adicionar a aplicação à lista de jogos a partir da janela de notificação.

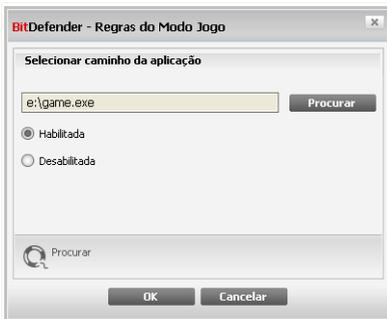
Se deseja desactivar o Modo de Jogo Automático para uma determinada aplicação da lista, limpe a correspondente caixa de selecção. Deve de desactivar o Modo de Jogo Automático para as aplicações que regularmente entram em modo de ecrã inteiro, tais como os exploradores da Internet e os leitores de filmes.

Para gerir a lista de jogos, pode usar os botões colocados no topo da tabela:

- **Adicionar** - adicionar um novo aplicativo à lista de jogos.
- **Remover** - remover um aplicativo da lista de jogos.
- **Editar** - editar um registo existente na lista de jogos.

Adicionar ou Editar Jogos

Quando adiciona ou edita uma entrada da lista de jogos, a seguinte janela aparecerá:



Adicionar Jogo

Clique em **Explorar** para seleccionar a aplicação e o caminho da mesma no campo de edição.

Se não quiser entrar automaticamente em Modo de Jogo quando a aplicação seleccionada é executada seleccione **Desactivar**.

Clique em **OK** para adicionar a entrada à lista de jogos.



23.1.3. Configurar as Definições do Modo de Jogo

Para configurar o comportamento das tarefas agendadas, use estas opções:

- **Tarefa de Análise** - para evitar que as tarefas de análise agendadas se executem enquanto estiver em Modo de Jogo. Você pode escolher uma das seguintes opções:

Opção	Descrição
Saltar Tarefa	Não executar de todo a tarefa agendada.
Adiar Tarefa	Executa a tarefa imediatamente após sair do Modo de Jogo.

Para desactivar automaticamente a firewall BitDefender enquanto estiver no Modo de Jogo, siga os seguintes passos:

1. Clique em **Configuração Avançada**. Uma nova janela irá aparecer.
2. Marcar a caixa **Não usar firewall**.
3. Clique em **OK** para salvar as alterações.

23.1.4. Mudar a Hotkey do Modo de Jogo

Pode entrar manualmente em Modo de Jogo usando a hotkey por defeito Ctrl+Alt+Shift+G. Se deseja mudar a hotkey, siga estes passos:

1. Clique em **Configuração Avançada**. Uma nova janela irá aparecer.



Configurações Avançadas



2. Por baixo da opção **Usar HotKey** , defina a hotkey desejada:
 - Escolha as teclas que deseja usar ao seleccionar uma das seguintes: Tecla Control (**Ctrl**), Tecla Shift (**Shift**) ou tecla Alternate (**Alt**).
 - No campo de edição, insira a letra correspondente à tecla que deseja usar.Por exemplo, se deseja usar a hotkey **Ctrl+Alt+D** , deve seleccionar **Ctrl** e **Alt** e inserir **D**.
3. Clique em **OK** para salvar as alterações.



Nota

Remover a selecção ao pé de **Activar HotKey** irá desactivar a hotkey.

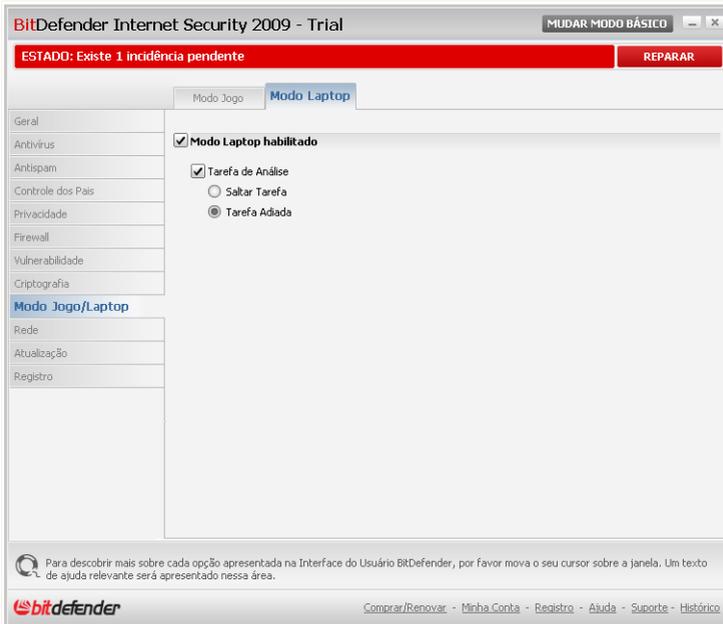
23.2. Modo de Portátil

O Modo Portátil foi especialmente desenhado para os usuários de laptops. O seu propósito é minimizar o impacto do BitDefender no consumo de energia enquanto o laptop estiver a funcionar a bateria.

Enquanto estiver em Modo de Portátil, as tarefas agendadas não serão levadas a cabo por defeito.

O BitDefender detecta quando o seu portátil está a funcionar a bateria e automaticamente entra em Modo de Portátil. De igual forma, O BitDefender sai automaticamente do Modo de Portátil quando detecta que o seu portátil já não está a funcionar a bateria.

Para configurar o Modo Laptop, vá para **Modo Jogo/Laptop>Modo Laptop** no Modo Avançado



Modo de Portátil

Pode ver se o Modo de Portátil está ou não ligado. Se o Modo de Portátil está ligado, o BitDefender aplicará as definições configuradas para o portátil a funcionar a bateria.

23.2.1. Configurar Definições do Modo de Portátil

Para configurar o comportamento das tarefas agendadas, use estas opções:

- **Tarefa de Análise** - para evitar que as tarefas de análise agendadas se executem enquanto estiver em Modo de Portátil. Você pode escolher uma das seguintes opções:

Opção	Descrição
Saltar Tarefa	Não executar de todo a tarefa agendada.



<i>Opção</i>	<i>Descrição</i>
Adiar Tarefa	Executar a tarefa agendada assim que sair do Modo de Portátil.



24. Rede

O módulo de rede permite-lhe gerir os produtos BitDefender instalados nos seus computadores em casa a partir de um só computador.

Mapa de Rede

Para poder gerir os produtos BitDefender instalados nos computadores de casa, siga os seguintes passos:

1. Adira à rede pessoal do BitDefender no seu computador. Adirir à rede consiste em configurar uma senha administrativa para o gestor da rede pessoal.
2. Vá a cada computador que deseja gerir e adira-o à rede (defina a senha).
3. Volte para o seu computador e adicione os computadores que deseja gerir.



24.1. Aderir à Rede BitDefender

Para aderir à rede pessoal BitDefender, siga os seguintes passos:

1. Clique em **Aderir/Criar Rede**.>. Será notificado para configurar a senha de gestão de rede pessoal.

BitDefender

Inserir uma senha

Uma senha é necessária para juntar-se ou criar uma rede por razões de segurança (protege o acesso ao seu computador através da sua rede pessoal).

Digite a senha:

Redigite a senha:

OK Cancelar

Configurar senha

2. Insira a mesma senha em cada um dos campos editáveis.
3. Clique em **OK**.

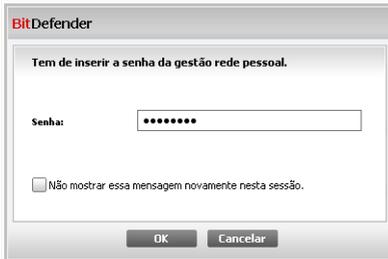
Pode ver o nome do computador a aparecer no mapa de rede.

24.2. Adicionar Computadores à Rede BitDefender

Antes que possa adicionar um computador à rede doméstica BitDefender, deve de configurar a sua senha de gestão de rede pessoal no respectivo computador.

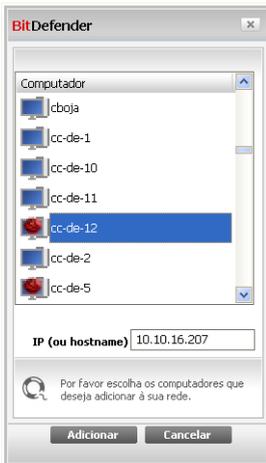
Para adicionar um computador à rede pessoal BitDefender, siga os seguintes passos:

1. Clique em **Gerir Rede**. Será notificado para inserir a sua senha de gestão de rede pessoal local.



Inserir senha

2. Insira a senha de gestão rede pessoal e clique em **OK**. Uma nova janela irá aparecer.



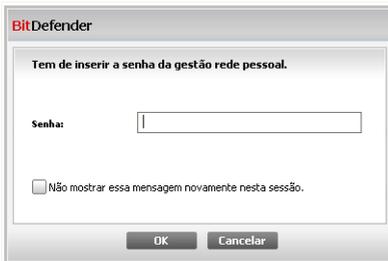
Adicionar Computador

Pode ver a lista dos computadores na rede. O significado do ícone é o seguinte:

-  Indica um computador on-line sem produtos BitDefender instalados.
-  Indica um computador on-line com o BitDefender instalado.
-  Indica um computador offline com o BitDefender instalado.



3. Faça uma das coisas seguintes:
 - Seleccione da lista o nome do computador a adicionar.
 - Insira o endereço IP ou o nome do computador a adicionar no campo correspondente.
4. Clicando **Adicionar**. Será notificado para inserir a sua senha de gestão de rede pessoal do respectivo computador.



Autenticar

5. Insira a senha de gestão de rede pessoal configurada no respectivo computador.
6. Clique em **OK**. Se forneceu a senha correta, a nome do computador seleccionado aparecerá no mapa de rede.

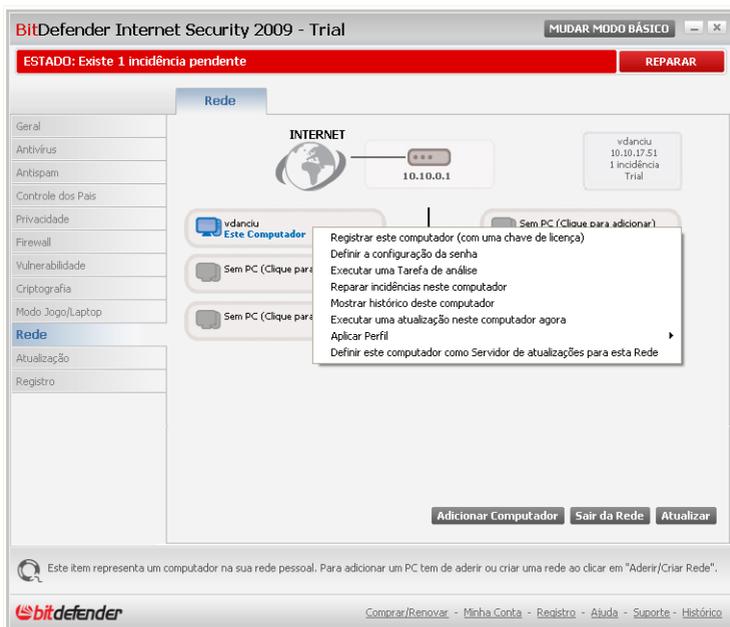


Nota

Podem adicionar até cinco computadores neste mapa de rede.

24.3. Gerir a Rede BitDefender

Uma vez que tenha criado com sucesso a sua rede pessoal BitDefender pode gerir todos os produtos BitDefender a partir de um único computador.



Mapa de Rede

Se mover o curso do seu mouse sobre um computador do mapa de rede, pode ver alguma informação acerca dele (nome, endereço IP, número de incidências que estão a afetar a segurança do sistema, o estado de registo do BitDefender).

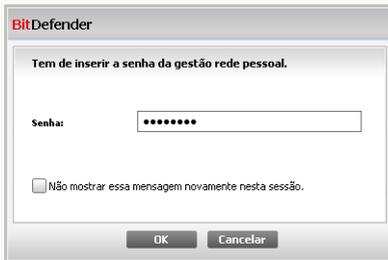
Se clicar botão direito do mouse sobre o nome de um computador no mapa de rede, pode ver todas as tarefas administrativas que pode levar a cabo no computador remoto.

- **Registrar este computador**
- **Definir senha definições**
- **Executar uma tarefa de análise**
- **Reparar incidências neste computador**
- **Mostrar histórico deste computador**
- **Levar a cabo uma actualização neste computador agora**



- Aplicar Perfil
- Levar a cabo uma tarefa de Tuneup neste computador
- Definir este computador como Servidor de Actualizações desta Rede

Antes de levar a cabo uma tarefa num computador específico, será notificado para inserir a senha de gestão de rede pessoal local.



Inserir senha

Insira a senha de gestão rede pessoal e clique em **OK**.



Nota

Se planeia levar a cabo várias tarefas, seleccione **Não me mostrem mais esta mensagem durante esta sessão**. Ao seleccionar esta opção, não será notificado novamente pela senha durante esta sessão.



25. Atualização

Novo malware é achado e identificado todos os dias. É por isso que é muito importante manter o BitDefender atualizado com as últimas assinaturas de malware.

Se você se conectar a Internet através de banda-larga ou DSL, o BitDefender se encarrega da atualização. Ele verifica novas assinaturas de vírus quando você liga o seu computador e toda **hora** depois.

Se uma actualização é detectada, poderá ser notificado para confirmar a actualização ou a mesma é levada a cabo automaticamente, dependendo das **definições automáticas da actualização**.

O processo de atualização é executado "on the fly", o que significa que os arquivos são substituídos progressivamente. Desta forma, o processo de atualização não afetará o funcionamento do produto e, ao mesmo tempo, exclui qualquer possibilidade de vulnerabilidade.

Atualizações vêm das seguintes formas:

- **Atualização dos mecanismos antivírus** - conforme novas ameaças aparecem, os arquivos contendo as assinaturas de vírus devem ser atualizados para assegurar proteção permanente atualizada contra eles. Esta atualização também é conhecido como **Atualização de Definições de Vírus**.
- **Atualização dos mecanismos Anti-spam** - novas regras serão adicionadas aos filtros heurístico e de URL e novas imagens serão adicionadas ao Filtro de Imagem. Isso ajudará a aumentar a eficácia de seus mecanismos Anti-spam. Esta atualização também é conhecido como **Atualização do Anti-Spam**.
- **Atualizações para os motores anti-spyware** - novas assinaturas de spyware serão adicionadas a base de dados. Esta atualização também é conhecido como **Atualização Anti-spyware**.
- **Atualização do produto** - quando uma nova versão do produto é lançada, novos recursos e técnicas de verificação são introduzidos para aprimorar a performance do produto. Esta atualização também é conhecido como **Atualização de versão do produto**.

25.1. Atualização Automática

Para ver informação relacionada com actualizações e executar actualizações automáticas, clique em **Actualização>Actualização** no Modo Avançado.



The screenshot shows the BitDefender Internet Security 2009 - Trial interface. At the top, there is a red status bar indicating "ESTADO: Existe 1 incidência pendente" and a "REPARAR" button. Below this, the "Atualização" (Update) section is active, showing that automatic updates are enabled. It displays the last update analysis and update times as 12/30/2008 2:15:35 PM. A "Atualizar agora" (Update now) button is present. The "Propriedades das assinaturas de Vírus" (Virus signature properties) section shows 2395696 signatures and version 7.22861, with a "Ver lista de vírus" (View virus list) button. The "Status do Download" (Download status) section indicates no updates are available and shows progress bars for "Arquivo:" (0% / 0 kb) and "Total da atualização" (0% / 0 kb). A help icon and text are at the bottom left, and navigation links like "Comprar/Renovar" and "Minha Conta" are at the bottom right.

Atualização Automática

Aqui poderá ver quando foi feita a última actualização e a última verificação de actualizações, com também a informação da última actualização feita (se bem-sucedida, se ocorreram erros). Também a informação acerca da versão do motor e o número de assinatura são mostrados.

Se abrir esta secção durante uma actualização, poderá o estado do download.



Importante

Para estar protegido contra as mais recentes ameaças mantenha a **Actualização Automática** activada.

Pode obter as assinaturas de malware do seu BitDefender ao clicar **Mostrar Lista de Vírus**. Um arquivo HTML que contém todas as assinaturas disponíveis será criado e aberto no browser da internet. Pode procurar uma assinatura específica de malware por entre a base de dados ou clicar **Lista de Vírus BitDefender** para aceder à base de dados de assinaturas BitDefender on-line.



25.1.1. Solicitar uma Actualização

A actualização automática também pode ser feita a qualquer hora clicando em **Atualizar Agora**. Também conhecido por **Actualização a pedido do usuário**.

O módulo de **Actualização** irá conectar ao servidor de actualização do BitDefender e verificará se uma actualização está disponível. Caso seja verdadeiro, dependendo das opções configuradas na seção **Opções de Actualização Manual** você será indagado a confirmar a actualização ou a mesma será feita automaticamente.



Importante

Talvez seja necessário reiniciar o computador depois da actualização. Caso seja necessário, recomendamos que o faça o mais rápido possível.

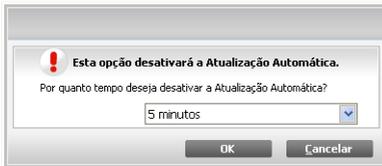


Nota

Se você estiver conectado a Internet através de uma conexão discada, é uma boa idéia gerar o hábito de actualizar o BitDefender a pedido do usuário.

25.1.2. Desabilitar Actualização Automática

Se você desabilitar a actualização automática, uma janela de alerta aparecerá.



Desabilitar 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

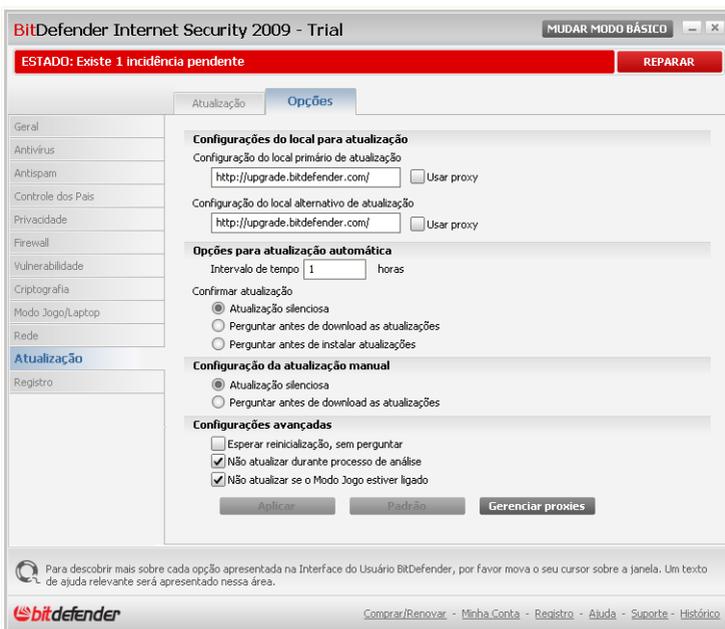
Esta é uma incidência de segurança crítica. recomendamos que desactive a actualização automática pelo menor tempo possível. Se o BitDefender não for actualizado regularmente, não será capaz de o proteger contra as ameaças mais recentes.



25.2. Opções de Actualização

Actualizações podem ser feitas da rede local, pela Internet, diretamente ou por um servidor Proxy. Por defeito, o BitDefender verificará as actualizações a cada hora, via Internet, e instalará as que estejam disponíveis sem o avisar.

Para configurar as definições de actualização e gerir proxies, clique em **Actualização>Configuração** no Modo Avançado.



Opções de Actualização

As configurações da actualização estão agrupadas em 4 categorias (**Configuração da Localização da Actualização**, **Configuração de actualização automática**, **Configuração de Actualização Manual** e **Configuração Avançada**). Cada categoria será descrita separadamente.



25.2.1. Definir local para atualização

Para definir a localização da actualização, use as opções da categoria **Configuração da Localização da Actualização** .



Nota

Configure estas definições apenas se estiver ligado a uma rede local que armazena localmente as assinaturas de malware do BitDefender ou se liga à Internet através de um servidor proxy.

Para actualizações melhores e mais rápidas, você pode configurar dois locais de actualização: uma **Local de actualização primário** e uma **Local de actualização alternativo**. Por defeito estas localizações são iguais: <http://upgrade.bitdefender.com>.

Para modificar um dos locais de actualização, insira o URL do local mirror no campo **URL** que corresponde ao novo local para o qual deseja mudar.



Nota

Recomendamos que defina como local primário de actualização o local mirror e deixar o local alternativo de actualização como está, como um plano de backup em caso do local mirror ficar indisponível.

No caso em que a empresa usa um servidor proxy para se ligar à Internet, seleccione **Usar proxy** de depois clique em **Gerir proxies** para configurar as definições do proxy. Para mais informação, por favor consulte "**Gerir Proxies**" (p. 285)

25.2.2. Configurar Atualização Automática

Para configurar o processo de actualização automática do BitDefender, use as opções na categoria **Configuração Actualização Automática** .

Pode definir o intervalo entre duas verificações 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:

- **Atualização Silenciosa** - O BitDefender faz download automaticamente e implementa a actualização.
- **Perguntar antes de fazer download das actualizações** - todas as vezes que uma actualização estiver disponível, você será indagado antes do download ser feito.



- **Perguntar antes de instalar atualizações** - todas as vezes que uma atualização for feita em download, você será indagado antes de ela ser instalada.

25.2.3. Configurar Atualização Manual

Para definir como a atualização manual (atualização a pedido do usuário) deve ser executada, selecione uma das seguintes opções na categoria **Configuração Atualização Manual**:

- **Atualização silenciosa** - a atualização manual será feita em segundo plano automaticamente.
- **Perguntar antes de fazer download das atualizações** - todas as vezes que uma atualização estiver disponível, você será indagado antes do download ser feito.

25.2.4. Configurar Opções Avançadas

Para evitar que o processo de actualização do BitDefender interfira com o seu trabalho, configure as opções na categoria **Configuração Avançada**:

- **Esperar reinicialização, sem perguntar** - Se uma atualização requerer uma inicialização, o produto continuará funcionando com os arquivos antigos até o sistema reiniciar. O usuário não será indagado para reiniciar o sistema, sendo assim o processo de atualização do BitDefender não irá interferir no trabalho do usuário.
- **Não actualizar se a análise estiver a decorrer** - O BitDefender não vai actualizar se estiver a decorrer uma análise. Desta forma, o processo de actualização do BitDefender não vai interferir com as tarefas de análise.



Nota

Se o BitDefender for actualizado enquanto a análise estiver a decorrer, o processo de análise será cancelado.

- **Não actualizar se o modo de jogo estiver ligado** - O BitDefender não actualizará se o Modo de Jogo estiver ligado. Desta forma, poderá minimizar a influência do produto no desempenho do sistema durante os jogos.

25.2.5. Gerir Proxies

Se a sua empresa usa um servidor proxy para se ligar à Internet, deverá especificar as definições do proxy de forma a que o BitDefender se atualize sozinho. De outra forma, usará as definições do administrador que instalou o produto ou o usuário atual por defeito do browser, caso haja algum.



Nota

As definições do proxy só podem ser configuradas por usuários com direitos administrativos no computador ou por power users (usuários que sabem a senha da configuração do produto).

para gerir as definições do proxy, clique em **Gerir proxies**. A janela **Gestor Proxy** irá aparecer.

Configurações Proxy

Definições de administrador do proxy (detectadas durante o período de instalação)

Endereço: Porta: Nome do Usuário:
Senha:

Definições de proxy do usuário atual (browser padrão)

Endereço: Porta: Nome do Usuário:
Senha:

Especifique as suas definições de proxy

Endereço: Porta: Nome do Usuário:
Senha:

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 esteve logged com essa conta. Se o servidor proxy requer um nome de usuário e uma senha, deverá inseri-los nos campos correspondentes.
- **Definições de proxy do usuário atual (do browser por defeito)** - as definições de proxy do usuário atual, extraídas do explorador por defeito. Se o servidor proxy requer um nome de usuário e uma senha, deverá inseri-los nos campos correspondentes.



Nota

Os browsers de internet suportados são o Internet Explorer, Mozilla Firefox e Opera. Se utiliza outro explorador por defeito, o BitDefender não será capaz de obter as definições do proxy do atual usuário.

- **O seu próprio conjunto de definições de proxy** - definições de proxy que pode configurar se estiver logged in como administrador.

As seguintes definições devem ser especificadas:

- **Endereço** - introduza o IP do servidor proxy.
- **Porta** - insira a porta que o BitDefender usa para se ligar ao servidor proxy.
- **Usuário do proxy** - digite um usuário reconhecido pelo Proxy.
- **Senha do proxy** - digite a senha válida para o usuário especificado anteriormente.

Quando tentar ligar-se à Internet, cada conjunto de definições do proxy é experimentado na sua vez, até que o BitDefender se consiga ligar.

Primeiro, o conjunto que contém as suas definições do proxy será utilizado para ligar a Internet. Se esse não funcionar, as definições de proxy detectadas durante a instalação serão experimentadas logo a seguir. Finalmente se nenhuma dessa funcionar, as definições de proxy do usuário atual serão retiradas do seu browser por defeito e usadas para obter a ligação à Internet.

Clique em **OK** para guardar as alterações e fechar a janela.

Clique em **Aplicar** para salvar as alterações ou clique em **Padrão** para retornar às opções padrão.



26. Registro

Para saber toda a informação sobre o seu produto BitDefender e o estado do registo, clique em **Registro** no Modo Avançado.

Registro

Esta secção mostra:

- **Informação do Produto** : O produto BitDefender e a sua versão.
- **Informação de Registro** : o endereço de e-mail usado para entrar na sua conta BitDefender (se configurada), a actual chave de licença e o número de dias que faltam para a licença expirar.



26.1. Registrar BitDefender Internet Security 2009

Clique em **Registrar agora** para abrir a janela de registo do produto.



Pode ver o estado do registo do BitDefender, a actual chave de licença e quantos dias faltam para a licença expirar.

Para registar BitDefender Internet Security 2009:

1. Selecciona **Desejo registar o produto com uma nova chave**.
2. Insira a chave de licença no campo de edição.



Nota

- Pode encontrar a sua chave de licença:
- Na bolsa do CD.
 - ou no cartão de registo do produto.
 - no e-mail da sua compra on-line.



Se não possuir uma chave de licença BitDefender, clique no link que lhe facultamos para ir até à loja on-line do BitDefender e adquirir uma.

Clique em **Finalizar**.

26.2. Criar uma conta BitDefender

Como parte do processo de registo, você PRECISA criar sua conta BitDefender. A sua cna BitDefender lhe oferece acesso às atualizações de vírus BitDefender, suporte técnico grátis, além de ofertas e promoções especiais. Se perder a sua chave de licença BitDefender, pode entrar na sua conta em <http://myaccount.bitdefender.com> e recuperá-la.



Importante

Você precisa se registrar criando uma conta dentro de 15 dias após ter instalado BitDefender (se você o fizer, o prazo limite se estenderá para 30 dias). Caso contrário, BitDefender não mais efetuará atualizações de antivírus.

Se ainda não criou uma conta BitDefender, clique em **Criar uma conta** para abrir a janela de registo da conta do produto



BitDefender Internet Security 2009

Criar Conta

Registro da Minha Conta

Para que seu produto seja atualizado com as mais novas vacinas e ferramentas antivírus, favor registrar e criar uma conta BitDefender. Desta forma, seu computador estará inteiramente protegido e você terá acesso prioritário ao nosso suporte. Você poderá adiar o processo de registro por 15 dias caso esteja testando nosso produto ou 30 dias caso tenha uma licença paga. Para saber mais sobre sua conta, favor acessar: http://www.bitdefender.com/why_register.

Entre na Conta BitDefender já existente

Endereço E-mail:

Senha:

[Esqueceu a sua senha?](#)

Crie uma nova Conta BitDefender

Endereço E-mail:

Senha (6-16 caracteres):

Redigite a senha:

Nome:

Apelido:

País:

Registrar mais tarde (o registro é obrigatório)

Envie-me todas as mensagens da BitDefender

Envie-me só as mensagens mais importantes

Não me envie quaisquer mensagens



Criar uma Conta

Se não deseja criar uma conta BitDefender neste momento, seleccione **Saltar o registo** e clique em **Terminar**. De outra forma, actue de acordo com a sua presente situação:

- “Não tenho uma conta BitDefender” (p. 291)
- “Já tenho uma conta BitDefender” (p. 292)

Não tenho uma conta BitDefender

Para criar uma conta BitDefender, seleccione **Criar uma nova conta BitDefender** e fornecer a devida informação. Os dados que nos fornecer serão mantidos confidenciais.

- **E-mail** - insira o seu endereço de e-mail.
- **Senha** - insira uma Senha para a sua conta BitDefender. A senha deve ter pelo menos seis caracteres em tamanho.
- **Re-insira a senha** - insira novamente a senha previamente definida.



- **Nome** - insira o seu nome.
- **Apelido** - insira o seu apelido.
- **País** - selecciona o país onde reside.



Nota

Use o endereço de e-mail e a senha que nos forneceu para fazer log in na sua conta em <http://myaccount.bitdefender.com>.

Para criar com sucesso uma conta deverá em primeiro lugar ativar o seu endereço de e-mail. Verifique o seu endereço de e-mail e siga as instruções descrita no e-mail enviado para você pelo serviço de registo da BitDefender.

Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta. Escolha uma das seguintes opções:

- **Enviem-me todas as mensagens da BitDefender**
- **Enviem-me apenas as mensagens mais importantes**
- **Não me enviem quaisquer mensagens**

Clique em **Finalizar**.

Já tenho uma conta BitDefender

O BitDefender detectará automaticamente se já registou previamente uma conta BitDefender no seu computador. Neste caso, forneça a senha da sua conta.

Se já possui uma conta ativa, selecione **Entrar numa conta BitDefender existente** e forneça o endereço de e-mail e a senha da sua conta.

Se não se lembra da sua senha, clique em **Esqueceu a sua senha?** e siga as instruções.

Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta. Escolha uma das seguintes opções:

- **Enviem-me todas as mensagens da BitDefender**
- **Enviem-me apenas as mensagens mais importantes**
- **Não me enviem quaisquer mensagens**

Clique em **Finalizar**.



Ajuda



27. Suporte

Como um fabricante de valor agregado, a BitDefender garante um nível de serviço sem precedentes de suporte rápido e qualificado. O Centro de Suporte (cujo endereço é providenciado em baixo) mantém-se continuamente atualizado contra as ameaças mais recentes. É aqui onde obterá respostas e a informação necessária de uma forma rápida.

Com o BitDefender, tem sido sempre a nossa prioridade poupar aos nossos clientes tempo e dinheiro ao fornecer-lhes os produtos mais avançados aos preços mais económicos. Mais ainda, pensamos que um negócio de sucesso é baseado numa boa comunicação e num compromisso de excelência no suporte ao cliente.

Convidamo-lo desde já a colocar as suas questões em suporte@bitdefender.com.br a qualquer altura. Para uma resposta rápida, por favor inclua no seu e-mail o máximo de detalhes que consiga sobre seu BitDefender, seu sistema e uma descrição do problema tão completa e fiel quanto possível.

27.1. BitDefender Knowledge Base

O BitDefender Knowledge Base é um repositório on-line de informação sobre os produtos BitDefender. Ele armazena em formato facilitado relatórios sobre resultados de problemas técnicos e questionamentos sendo analisados pela equipe de suporte e desenvolvimento BitDefender, com artigos de informações gerais sobre prevenção de vírus, gerenciamento das soluções e explicações detalhadas.

O BitDefender Knowledge Base é aberto ao público e gratuito. Este rico meio de informação é outra forma de providenciar aos clientes BitDefender conhecimento técnico e visão necessária. Todas as requisições sobre problemas encontrados por clientes BitDefender eventualmente acabam chagando ao BitDefender Knowledge Base, como relatórios de bugfix e arquivos de ajuda.

O BitDefender Knowledge Base está disponível em <http://kb.bitdefender.com>.

27.2. Pedir Ajuda

27.2.1. Vá até ao Self-Service Web

Tem uma dúvida? Os nossos peritos em segurança estão disponíveis para o ajudar 24/7 via e-mail ou chat sem custos adicionais.



Por favor siga os seguintes links:

English

<http://www.bitdefender.com/site/KnowledgeBase/>

German

<http://www.bitdefender.com/de/KnowledgeBase/>

French

<http://www.bitdefender.com/fr/KnowledgeBase/>

Romanian

<http://www.bitdefender.com/ro/KnowledgeBase/>

Spanish

<http://www.bitdefender.com/es/KnowledgeBase/>

27.2.2. 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/>

27.3. Informação sobre contato

Comunicação eficiente é a chave para um negócio de sucesso. Nos últimos 10 anos a BITDEFENDER estabeleceu uma reputação indiscutível excedendo as expectativas dos clientes e parceiros, sempre buscando uma melhor comunicação. Por favor, não hesite em nos contactar sobre quaisquer assuntos ou dúvidas que você possa ter.



CD de Resgate BitDefender



28. Sumário

BitDefender Internet Security 2009 dá-lhe acesso a CD de arranque (Cd de Emergência BitDefender) capaz de analisar e desinfetar todos os discos duros antes de o seu sistema operacional iniciar.

Você deve usar o CD de Resgate BitDefender a qualquer momento que o seu sistema operacional não estiver funcionando corretamente por infecção de vírus. Isto normalmente acontece quando você não usa um produto antivírus.

A atualização das assinaturas de vírus é feita automaticamente, sem a intervenção do usuário quando você executa o CD de Resgate BitDefender.

O CD de Emergência BitDefender é uma distribuição do Knoppix recompilada por BitDefender, que integra a mais recente solução BitDefender de segurança para Linux dentro do CD ao Vivo GNU/Linux Knoppix, que lhe oferece uma protecção instantânea de antivírus que é capaz de analisar e desinfetar discos duros existentes (incluindo partições Windows NTFS. Ao mesmo tempo, o CD de Emergência BitDefender pode ser usado para recuperar a sua preciosa informação quando não consegue arrancar com o Windows.



Nota

O CD de Emergência BitDefender pode ser descarregado a partir deste local na net:
http://download.bitdefender.com/rescue_cd/

28.1. Requisitos de Sistema

Antes de arrancar com o CD de Emergência BitDefender, deve em primeiro lugar verificar se o seu sistema possui os seguintes requisitos.

Processador

Compatível com x86, mínimo de 166 MHz. Um processador de geração i686, de 800MHz, seria uma melhor escolha mínima.

Memória

512 MB de memória RAM (1 GB recomendado)

CD-ROM

O CD de Emergência BitDefender, é executado a partir do CD-ROM, logo um CD-ROM e uma BIOS capaz de arrancar a partir do mesmo são necessários.



Conexão a Internet

Apesar de o CD de Emergência BitDefender se executar sem ligação à Internet, os processos de actualização requerem uma ligação HTTP activa, mesmo que seja através de um servidor proxy. Logo, para ter uma protecção actualizada, a Ligação à Internet tem de EXISTIR.

Resolução gráfica

Placa gráfica Standard SVGA compatível.

28.2. Software incluído

O CD de Resgate BitDefender inclui os seguintes pacotes de programas.

Xedit

Este é um arquivo de um editor de texto.

Vim

Este é um poderoso arquivo de um editor de texto, contendo uma sintaxe highlighting, uma GUI e muito mais. Para mais informação consulte a [página web da Vim](#).

Xcalc

Este é uma calculadora.

RoxFiler

RoxFiler é um rápido e poderoso gestor de arquivos gráficos.

Para mais informação, consultar a [página internet da RoxFiler](#).

MidnightCommander

GNU Midnight Commander (mc) um gestor de arquivos em modo de texto.

Para mais informação, consultar [a página internet da MC](#).

Pstree

Pstree mostra processos que estão a decorrer.

Top

Top mostra as tarefas do Linux.

Xkill

Xkill mata um cliente com os seus recursos X.



Partition Image

Partition Image ajuda-o a guardar partições em arquivos de sistema EXT2, Reiserfs, NTFS, HPFS, FAT16, e FAT32 para um arquivos de imagem. Este programa pode ser útil para propósitos de backup.

Para mais informação, consulte a [página web da Partimage](#).

GtkRecover

GtkRecover é uma versão da GTK da recuperação do programa de consola. Ajuda-o a recuperar um arquivo.

Para mais informação, consulte a [página web da GtkRecover](#).

ChkRootKit

ChkRootKit é uma ferramenta que o ajuda a analisar o seu computador em busca de rootkits.

Para mais informação, consulte a [página web do ChkRootKit](#).

Nessus Network Scanner

Nessus um analisador remoto de segurança para Linux, Solaris, FreeBSD, e Mac OS X.

Para mais informação, consulte a [página web do Nessus](#).

Iptraf

Iptraf é um Software de Monitorização de Rede por IP.

Para mais informação, consulte a [página web do Iptraf](#).

Iftop

Iftop mostra num interface o grau de utilização de banda.

Para mais informação, consulte a [página web do Iftop](#).

MTR

MTR é uma ferramenta de diagnóstico de rede.

Para mais informação, consulte a [página web da MTR](#).

PPPStatus

PPPStatus mostra as estatísticas acerca do tráfego TCP/IP de entrada e saída.

Para mais informação, consulte a [página web da PPPStatus](#).

Wavemon

Wavemon uma aplicação de monitorização para dispositivos de redes wireless.

Para mais informação, consulte a [página web da Wavemon](#).

**USBView**

USBView mostra informação acerca de dispositivos ligados ao USB bus.

Para mais informação, consulte a [página web da USBView](#).

Pppconfig

Pppconfig ajuda-o a definir automaticamente uma ligação por dial up ppp.

DSL/PPPoE

DSL/PPPoE configura uma ligação PPPoE (ADSL).

I810rotate

I810rotate toggles o video output em i810 hardware usando o i810switch(1).

Para mais informação, consulte a [página internet da I810rotate](#).

Mutt

Mutt é um poderoso cliente de e-mail MIME baseado em texto.

Para mais informação, consulte a [página internet da Mutt](#).

Mozilla Firefox

Mozilla Firefox é um browser de internet bastante conhecido.

Para mais informação, consulte a [página internet da Mozilla Firefox](#).

Elinks

Elinks um browser de internet em modo de texto.

Para mais informação, consulte a [página internet da Elinks](#).



29. Como Usar o CD de Emergência BitDefender

Este capítulo contém informação sobre como começar e parar o CD de Emergência BitDefender, analisar o seu computador em busca de malware como também guardar dados do seu comprometido PC Windows para um dispositivo amovível. No entanto ao usar as aplicações que vem com o CD, pode fazer muita tarefas cuja descrição vai muito para além deste manual de usuário.

29.1. Iniciar CD de Resgate BitDefender

Para iniciar o CD, configure a BIOS do seu computador para iniciar diretamente do CD, coloque o CD no drive e reinicie o computador. Tenha certeza que o seu computador pode iniciar do CD.

Espere até a próxima tela aparecer e siga as instruções na tela para iniciar o CD de Resgate BitDefender.



Nota

Selecione a linguagem que deseja usar para o CD de Emergência a partir da lista disponível.



Boot Splash Screen



A actualização das assinaturas dos vírus é feita automaticamente, cada vez que arranca com o Cd de Emergência do BitDefender. Isto pode demorar um pouco.

Quando o processo finalizar você verá o próximo desktop. Você pode agora usar o CD de Resgate BitDefender.



O Desktop

29.2. Parar o CD de Resgate BitDefender

Pode desligar em segurança o seu computador ao seleccionar **Sair** a partir do menu do CD de Emergência BitDefender (clique botão-direito para o abrir) ou ao emitir o comando **halt** num terminal.



Escolha "EXIT"

Quando o CD de Emergência BitDefender fechar com sucesso todos os programas mostra-lhe uma tela como a imagem seguinte. Pode remover o CD de forma a arrancar pelo seu disco rígido. Agora é OK desligar o seu computador ou reiniciá-lo.



```
X Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Killing processes with signal 15: (init) (aufsd) (aufsd) (aufsd) (aufsd)
ald) (hald-addon-acpi) (hald-addon-keyb) (ksoftirqd/0) (logsave) (inetd)
s/0) (khelper) (kthread) (ata/0) (ata_aux) (kseriod) (kpsmoused) (ksusp
) (aio/0) Done.
Waiting for processes to finish.....
Killing processes with signal 9: (init) (aufsd) (aufsd) (aufsd) (aufsd)
(kblockd/0) (kacpid) (knoppix-halt) (events/0) (khelper) (kthread) (ata/
d) (khpsbpkt) (pdflush) (pdflush) (kswapd0) (aio/0) Done.
Waiting for processes to finish.....
Syncing/Unmounting filesystems: /sys/fs/fuse/connections /UNIONFS/lib/in
Turning off swap... Done.
Unmounting remaining file systems.
rootfs unmounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return [auto 2 minutes].
```

Espere por esta mensagem enquanto estiver a desligar

29.3. Como executo uma verificação antivírus?

Um assistente aparecerá quando o processo de arranque terminar e permite-lhe analisar totalmente o seu computador. Tudo o que tem de fazer é clicar no botão **Iniciar**.



Nota

Se a resolução do seu ecrã não for suficiente, ser-lhe-á solicitado que inicie a análise em modo de texto.

Siga o processo guiado de três passos para completar o processo de análise.

1. Pode ver o estado da análise e as estatísticas (velocidade da análise, tempo decorrido, número de objectos analisados / infectados / suspeitos / ocultos e outras).



Nota

O processo de análise pode demorar algum tempo, dependendo da complexidade da mesma.

2. Pode ver o número de incidências que afectam o seu sistema.

As incidências são mostradas em grupos. Clique na caixa com "+" para abrir um grupo ou na caixa com "-" para fechar um grupo.



Pode escolher uma acção geral a ser tomada para cada grupo de incidências ou pode seleccionar separar as acções para cada incidência.

3. Pode ver o sumário dos resultados.

Se deseja analisar uma determinada directoria apenas, faça o seguinte:

Navegue pelas pastas, clique com o botão direito em um arquivo ou pasta e selecione **Enviar**. Então escolha **BitDefender Scanner**.

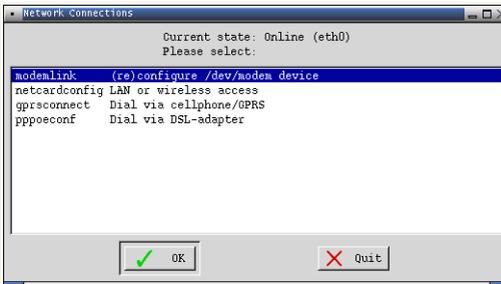
Ou você pode digitar o próximo comando no terminal. O **BitDefender Antivirus Scanner** irá começar pelo arquivo ou pasta seleccionada como local padrão de verificação.

```
# bdscan /path/to/scan/
```

29.4. Como posso configurar a Ligação à Internet?

Se você estiver em uma rede DHCP e você tiver uma placa de rede ethernet, uma conexão de Internet já deveria estar detectada e configurada. Para uma configuração manual, siga os próximos passos.

1. Duplo Clique sobre o atalho das Ligações de Rede no Ambiente de Trabalho. A seguinte janela irá aparecer:



Ligações de Rede

2. Selecciono o tipo de ligação que está a usar e clique em OK.



Conexão	Descrição
modemlink	Selecione este tipo de ligação quando está a usar um modem e uma ligação telefónica para aceder à Internet.
netcardconfig	Selecione este tipo de ligação quando está a usar uma rede de área local (LAN) para aceder à Internet. É também utilizada para ligações sem fios.
gprsconnect	Selecione este tipo de ligação quando está a usar uma rede de telemóvel com o protocolo GPRS (General Packet Radio Service). Também pode estar a usar um modem GPRS em vez de um telemóvel.
pppoeconf	Selecione este tipo de ligação quando estiver a usar um modem DSL (Digital Subscriber Line) para aceder à Internet.

3. Siga as instruções na tela. Se você não tiver certeza do que está fazendo, contacte o administrador da rede para detalhes.



Importante

Tenha em mente que apenas activou o modem ao seleccionar as opções acima mencionadas. Para configurar a ligação à rede siga estes passos.

1. Clique botão direito do mouse sobre o Ambiente de Trabalho. O menu contextual do CD de Emergência do BitDefender aparecerá.
2. Selecione **Terminal (como raiz)**.
3. Insira os seguintes comandos:

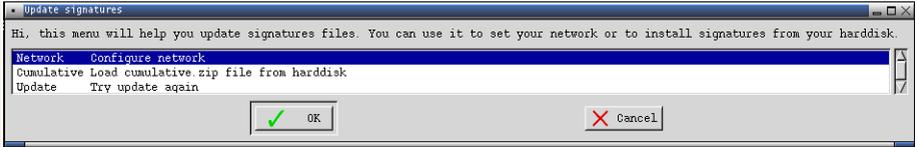
```
# pppconfig
```

4. Siga as instruções na tela. Se você não tiver certeza do que está fazendo, contacte o administrador da rede para detalhes.

29.5. Como eu posso atualizar o BitDefender?

A actualização das assinaturas dos vírus é feita automaticamente, cada vez que arranca com o Cd de Emergência do BitDefender. Mas se saltar este passo, então siga os passos seguinte para actualizar o BitDefender.

1. Duplo clique no atalho da Actualização de assinaturas no Ambiente de Trabalho. A seguinte janela irá aparecer.



Actualização de Assinaturas

2. Faça uma das coisas seguintes:
 - Selecione **Cumulativa** para instalar as assinaturas guardadas no seu disco rígido devido a ter descarregado no seu computador o arquivo `cumulative.zip`.
 - Selecione **Actualização** para ligar-se imediatamente à internet e descarregar as últimas assinaturas de vírus.
3. Clique em **OK**.

29.5.1. Como posso actualizar o BitDefender através de um proxy?

Se existe um servidor proxy entre o vosso computador e a internet, algumas configurações têm de ser feitas de forma a poder actualizar o seu BitDefender.

Para actualizar o BitDefender através de um proxy, siga os seguintes passos:

1. Clique botão direito do mouse sobre o Ambiente de Trabalho. O menu contextual do CD de Emergência do BitDefender aparecerá.
2. Seleccione **Terminal (como raiz)**.
3. Digite o comando: `cd /ramdisk/BitDefender-scanner/etc`.
4. Digite o comando: `mcedit bdscan.conf` para editar este arquivo usando o GNU Midnight Commander (`mc`).
5. Uncomment a seguinte linha: `#HttpProxy =` (apenas apague o sinal `#`) e especifique o domínio, nome, senha e a porta do servidor proxy. Por exemplo, a linha respectiva deverá parecer-se com o seguinte:
`HttpProxy = myuser:mypassword@proxy.company.com:8080`
6. Prima **F2** para guardar o arquivo atual, confirme o guardar, e depois prima **F10** para o fechar.
7. Digite o comando: `bdscan update`.



29.6. Como posso salvar os meus dados?

vamos partir do princípio que não consegue arrancar o seu PC em Windows PC devido a incidências desconhecidas. Ao mesmo tempo, você necessita desesperadamente de aceder a alguma informação importante do seu computador. Eis aqui uma situação em que o CD de Emergência BitDefender se revela extremamente útil.

Para guardar os seus dados do computador para um dispositivo amovível, tal como um stick de memória USB, siga os seguintes passos:

1. Coloque o CD de Emergência BitDefender na drive de CDs, e o stick de memória na entrada USB e depois reinicie o computador.



Nota

Se conectar o stick de memória mais tarde, tem de montar o dispositivo amovível seguindo os seguintes passos:

- a. Faça duplo-clique com o rato sobre o atalho do Terminal Emulator no Ambiente de Trabalho.
- b. Insira o seguinte comando:

```
# mount /media/sdb1
```

Lembre-se que dependendo da configuração do seu computador poderá ser `sda1` em vez de `sdb1`.

2. Espere que o CD de Emergência BitDefender termine de arrancar o PC. A seguinte janela irá aparecer.



Ecrã de Ambiente de Trabalho

3. Faça duplo clique sobre a partição onde os dados que deseja salvar se encontram (ex. [sda3]).



Nota

Quando está a trabalhar com o CD de Emergência BitDefender, estará a lidar com nomes de partições baseado em Linux. Assim, [sda1] provavelmente corresponderá à partição Windows (C:), [sda3] a (F:), e [sdb1] ao stick de memória.



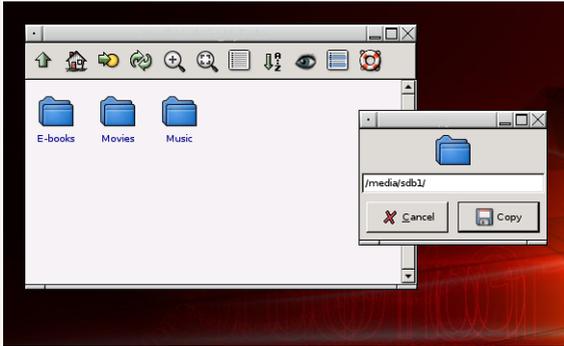
Importante

Se o computador não for desligado correctamente, é possível que certas partições não sejam montadas automaticamente. Para montar uma partição siga estes passos.

- a. Faça duplo-clique com o rato sobre o atalho do Terminal Emulator no Ambiente de Trabalho.
- b. Insira o seguinte comando:

```
# mount /media/partition_name
```

4. Explore as suas pastas e abra a directoria que deseja. Por exemplo, Meus Dados que contém as sub-directorias Filmes, Música e E-books .
5. Clique botão direito do mouse sobre o directorio desejado e selecione **Copiar**. A seguinte janela irá aparecer:



Guardar Dados

6. Insira `/media/sdb1/` na correspondente caixa de texto e clique em **Copiar**.
Lembre-se que dependendo da configuração do seu computador poderá ser `sda1` em vez de `sdb1`.



Glossário

ActiveX

ActiveX é um modelo para escrever programas para que outros programas e seus sistemas operacionais possam buscá-los. A tecnologia ActiveX é usada com o Microsoft Internet Explorer para fazer páginas da Web interativas que se parecem e se comportam como programas de computador, melhor que páginas estáticas. Com o ActiveX, usuários podem perguntar ou responder questões, apertar botões e interagir de outras formas com a página. Controles ActiveX são também escritos usando Visual Basic.

O ActiveX é notável para uma completa falta de controles de segurança; especialistas em segurança de computador desencorajam seu uso pela Internet.

Adware

O Adware é sempre combinado com um programa host sem custo enquanto o usuário concordar em aceitar o adware. Não existem implicações neste tipo de instalação, pois o usuário concordou com o propósito do aplicativo.

No entanto, propagandas do tipo “pop-up” podem se tornar uma inconveniência, e em alguns casos afetar a performance do seu sistema. Além disso, a informação que alguns destes programas coleta pode causar problemas de privacidade para usuários que não estão totalmente cientes do funcionamento do programa.

Arquivo

Um disco, fita ou diretório que contém arquivos que podem ter sido gravados como backup.

Um arquivo que contém um ou mais arquivos em formato compactado.

Backdoor

Um furo na segurança do sistema deixado deliberadamente pelos desenvolvedores ou mantenedores. A motivação para tais furos não é sempre sinistra, alguns sistemas operacionais, por exemplo, saem com contas privilegiadas para uso em campo para serviço dos técnicos ou programa de manutenção dos programadores do fabricante.

Setor de boot

O setor de boot é um setor no começo de cada disco que identifica a arquitetura do disco (tamanho do setor, tamanho do cluster, e assim por diante). Para inicializar os discos, o setor de boot também um programa que carrega o sistema operacional.



Vírus de boot

Um vírus que infecta o setor de boot do disco rígido ou de um disquete. Uma tentativa de inicialização com um disquete infectado com vírus de boot fará com que o vírus se torne ativo na memória. Toda vez que você reiniciar seu sistema daquele ponto em diante, você terá um vírus ativo na memória.

Navegador

Termo simplificado para navegador da web, um programa utilizado para localizar e exibir páginas da Internet. Os dois mais populares são Netscape Navigator e Microsoft Internet Explorer. Ambos são navegadores gráficos o que significa que podem exibir tanto gráficos como texto. Em adição, os navegadores mais modernos podem apresentar informações multimídia, como som e vídeo, através de plugins para alguns formatos.

Linha de comando

Na interface de linha de comando, os usuários digitam os comando em um espaço fornecido diretamente na tela usando comandos da linguagem.

Cookie

Dentro da indústria da Internet, os cookies são descritos como pequenos arquivos de texto que contém informações sobre computadores individuais que podem ser analisados e usados pelos anunciantes para rastrear gostos e interesses on-line. Nesse reino, a tecnologia de cookies está sendo desenvolvida ainda e a intenção é direcionar os anúncios diretamente aos seus interesses. É uma espada de dois gumes para muitos porque por um lado é eficiente e pertinente porque só vê anúncios que interessam a você. E por outro lado, envolve “rastrear” e “seguir” a onde você vai e onde está clicando. Compreensível assim, existe um debate sobre a privacidade e muitas pessoas que se sentem ofendidas pelo fato de serem observados com um número SKU (você sabe, o código de barras na parte traseira dos pacotes que são lidos na saída do supermercado). Embora esse ponto de vista possa ser extremo, em alguns casos é exato.

Unidade de disco

É uma máquina que lê e escreve dados em um disco.

Uma unidade de disco rígido lê e escreve em um disco rígido.

Uma unidade de disquete acessa disquetes.

Os discos rígidos podem ser internos (armazenado dentro do computador) ou externos (armazenado em uma caixa separada que está conectada ao computador).



Download

Copiar dados (geralmente um arquivo inteiro) de uma fonte principal para um periférico. O termo é muitas vezes usado para descrever o processo de copiar um arquivo de um serviço on-line para seu próprio computador. Download também pode se referir a copiar um arquivo de um servidor de rede para um computador na rede.

E-mail

Correio eletrônico. Um serviço que envia mensagens para computadores em redes locais ou mundiais.

Eventos

Uma ação ou ocorrência detectada por um programa. Eventos podem ser ações de usuários, tais como clicar com botão do mouse ou pressionar uma tecla, ou ocorrências do sistema, como sem memória.

Falso positivo

Ocorre quando a verificação identifica um arquivo infectado quando de fato não está.

Extensão do arquivo

É a parte do arquivo, após o ponto final, indica o tipo de dados que estão armazenados no arquivo.

Muitos sistemas operacionais usam extensões de arquivos, ex. Unix, VMS, MS-DOS. Eles são usualmente de uma a três letras e / ou números (alguns sistemas operacionais antigos não suportam mais que três). Exemplos: ".c" para códigos em C, ".ps" para PostScript, ".txt" para texto.

Heurística

Um método baseado em regras para identificar novos vírus. Esse método de verificação não se baseia em definições de vírus específicas. A vantagem da verificação heurística é que ela não é enganada por uma nova variante do vírus. Entretanto, ela pode relatar um código suspeito em um programa normal, gerando assim um chamado "falso positivo".

IP

Um protocolo roteável no conjunto do protocolo TCP/IP que é responsável pelo endereçamento IP, roteamento, e fragmentação e montagem dos pacotes IP.

Java applet

Um programa em Java que é projetado para ser executado somente em uma página web. Para usar um aplicativo em uma página web, você deve especificar o nome do aplicativo e o tamanho (comprimento e largura em pixels) que o aplicativo pode utilizar. Quando a página da web é acessada, o navegador



descarrega-a de um servidor e executa na máquina do usuário (o cliente). Os aplicativos diferem dos programas em que eles são comandados por um protocolo estrito de segurança.

Por exemplo, mesmo um aplicativo funcione em um cliente, eles não podem ler ou escrever dados na máquina do cliente. Adicionalmente, os aplicativos são mais restringidos de modo que só podem ler e escrever dados nos domínios aos quais servem.

Vírus de macro

Um tipo de vírus de computador que é codificado como uma macro dentro de um documento. Muitas aplicações, como Microsoft Word e Excel, suportam poderosa linguagem de macro.

Essas aplicações permitem a você colocar uma macro em um documento, e mandam a macro ser executada cada vez que o documento é aberto.

Cliente de e-mail

É uma aplicação que permite a você enviar e receber e-mails.

Memória

São áreas internas de armazenamento do computador. O termo memória identifica o armazenamento de dados que vem em forma de chips. Todo computador vem com uma certa quantidade de memória física, geralmente referida com memória RAM.

Não heurística

Esse método de verificação confia em definições de vírus específicas. A vantagem da verificação não heurística é que ela não pode ser enganada por algo que parece um vírus, e não gera falsos alarmes.

Programas compactados

Um arquivo em formato compactado. Muitos sistemas operacionais e programas contêm comando que permitem a você compactar um arquivo de modo que ocupe menos memória. Por exemplo: suponha que você tenha um texto que contém dez caracteres de espaço consecutivos. Normalmente, isso requereria dez bytes de armazenamento.

Entretanto, um programa que compacta arquivos substituiria os caracteres de espaço por caractere especial série-espaço seguido do número de espaços que estão sendo substituídos. Esta é apenas uma técnica de compactação, existem muitas outras.



Caminho

As direções exatas de um arquivo em um computador. Estas direções são descritos geralmente por meio do sistema de arquivamento hierárquico de cima para baixo.

A rota entre dois pontos quaisquer, com os canais de comunicação entre dois computadores.

Phishing

O ato de enviar e-mail a um usuário declarando falsamente ser uma empresa legítima em uma tentativa de enganar o usuário a entregar informações que serão usadas para roubo de identidade. O e-mail direciona o usuário a uma página web onde é perguntado a fornecer informação pessoal, tais como senhas, cartão de crédito, cadastros e contas em bancos, que a empresa legítima em questão já possui. A página web, no entanto, é falsa e existe apenas para roubar informação do usuário.

Vírus polimórfico

Um vírus que muda sua forma cada vez que um arquivo é infectado. Como não têm nenhum padrão binário consistente, tais vírus são duros de identificar.

Porta

Uma interface no computador na qual você pode conectar um dispositivo. Computadores pessoais possuem vários tipos de portas. Internamente, existem vários tipos de portas conectando unidades de disco, monitores e teclados. Externamente, os computadores pessoais possuem portas conectando modems, impressoras, mouse e outros dispositivos periféricos.

Em redes TCP/IP e UDP, um ponto final a uma conexão lógica. A número da porta identifica que tipo de porta é. Por exemplo, porta 80 é usada para tráfego HTTP.

Arquivo de relatório

Um arquivo que lista as ações que ocorreram. Por exemplo BitDefender mantém um arquivo de relatório com uma lista dos caminhos verificados, as pastas, o número de arquivos e arquivos compactados verificados, quantos arquivos infectados e suspeitos foram encontrados.

Rootkit

Um rootkit é um pacote de ferramentas de software que proporcionam um nível de acesso de administrador a um sistema. O termo foi usado em primeiro lugar nos sistemas operativos UNIX e referia-se a ferramentas recompiladas que proporcionavam aos intrusos direitos de administração, permitindo-lhes ocultar a sua presença de forma a não serem vistos pelos administradores do sistema.



O papel principal dos rootkits é ocultar processos, arquivos, logins e registros. Eles também podem interceptar dados dos terminais, ligações de rede ou periféricos, se eles incorporarem o software para tal.

Os rootkits não são maliciosos por natureza. Por exemplo, os sistemas e mesmo algumas aplicações ocultam arquivos críticos usando rootkits. No entanto, eles são essencialmente utilizados para ocultar malware ou para esconder a presença de um intruso no sistema. Quando combinados com o malware, os rootkits são uma grande ameaça à integridade e segurança de um sistema. Eles podem monitorizar tráfego, criar backdoors no sistema, alterar arquivos e relatórios e evitam ser detectados.

Script

Outro termo para um arquivo de macro ou arquivo de comandos, um script é uma lista de comandos que podem ser executados sem a interação do usuário.

Spam

Lixo eletrônico em forma de mensagens. Normalmente conhecido como e-mail não solicitado.

Spyware

Qualquer software que coleta informação do usuário através da conexão de Internet sem o seu consentimento, normalmente para propósitos de propaganda. Aplicativos spyware são tipicamente distribuídos de forma oculta juntamente com programas freeware ou shareware que podem ser baixados da Internet; no entanto, deve ser notado que a maioria dos programas shareware e freeware não apresentam spyware. Uma vez instalado, o spyware monitora a atividade do usuário na Internet e transmite essa informação de forma oculta para outra pessoa. O spyware pode coletar também endereços de e-mail e até mesmo número de cartões de crédito e senhas.

A similaridade do spyware com o cavalo de tróia é que o usuário instala algo que não deseja instalando algum outro produto. Um modo comum de se tornar uma vítima de spyware é baixar alguns programas de compartilhamento de arquivos (peer-to-peer) que estão disponíveis hoje em dia.

Colocando de lado as questões de ética e privacidade, o spyware prejudica o usuário consumindo memória do computador e conexão com a Internet quando manda a informação de volta a sua base usando a conexão de Internet do usuário. Porque o spyware usa a memória e os recursos do sistema, os aplicativos sendo executados podem levar o sistema ao colapso ou instabilidade geral.



Itens para inicializar

Qualquer arquivo colocado nessa pasta será executado quando o computador iniciar. Por exemplo uma tela de boas-vindas, um arquivo de som, um aviso de calendário ou uma aplicação pode ser um item para inicializar.

Barra de tarefas

Introduzido com o Windows 95, a área de notificação é localizada na barra de tarefas do Windows (geralmente na parte inferior próxima ao relógio) e contém miniaturas de ícones para fácil acesso de funções do sistema como fax, modem, volume, e outros. Dois cliques ou um clique como o botão direito do mouse para ver ou acessar detalhes dos controles.

TCP/IP

Transmission Control Protocol/Internet Protocol - Protocolo de controle de transmissão / protocolo da Internet. Um conjunto de protocolos largamente utilizados na Internet que fornece comunicação através de redes de computadores interconectadas com diversas arquiteturas de hardware e vários sistemas. O TCP/IP inclui padrões de como os computadores comunicam e convenções para conexões da rede e roteamento de tráfego.

Trojan

Um programa destrutivo que oculta uma aplicação benigna. Ao contrário do vírus, um cavalo de tróia não se replica mas pode ser muito destrutivo. Uma dos tipos mais incidentes de cavalos de tróia é um programa que diz se livras dos vírus do seu computador, mas ao invés disso ele introduz vírus em seu computador.

O termo vem da estória de Ilíada de Homero, na qual os gregos deram um cavalo de madeira gigante seus inimigos, os Troianos como uma oferta de paz. Mas depois dos troianos arrastarem o cavalo para dentro dos muros da cidade, os soldados Gregos saíram furtivamente da barriga do cavalo e abriram os portões da cidade, permitindo que seus compatriotas derrubassem e capturassem Tróia.

Atualização

Uma nova versão do programa ou driver do produto projetado para substituir uma versão antiga do mesmo produto. Além disso, as rotinas de instalação verificam se uma versão mais antiga está instalada no seu computador, caso contrário, você não pode instalar.

O BitDefender possui um módulo de atualização que permita a você verificar manualmente por atualizações ou deixa que ele automaticamente atualize o produto.



Virus

Um programa ou uma parte do código que é carregado no seu computador sem o seu conhecimento e se executa contra a sua vontade. A maioria dos vírus pode também se duplicar. Todos os computadores são feitos pelo homem. Um simples vírus pode fazer uma cópia dele mesmo repetidamente é fácil de se produzir. Mesmo um simples vírus é perigoso porque pode rapidamente usar toda memória disponível a fazer os sistema parar. O tipo de vírus mais perigoso é aquele que é capaz de transmitir-se através de uma rede ou contornando sistemas de segurança.

Definições de vírus

É um padrão binário de vírus, utilizado pelo programa antivírus para detectar e eliminar os vírus.

Worm

Um programa que se propaga pela rede, se reproduzindo enquanto isso. Ele não pode se anexar a outros programas.