Bitdefender®

TOTAL SECURITY 2018

MANUAL DO UTILIZADOR

Bitdefender Total Security 2018
Manual do Utilizador

Editado 06/08/2018

Copyright© 2018 Bitdefender

Aviso Legal

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

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

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

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

Bitdefender

Índice

Sobre este guia x
1. Propósito e público-alvo x
2. Como utilizar este guia x

Total Security para PC 1

1. Instalação 2
1.1. A preparar a instalação 2
1.2. Requisitos do sistema 2
1.3. Instalação do seu produto Bitdefender 4

2. Introdução 11
2.1. Os básicos 11
2.1.1. A reparar problemas 13
2.1.2. Notificações 15
2.1.3. Autopilot 16
2.1.4. Perfis 17
2.1.5. Definições de proteção da palavra-passe de Bitdefender 18
2.1.6. Relatórios anónimos de utilização 19
2.1.7. Notificações de ofertas especiais 19
2.2. Interface Bitdefender 19
2.2.1. Ícone na área de notificação 20
2.2.2. Janela Principal 22
2.2.3. As secções do Bitdefender 25
2.2.4. Dispositivo de Segurança 30
2.2.5. Actividade 32
2.3. Bitdefender Central 35
2.3.1. As minhas subscrições 36
2.3.2. Meus dispositivos 38
2.3.3. Actividade 41
2.3.4. Minha Conta 42
2.3.5. Notificações 43
2.4. Mantenha o seu Bitdefender atualizado. 43
2.4.1. Verifique se o Bitdefender está atualizado 44
2.4.2. A efetuar uma atualização 44
2.4.3. Ligar ou desligar a atualização automática 45
2.4.4. Ajuste das configurações da atualização 45
2.4.5. Atualizações contínuas 46

3. Como 48
3.1. Instalação 48
3.1.1. Como instalo o Bitdefender num segundo computador? 48
3.1.2. Como posso reinstalar Bitdefender? 48
3.1.3. Onde posso transferir o meu produto Bitdefender? 49
3.1.4. Como é que posso alterar o idioma do meu produto Bitdefender? 50
3.1.5. Como utilizo a minha subscrição do Bitdefender após uma atualização do Windows? 52
3.1.6. Como posso atualizar para a mais recente versão de Bitdefender? 54

3.2. Assinaturas 55
3.2.1. Como é que ativo a minha subscrição do Bitdefender através da chave de licença? 55
3.3. Bitdefender Central 56
3.3.1. Como é que é inicio sessão na Bitdefender Central utilizando outra conta online? 56
3.3.2. Como é que desativo as mensagens de ajuda da Bitdefender Central? . . . 56
3.3.3. Esqueci-me da palavra-passe que defini para a minha conta Bitdefender. Como é que a reponho? 57
3.3.4. Como posso gerir os inícios de sessão associados à minha conta do Bitdefender? 58
3.4. A analisar com Bitdefender 58
3.4.1. Como posso analisar um ficheiro ou uma pasta? 58
3.4.2. Como posso analisar o seu sistema? 59
3.4.3. Como programar uma verificação? 59
3.4.4. Como posso criar uma tarefa de análise personalizada? 60
3.4.5. Como posso excluir uma pasta da análise? 60
3.4.6. O que fazer se o Bitdefender identificar um ficheiro limpo como infectado? 61
3.4.7. Como posso saber que ameaças o Bitdefender detetou? 62
3.5. Consultor Parental 63
3.5.1. Como posso proteger os meus filhos de ameaças online? 63
3.5.2. Como bloqueio o acesso do meu filho a um website? 64
3.5.3. Como impeço o meu filho de jogar um jogo? 65
3.5.4. Como previno que os meus filhos entrem em contato com pessoas desconhecidas? 65
3.5.5. Como posso definir um local como seguro ou restrito para o meu filho? 67
3.5.6. Como posso bloquear o acesso do meu filho a dispositivos atribuídos durante os dias de escola? 69
3.5.7. Como posso bloquear o acesso do meu filho a dispositivos atribuídos durante as noites de escola? 68
3.5.8. Como posso bloquear o acesso do meu filho a dispositivos atribuídos durante os fins de semana? 69
3.5.9. Como remover um perfil de criança 70
3.6. Protecção de Privacidade 70
3.6.1. Como posso ter a certeza de que a minha transação online é segura? 70
3.6.2. O que posso fazer se o meu dispositivo tiver sido roubado? 70
3.6.3. Como posso usar os cofres de ficheiros? 71
3.6.4. Como removo um ficheiro permanentemente com o Bitdefender? 73
3.6.5. Como protejo a minha câmara Web contra hacking? 73
3.7. Ferramentas de Otimização 74
3.7.1. Como posso usar melhorar o desempenho do meu sistema? 74
3.7.2. Como posso melhorar o tempo de arranque do meu sistema? 75
3.8. Informações Úteis 76
3.8.1. Como posso testar a minha solução de segurança? 76
3.8.2. Como posso remover o Bitdefender? 76
3.8.3. Como removo o Bitdefender VPN? 77
3.8.4. Como desligo automaticamente o meu computador após terminar a análise? 78

3.8.5. Como posso configurar Bitdefender para usar um proxy de ligação à Internet? ... 79
3.8.6. Estou a utilizar uma versão de 32 ou 64 Bit do Windows? ... 80
3.8.7. Como posso mostrar objetos ocultos no Windows? ... 81
3.8.8. Como posso remover outras soluções de segurança? ... 82
3.8.9. Como posso reiniciar no Modo de Segurança? ... 83

4. Gerir a sua segurança ... 85
4.1. Proteção Antivírus ... 85
4.1.1. Análise no acesso (proteção em tempo real) ... 86
4.1.2. Verificação por ordem ... 91
4.1.3. Análise automática de média removíveis ... 100
4.1.4. Analisar ficheiro hosts ... 102
4.1.5. Configurar exceções da análise ... 102
4.1.6. Gerir ficheiros da quarentena ... 105
4.2. Advanced Threat Defense ... 107
4.3. Proteção da Internet ... 109
4.4. Antispam ... 111
4.4.1. Compreender o Antispam ... 112
4.4.2. Ligar ou desligar a proteção antispam ... 113
4.4.3. Utilizar a barra de ferramentas Antispam na janela do seu cliente de email ... 113
4.4.4. Configurar a Lista de Amigos ... 116
4.4.5. Configurar a lista de Spammers ... 117
4.4.6. A configurar os filtros locais Antispam ... 119
4.4.7. Configurar as definições da nuvem ... 119
4.5. Firewall ... 120
4.5.1. A gerir regras de aplicações ... 121
4.5.2. Gerir definições da ligação ... 124
4.5.3. Configurar definições avançadas ... 124
4.6. Vulnerabilidade ... 125
4.6.1. Procurar vulnerabilidades no seu sistema ... 126
4.6.2. Usar monitorização de vulnerabilidade automática ... 127
4.6.3. Consultor de Segurança Wi-Fi ... 130
4.7. Proteção da Webcam ... 133
4.8. Safe Files ... 135
4.8.1. Ativar ou desativar Safe Files ... 136
4.8.2. Proteja os seus ficheiros pessoais contra ataques de ransomwares ... 137
4.8.3. A configurar o acesso de aplicações ... 137
4.8.4. Proteção no arranque ... 138
4.9. Encriptação de ficheiro ... 138
4.10. Proteção do Gestor de palavras-passe para as suas credenciais ... 144
4.11. VPN ... 151
4.12. Segurança Safepay para transações online ... 154
4.13. Proteção de dados ... 158
4.14. Consultor Parental ... 159
4.14.1. A aceder ao Consultor Parental - OS MEUS FILHOS ... 160
4.14.2. Adicionar o perfil do seu filho ... 161
4.14.3. Configurar perfis do Consultor Parental ... 166
4.15. Dispositivo Anti-Roubo ... 172

4.16. Bitdefender USB Immunizer 174
5. Otimização do sistema 176
5.1. Ferramentas 176
5.1.1. A otimizar a velocidade do seu sistema com apenas um clique 176
5.1.2. A otimizar o tempo de arranque do seu PC. 177
5.1.3. A otimizar o seu disco 178
5.2. Perfis 180
5.2.1. Perfil Trabalho 181
5.2.2. Perfil de Filme 182
5.2.3. Perfil de Jogo 184
5.2.4. Perfil Wi-Fi Público 185
5.2.5. Perfil do Modo de Bateria 185
5.2.6. Otimização em tempo real 186
6. Solução de problemas 188
6.1. Resolver incidências comuns 188
6.1.1. O meu sistema parece estar lento 188
6.1.2. A análise não inicia 190
6.1.3. Já não posso utilizar uma aplicação 192
6.1.4. O que fazer quando o Bitdefender bloqueia um site Web ou uma aplicação online segura 193
6.1.5. O que fazer se o Bitdefender detetar uma aplicação segura como ransomware 194
6.1.6. Não consigo ligar-me à Internet 194
6.1.7. Não consigo aceder a um dispositivo na minha rede 195
6.1.8. A minha Internet está lenta 197
6.1.9. Como atualizar o Bitdefender numa ligação à Internet lenta 198
6.1.10. Os serviços Bitdefender não estão a responder 199
6.1.11. O filtro Antispam não está a funcionar corretamente 200
6.1.12. A funcionalidade Preenchimento automático na minha Carteira não funciona 204
6.1.13. Remoção de Bitdefender falhou 205
6.1.14. O meu sistema não reinicia após a instalação de Bitdefender 207
6.2. Remover ameaças do seu sistema 210
6.2.1. Modo de Recuperação Bitdefender (ambiente de recuperação no Windows 10) 210
6.2.2. O que fazer se o Bitdefender encontrar ameaças no seu computador? 214
6.2.3. Como posso limpar uma ameaça num ficheiro? 216
6.2.4. Como posso limpar uma ameaça num ficheiro de e-mail? 217
6.2.5. O que fazer se suspeitar que um ficheiro é perigoso? 218
6.2.6. O que são os ficheiros protegidos por palavra-passe no relatório de análise? 218
6.2.7. O que são os itens ignorados no relatório de análise? 219
6.2.8. O que são os ficheiros muito comprimidos no relatório de análise? 219
6.2.9. Por que é que Bitdefender eliminou automaticamente um ficheiro infectado? 219
Antivirus para Mac 221

7. Instalação e Remoção 222
7.1. Requisitos de Sistema 222
7.2. A instalar Bitdefender Antivirus for Mac 222
7.2.1. Processo de instalação 223
7.3. Remover o Bitdefender Antivirus for Mac 228
8. Introdução 229
8.1. Sobre o Bitdefender Antivirus for Mac 229
8.2. A abrir o Bitdefender Antivirus for Mac 229
8.3. Janela principal da aplicação 230
8.4. Ícone de doca da aplicação 231
9. Proteger contra software malicioso 233
9.1. Dicas de Utilização 233
9.2. Analisar o seu Mac 234
9.3. Ativar ou desativar o Autopilot 235
9.4. Proteção da Máquina do Tempo 235
9.5. Assistente de Análise 237
9.6. Reparar Incidência 238
9.7. Proteção da Internet 239
9.8. Atualizações 240
9.8.1. Solicitar uma Actualização 241
9.8.2. A obter atualizações através de um servidor proxy 241
9.8.3. Atualizar para uma nova versão 241
9.8.4. Encontrar informações sobre o Bitdefender Antivirus for Mac 242
10. Configurar preferências 243
10.1. Aceder às preferências 243
10.2. Info da conta 243
10.3. Preferências de proteção 244
10.3.1. Exclusões de Análise 245
10.4. Safe Files 246
10.4.1. Gerir aplicações 248
10.5. Histórico 248
10.6. Quarentena 249
11. VPN 271
11.1. Sobre a VPN 251
11.2. A instalar a VPN 251
11.3. A abrir a VPN 252
11.4. Interface 252
11.5. Assinaturas 272
12. Bitdefender Central 255
12.1. Sobre Bitdefender Central 255
12.2. A aceder Bitdefender Central 255
12.3. As minhas subscrições 256
12.3.1. Ativar subscrição 256
12.3.2. Comprar assinatura 256
12.4. Meus dispositivos 257
12.4.1. Personalize o seu dispositivo 257

12.4.2. Ações remotas 258
13. Perguntas Frequentes 260

Mobile Security para iOS 265

14. Em que consiste o Bitdefender Mobile Security for iOS 266
15. Introdução 267
16. VPN 271
16.1. Assinaturas 272
17. Privacidade de conta 274
18. Funcionalidades Anti Furto 276
19. Conta Bitdefender 280

Mobile Security para Android 282

20. Funcionalidades da Protecção 283
21. Introdução 284
22. Analisador de Malware 289
23. Privacidade de conta 292
24. Proteção da Internet 294
25. VPN 296
26. Funcionalidades Anti Furto 299
27. Bloqueio de Aplicativo 305
28. Relatórios 310
29. WearON 311
30. Definições 312
31. Sobre 313
32. Bitdefender Central 314
33. Perguntas Frequentes 318

Contacte-nos 324

34. Pedir Ajuda 325
35. Recursos online 328
35.1. Centro de Suporte Bitdefender 328
35.2. Fórum de Suporte Bitdefender 329

35.3. Portal HOTforSecurity 329
36. Informação de Contacto 330
36.1. Endereços Web 330
36.2. Distribuidores locais 330
36.3. Escritórios Bitdefender 330
Glossário 333

Sobre este guia

1. Propósito e público-alvo

A sua subscrição Bitdefender Total Security 2018 pode proteger até 10 PCs, Macs, iOS smartphones e tablets Android diferentes. A gestão dos seus dispositivos protegidos pode ser realizada através de uma conta Bitdefender, que deve estar vinculada a uma subscrição ativa.

Este guia auxilia na configuração e utilização dos produtos incluídos no sua subscrição : Bitdefender Total Security, Bitdefender Antivirus for Mac, Bitdefender Mobile Security for iOS e Bitdefender Mobile Security para dispositivos Android.

Pode descobrir como configurar o Bitdefender em diferentes dispositivos para mantê-los protegidos contra todo o tipo de ameaças.

2. Como utilizar este guia

Este guia está organizado para os quatro produtos incluídos no Bitdefender Total Security 2018:

- “Total Security para PC” (p. 1)

  Aprenda a utilizar o produto nos seus PCs e portáteis com Windows.

- “Antivirus para Mac” (p. 221)

  Aprenda a utilizar o produto nos seus Macs.

- “Mobile Security para iOS” (p. 265)

  Aprenda a utilizar o produto nos seus smartphones e tablets iOS.

- “Mobile Security para Android” (p. 282)

  Aprenda a utilizar o produto nos seus smartphones e tablets Android.

- “Contacte-nos” (p. 324)

  Veja onde procurar por ajuda caso algo inesperado apareça.

TOTAL SECURITY PARA PC

1. INSTALAÇÃO

1.1. A preparar a instalação

Antes de instalar o Bitdefender Total Security, complete estes procedimentos para assegurar uma boa instalação:

- Assegure-se que o computador onde vai instalar o Bitdefender contém os requisitos minimos do sistema. Se o seu computador não contém os requisitos mínimos do sistema, o Bitdefender não será instalado ou, se instalado, não trabalhará corretamente e provocará lentidão e instabilidade no sistema. Para ver a lista completa dos requisitos mínimos do sistema, consulte o "*Requisitos de Sistema*" (p. 222).
- Ligue-se ao computador utilizando uma conta de Administrador.
- Remova quaisquer outros softwares semelhantes do seu computador. Se for detetada qualquer coisa durante o processo de instalação da Bitdefender, será notificado para desinstalar. Executar dois programas de segurança simultaneamente poderá afetar o seu funcionamento e causar grandes problemas no sistema. O Windows Defender será desativado durante a instalação.
- Desativar ou remover qualquer programa de firewall que possa estar em execução no computador. Executar dois programas de firewall simultaneamente poderá afetar o seu funcionamento e causar grandes problemas no sistema. A Firewall do Windows será desativada durante a instalação.
- Recomenda-se que o seu computador esteja ligado à internet durante a instalação, mesmo quando realiza a instalação a partir de um CD/DVD. Se estiverem disponíveis versões mais recentes dos ficheiros da aplicação incluidos no pacote de instalação, o Bitdefender irá descarregá-las e instalá-las.

1.2. Requisitos do sistema

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

- Windows 7 com o Service Pack 1
- Windows 8
- Windows 8.1

- Windows 10

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

Nota

Para saber qual é o sistema operativo Windows executado no seu computador e informações do hardware:

- No **Windows 7**, clique com o botão direito em **Computador** no ambiente de trabalho, depois selecione **Propriedades** no menu.
- No **Windows 8**, no ecrã inicial, localize **Computador** (por exemplo, pode começar a escrever "Computador" diretamente no ecrã inicial) e depois clique com o botão direito no seu ícone. No **Windows 8.1**, localize **Este PC**.

  Selecione **Propriedades** no menu inferior. Verifique a área do **Sistema** para encontrar mais informações sobre o sistema.
- No **Windows 10**, digite **Sistema** na caixa de pesquisa da barra de tarefas e clique no seu ícone. Verifique a área do **Sistema** para encontrar mais informações sobre o sistema.

Requisitos mínimos do sistema

- 1.5 GB de espaço disponível em disco
- Processador dual core 1.6 GHz
- 1 GB de memória (RAM)

Requisitos de sistema recomendados

- 2 GB de espaço disponível no disco rígido (pelo menos 800 MB na unidade do sistema)
- Processador Intel Core Duo (2 GHz) ou equivalente
- 2 GB de memória (RAM)

Requisitos de Software

Para conseguir usar o Bitdefender e todos os seus recursos, o seu computador deve cumprir os seguintes requisitos de software:

- Microsoft Edge 40 e superior
- Internet Explorer 10 ou superior
- Mozilla Firefox 51 e superior

- Google Chrome 34 e superior
- Skype 6.3 ou superior
- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 e superior

1.3. Instalação do seu produto Bitdefender

Pode instalar o Bitdefender utilizando o disco de instalação ou através do instalador Web transferido para o seu computador na Bitdefender Central.

Se a sua aquisição cobrir mais do que um computador, repita o processo de instalação e ative o seu produto com a mesma conta em cada computador. A conta a ser utilizada deve ser igual à que contém a sua subscrição ativa do Bitdefender.

Instalar da Bitdefender Central

Na Bitdefender Central pode transferir o kit de instalação que corresponde à assinatura adquirida. Uma vez que o processo de instalação estiver concluído, o Bitdefender Total Security é ativado.

Para transferir o Bitdefender Total Security da Bitdefender Central:

1. Aceda Bitdefender Central.
2. Selecione o painel **Os meus dispositivos**, e clique em **INSTALAR PROTEÇÃO LOCAL**.
3. Escolha uma das duas opções disponíveis:
   - **DOWNLOAD**

     Clique no botão e guarde o ficheiro de instalação.
   - **Noutro dispositivo**

     Selecione **Windows** para transferir o produto Bitdefender e, em seguida, clique em **CONTINUAR**. Escreva um endereço de e-mail no campo correspondente e clique em **ENVIAR**.
4. Aguarde pela conclusão da transferência, em seguida, execute o instalador:

A validar a instalação

O Bitdefender primeiro verifica o sistema para validar a instalação.

Se o seu sistema não apresenta os requisitos mínimos para a instalação Bitdefender, você será informado das áreas que precisam de ser melhoradas antes de poder prosseguir.

Se for detetada uma solução de segurança incompatível ou uma versão anterior do Bitdefender, será solicitado a removê-lo do seu sistema. Por favor siga as instruções para remover o software do seu sistema, evitando assim que ocorram problemas mais tarde. Pode ser necessário reiniciar o computador para concluir a remoção das soluções de segurança detetadas.

O pacote de instalação do Bitdefender Total Security é continuamente atualizado.

Nota
Fazer download dos ficheiros de instalação pode demorar muito tempo, especialmente se tiver uma ligação à internet que seja lenta.

Quando a instalação for validada, o assistente de instalação aparece. Siga os passos para instalar o Bitdefender Total Security.

Passo 1 – instalação do Bitdefender

Antes de concluir o processo de instalação, deve concordar com o Contrato de Subscrição. Leia o Contrato de Subscrição com calma pois contém os termos e condições que regem a utilização do Bitdefender Total Security.

Se não concorda com estes termos, feche a janela. O processo de instalação terminará e sairá do mesmo.

Podem ser realizadas duas tarefas adicionais neste passo:

- Mantenha a opção **Enviar relatórios anónimos** ativada. Ao permitir esta opção, os relatórios que contêm informação sobre como usa o produto são enviados para os servidores Bitdefender. Esta informação é essencial para melhorar o produto e pode ajudar-nos a oferecer-lhe uma experiência melhor no futuro. Tenha em atenção que estes relatórios não contêm dados confidenciais, tais como o seu nome, endereço de IP ou outros, e que não serão usados para fins comerciais.
- Selecione o idioma em que pretende instalar o produto.

Clique em **INSTALAR** para iniciar o processo de instalação do produto Bitdefender.

Passo 2 - Instalação em curso

Espere até que a instalação termine. É apresentada informação detalhada sobre a evolução.

As áreas críticas do seu sistema são analisadas quanto a ameaças, as mais recentes versões dos ficheiros da aplicação são transferidas e instaladas e os serviços do Bitdefender são iniciados. Este passo pode demorar alguns minutos. Clique em **IGNORAR VERIFICAÇÃO** se deseja verificar o seu sistema depois. Para mais informações sobre executar uma verificação do sistema, aceda a "*Executar uma Análise do Sistema*" (p. 92).

Passo 3 - Instalação concluída

O seu produto Bitdefender foi instalado com sucesso.

É apresentado um resumo da instalação. Se tiver sido detetada uma ameaça ativa e removida durante a instalação, pode ser necessário reiniciar o sistema. Clique em **COMEÇAR A UTILIZAR O Bitdefender** para continuar.

Passo 4 - Introdução

Na janela **Introdução**, pode ver os detalhes sobre a sua assinatura ativa.

Clique em **FINALIZAR** para aceder à interface do Bitdefender Total Security.

Instalar a partir do disco de instalação

Para instalar o Bitdefender a partir do disco de instalação, insira o disco na unidade de leitura.

Deve aparecer um ecrã de instalação em alguns momentos. Siga as instruções para iniciar a instalação.

Se o ecrã de instalação não aparecer, utilize o Explorador do Windows para navegar até ao diretório de raiz do disco e clique duas vezes no ficheiro autorun.exe.

Se a velocidade da sua internet for lenta ou o seu sistema não estiver ligado à internet, clique no botão **Instalar de CD/DVD**. Neste caso, o produto Bitdefender disponível no disco será instalado e uma versão mais recente será transferida dos servidores Bitdefender através da atualização do produto.

A validar a instalação

O Bitdefender primeiro verifica o sistema para validar a instalação.

Se o seu sistema não apresenta os requisitos mínimos para a instalação Bitdefender, você será informado das áreas que precisam de ser melhoradas antes de poder prosseguir.

Se for detetada uma solução de segurança incompatível ou uma versão anterior do Bitdefender, será solicitado a removê-lo do seu sistema. Por favor siga as instruções para remover o software do seu sistema, evitando assim que ocorram problemas mais tarde. Pode ser necessário reiniciar o computador para concluir a remoção das soluções de segurança detetadas.

Nota
Fazer download dos ficheiros de instalação pode demorar muito tempo, especialmente se tiver uma ligação à internet que seja lenta.

Quando a instalação for validada, o assistente de instalação aparece. Siga os passos para instalar o Bitdefender Total Security.

Passo 1 – Instalação do Bitdefender

Antes de concluir o processo de instalação, deve concordar com o Contrato de Subscrição. Leia o Contrato de Subscrição com calma pois contém os termos e condições que regem a utilização do Bitdefender Total Security.

Se não concorda com estes termos, feche a janela. O processo de instalação terminará e sairá do mesmo.

Podem ser realizadas duas tarefas adicionais neste passo:

- Mantenha a opção **Enviar relatórios anónimos** ativada. Ao permitir esta opção, os relatórios que contêm informação sobre como usa o produto são enviados para os servidores Bitdefender. Esta informação é essencial para melhorar o produto e pode ajudar-nos a oferecer-lhe uma experiência melhor no futuro. Tenha em atenção que estes relatórios não contêm dados confidenciais, tais como o seu nome, endereço de IP ou outros, e que não serão usados para fins comerciais.
- Selecione o idioma em que pretende instalar o produto.

Clique em **INSTALAR** para iniciar o processo de instalação do produto Bitdefender.

Passo 2 - Instalação em curso

Espere até que a instalação termine. É apresentada informação detalhada sobre a evolução.

As áreas essenciais do seu sistema são analisadas quanto a ameaças e os serviços Bitdefender são iniciados. Este passo pode demorar alguns minutos. Clique em **IGNORAR VERIFICAÇÃO** se deseja verificar o seu sistema depois. Para mais informações sobre executar uma verificação do sistema, aceda a "*Executar uma Análise do Sistema*" (p. 92).

Passo 3 - Instalação concluída

É apresentado um resumo da instalação. Se tiver sido detetada uma ameaça ativa e removida durante a instalação, pode ser necessário reiniciar o sistema. Clique em **COMEÇAR A UTILIZAR O Bitdefender** para continuar.

Passo 4 - Conta Bitdefender

Após concluir a configuração inicial, a janela da conta Bitdefender aparece. É necessária uma conta Bitdefender para ativar o produto e utilizar as suas ferramentas online. Para mais informação, dirija-se a "*Bitdefender Central*" (p. 35).

Proceda consoante a sua situação.

Quero criar uma conta Bitdefender

Digite as informações obrigatórias nos campos correspondentes, depois clique em **CRIAR CONTA**.

Os dados que nos fornecer serão mantidos confidenciais.

A palavra-passe tem de ter, pelo menos, 8 carateres e incluir um número.

Leia os Termos de Serviço da Bitdefender antes de continuar.

> **Nota**
> Uma vez a conta criada, poderá utilizar o endereço de e-mail fornecido e a palavra-passe para entrar na sua conta em https://central.bitdefender.com.

Já tenho uma conta Bitdefender

Clique em **Iniciar Sessão** e depois digite o endereço de e-mail e a palava-passe da sua conta Bitdefender.

Clique em **INICIAR SESSÃO** para continuar.
Se se esqueceu da palavra-passe da sua conta, ou simplesmente pretende criar uma nova, clique na ligação **Esqueci-me da minha palavra-passe**. Escreva o seu endereço de e-mail e, em seguida, clique no botão **ESQUECI-ME DA PALAVRA-PASSE**. Verifique a sua conta de e-mail e siga as instruções fornecidas para definir a nova palavra-passe da sua conta Bitdefender.

Nota
Se já possuir uma conta MyBitdefender, pode utilizá-la para iniciar sessão na sua conta Bitdefender. Se se esqueceu da sua palavra-passe, necessita primeiro de aceder a https://my.bitdefender.com para redefini-la. Em seguida, utilize as credenciais atualizadas para iniciar sessão na sua conta Bitdefender.

Quero iniciar sessão com a minha conta do Microsoft, Facebook ou Google.
Para iniciar sessão na sua conta Microsoft, Facebook ou Google:

1. Selecione o serviço que deseja usar. Seá redireccionado para a página de início de sessão daquele serviço.
2. Siga as instruções fornecidas pelo serviço selecionado para ligar a sua conta ao Bitdefender.

Nota
O Bitdefender não obtém acesso a qualquer informação confidencial como a palavra-passe da conta que usa para iniciar sessão ou a informação particular dos seus amigos ou contactos.

Passo 5 - Ative o seu produto

Nota
Este passo aparece se selecionar criar uma nova conta Bitdefender durante o passo anterior ou se iniciar sessão utilizando uma conta com uma subscrição expirada.

É necessária uma ligação à internet para completar a ativação do seu produto.

Proceda consoante a sua situação:

- Tenho um código de ativação

  Neste caso, ative o produto seguindo estas etapas:

1. Digite o código de ativação no campo **Tenho um código de ativação** e, de seguida, clique **CONTINUAR**.

   Nota
   Pode encontrar o seu código de ativação:
   - na etiqueta do CD/DVD.
   - ou no cartão de registo do produto.
   - no e-mail da sua compra on-line.

2. **Desejo avaliar o Bitdefender**

   Neste caso, pode utilizar todos os recursos do produto durante 30 dias. Para começar o período experimental selecione **Não tenho assinatura, pretendo experimentar o produto de forma gratuita** e, de seguida, clique em **CONTINUAR**.

Passo 6 - Introdução

Na janela **Introdução**, pode ver os detalhes sobre a sua assinatura ativa.

Clique em **FINALIZAR** para aceder à interface do Bitdefender Total Security.

2. INTRODUÇÃO

2.1. Os básicos

Depois de instalar o Bitdefender Total Security, o seu computador fica protegido contra todos os tipos de ameaças (como malware, spyware, ransomware, exploits, botnets e cavalos de Troia) e ameaças da Internet (como hackers, phishing e spam).

A aplicação utiliza a tecnologia Photon para melhorar a velocidade e o desempenho do processo de análise de ameaças. Funciona através da aprendizagem dos padrões de utilização das suas aplicações de sistema para saber o que e quando analisar, minimizando o impacto no desempenho do sistema.

Ligar-se a redes sem fios públicas de aeroportos, shoppings, cafés ou hotéis sem proteção pode ser perigoso para o seu dispositivo e para os seus dados. Principalmente porque infratores podem estar a assistir às suas atividades e encontrar o melhor momento para roubar os seus dados pessoais, e também porque todos podem ver o seu endereço IP, tornando a sua máquina uma vítima para futuros ciberataques. Para evitar tais situações inoportunas, instale e use a aplicação "*VPN*" (p. 151).

Pode controlar as suas palavras-passe e contas online armazenando-as "*Proteção do Gestor de palavras-passe para as suas credenciais*" (p. 144) numa carteira. Com uma única palavra-passe principal pode proteger a sua privacidade contra intrusos que podem tentar deixá-lo sem dinheiro.

"*Proteção da Webcam*" (p. 133)impede que as aplicações não fidedignas acedam à sua câmara de vídeo, evitando qualquer tentativa de hacking. Com base na escolha dos utilizadores de Bitdefender, o acesso de aplicações populares à sua câmara Web será permitido ou bloqueado.

Para o proteger contra possíveis bisbilhoteiros e espiões quando o dispositivo está ligado a uma rede sem fios não protegida, Bitdefender analisa o nível de segurança e, quando necessário, fornece recomendações para aumentar a segurança das suas atividades online. Para instruções sobre como manter os seus dados pessoais seguros, aceda o "*Consultor de Segurança Wi-Fi*" (p. 130).

Os seus ficheiros pessoais armazenados localmente tais como documentos, fotografias ou filmes e também os armazenados na nuvem podem agora ficar longe das ameaças mais perigosas dos dias de hoje, nomeadamente

ransomware. Para mais informações sobre como colocar os ficheiros pessoais num abrigo, consulte "*Safe Files*" (p. 135).

Enquanto trabalha, joga ou vê filmes, Bitdefender pode oferecer-lhe uma experiência de utilizador contínua, adiando as tarefas de manutenção, eliminando as interrupções e ajustando os efeitos visuais do sistema. Pode beneficiar de tudo isto ao ativar e configurar os "*Perfis*" (p. 180).

Bitdefender tomará por si a maioria das decisões relacionadas com segurança e raramente surgirão alertas pop-up. Os detalhes sobre as ações tomadas e informações sobre a operação de programas estão disponíveis na janela de Notificações. Para mais informação, dirija-se a "*Notificações*" (p. 15).

De vez em quando, deve abrir o Bitdefender e corrigir as incidências existentes. Poderá ter que configurar componentes específicos do Bitdefender ou levar a cabo ações preventivas para proteger o seu computador e os seus dados.

Para utilizar as funcionalidades online do Bitdefender Total Security, gerir as suas subscrições e os dispositivos, aceda à sua conta Bitdefender. Para mais informação, dirija-se a "*Bitdefender Central*" (p. 35).

A "*Como*" (p. 48) secção é onde vai encontrar instruções passo-a-passo sobre como levar a cabo as tarefas mais comuns. Se experimentar incidências durante o uso do Bitdefender, consulte a "*Resolver incidências comuns*" (p. 188) secção de possíveis soluções para os problemas mais comuns.

A abrir a janela do Bitdefender

Para aceder à interface principal do Bitdefender Total Security, siga os passos abaixo:

- No **Windows 7**:
  1. Clique em **Iniciar** e vá para **Todos os Programas**.
  2. Clique em **Bitdefender 2018**.
  3. Clique em **Bitdefender Total Security** ou, mais rápido, clique duas vezes no ícone do Bitdefender no tabuleiro do sistema.
- No **Windows 8 e Windows 8.1**:

Localize o Bitdefender no ecrã inicial do Windows (por exemplo, pode começar a digitar "Bitdefender" diretamente no ecrã inicial) e depois clique no seu ícone. De forma alternativa, abra a aplicação do ambiente de trabalho, clique duas vezes no ícone Bitdefender no tabuleiro do sistema.

- No **Windows 10**:

  Digite "Bitdefender" na caixa de pesquisa da barra de tarefas, depois clique no seu ícone. Alternativamente, clique duas vezes no ícone do Bitdefender no tabuleiro do sistema.

Para mais informações sobre a janela e ícone do Bitdefender na barra de notificação, consulte "*Interface Bitdefender*" (p. 19).

2.1.1. A reparar problemas

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

As incidências detetadas incluem definições de proteção importantes que estão desligadas e outras condições que podem representar um risco de segurança. Estão organizadas em duas categorias:

- **Incidências críticas** - impedem que o Bitdefender o proteja contra ameaças ou representem um risco de segurança importante.
- **Incidências menores (não críticas)** - podem afetar a sua proteção num futuro próximo.

O ícone Bitdefender na área de notificação indica incidências pendentes alterando a sua cor conforme se indica a seguir:

Incidências críticas estão a afectar a segurança do seu sistema. Eles requerem a sua atenção máxima e devem ser corrigidos o mais rapidamente possível.
Incidências não críticas estão a afetar a segurança do seu sistema. Deve verificar e repará-las quando tiver oportunidade.

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

Quando abre a interface do Bitdefender, a área de estado da segurança na barra de ferramentas superior irá indicar a natureza dos problemas que afetam seu sistema.

Assistente de problemas de segurança

Para resolver os problemas detetados, siga o assistente de **Problemas de Segurança**.

1. Para abrir o assistente, faça uma das seguintes coisas:
   - Clique com o botão direito do rato no ícone do Bitdefender na área de notificação e selecione **Ver problemas de segurança**.
   - Abra a interface do Bitdefender e, de seguida, clique em qualquer lugar da área de estado de segurança na barra de ferramentas superior.
2. Pode verificar as incidências que afectam a segurança do seu computador e dos dados. Todas as incidências atuais foram selecionadas para serem reparadas.

   Se não quiser resolver uma incidência específica de imediato, limpe a caixa correspondente. Será notificado para especificar durante quanto tempo pretende adiar a reparação da incidência. Escolha a opção desejada no menu e clique em **OK**. Para parar de monitorizar a categoria de problema respetiva, escolha **Permanentemente**.

   O estado do problema irá mudar para **Adiado** e não será tomada nenhuma ação para corrigir o problema.
3. Para corrigir todos os problemas selecionados, clique em **Corrigir**. Algumas ocorrências são tratadas imediatamente. Para outras, o assistente ajuda-o a resolvê-las.

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

- **Desativar definições de segurança.** Tais incidências são reparadas imediatamente, ao ativar as respetivas definições de segurança.
- **Ferramentas preventivas de segurança que deve realizar.** Quando reparar a incidência, o assistente ajuda-o a completar com sucesso a tarefa.

Configurar os alertas de estado

O Bitdefender informa-o quando são detetadas incidências no funcionamento dos seguintes componentes do programa:

- Antivírus
- Firewall
- Atualização
- Segurança do Navegador

Pode configurar o sistema de alerta para melhor responder às suas necessidades de segurança escolhendo as incidências específicas sobre as quais pretende receber informações. Siga os seguintes passos:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Selecione o separador **AVANÇADO**.
3. Clique no link de **Configurar estado dos alertas**.
4. Clique nos botões para ligar ou desligar os alertas de estado de acordo com as suas preferências.

2.1.2. Notificações

O Bitdefender mantém um registo detalhado dos eventos relacionados com a sua atividade no seu computador. Sempre que ocorrer algo relevante para a segurança do seu sistema ou dados, será adicionada uma nova mensagem às Notificações do Bitdefender, de forma semelhante a um novo e-mail surgir na sua caixa de entrada.

As notificações são uma ferramenta importante na monitorização e gestão da proteção do seu Bitdefender. Por exemplo, pode verificar com facilidade se a atualização foi realizada com sucesso, se foram encontradas ameaças ou vulnerabilidades no seu computador, etc. Adicionalmente, pode realizar outras ações, se necessário, ou alterar ações tomadas pelo Bitdefender.

Para aceder ao registo das notificações, clique no ícone na barra lateral esquerda da interface do Bitdefender. Sempre que acontecer este evento crítico, pode ser observado um contador no ícone .

Dependendo do tipo e da gravidade, as notificações são agrupadas em:

- Os eventos **críticos** indicam problemas críticos. Deve verificá-los imediatamente.
- O eventos de **Aviso** indicam incidências não críticas. Deve verificar e repará-las quando tiver oportunidade.
- Eventos de **Informação** indicam operações bem sucedidas.

Clique em cada separador para ver mais detalhes sobre os eventos gerados. São apresentados breves detalhes com um único clique em cada título de evento, como uma descrição curta, a ação tomada pelo Bitdefender quando o evento ocorreu e a data e hora do evento. Pode ser fornecidas opções para tomar mais ações, caso seja necessário.

Para o ajudar a gerir com facilidade os eventos registados, a janela de notificações oferece opções para eliminar ou marcar como lidos todos os eventos naquela secção.

2.1.3. Autopilot

Para todos os utilizadores que desejam apenas que a sua solução de segurança os proteja sem os incomodar, o Bitdefender Total Security foi concebido com um modo AutoPilot incorporado.

Em Autopilot, o Bitdefender aplica uma configuração de segurança ótima e toma, por si, todas as decisões relacionadas com a segurança. Isto significa que raramente verá pop-ups e não terá de configurar quaisquer definições.

No modo Autopilot, o Bitdefender repara automaticamente incidências críticas, ativa opões e gere tranquilamente:

- Proteção antivírus, proporcionada pela análise no acesso e análise contínua.
- Proteção Firewall.
- Proteção da Internet.
- Atualizações Automáticas.

Para ligar ou desligar o Autopilot, clique no botão **AUTOPILOT** na barra de ferramentas superior da interface do Bitdefender.

Enquanto o Autopilot estiver ligado, o ícone Bitdefender na área de notificação mudará para .

> **Importante**
> Enquanto o Autopilot estiver ligado, se modificar alguma das definições este será desligado.

Para ver o histórico de ações realizadas pelo Bitdefender enquanto o Autopilot estava em execução, abra a janela Notificações.

2.1.4. Perfis

Algumas atividades do computador, tais como os jogos online ou apresentações de vídeo, requerem uma maior capacidade de resposta, elevado desempenho e nenhuma interrupção do sistema. Quando o seu computador portátil está ligado apenas com a bateria, é melhor que operações desnecessárias, que consomem mais energia, sejam adiadas até que o portátil esteja ligado á corrente.

Os Perfis do Bitdefender atribuem mais recursos do sistema às aplicações em execução, modificando temporariamente as definições de proteção e ajustando a configuração do sistema. Consequentemente, o impacto do sistema na sua atividade é minimizado.

Para adaptar-se a diferentes atividades, o Bitdefender vem com os seguintes perfis:

Perfil Trabalho
: Otimiza a sua eficiência de trabalho ao identificar e ajustar as definições do produto e do sistema.

Perfil de Filme
: Melhora os efeitos visuais e elimina as interrupções ao ver filmes.

Perfil de Jogo
: Melhora os efeitos visuais e elimina as interrupções ao jogar.

Perfil Wi-Fi Público
: Aplica definições do produto para beneficiar da proteção completa enquanto está ligado a uma rede sem fios insegura.

Perfil do Modo de Bateria
: Aplica definições de produto e coloca em pausa as atividades em segundo plano para economizar bateria.

Configure a ativação automática de perfis

Para uma experiência intuitiva, pode configurar o Bitdefender para gerir o seu perfil de trabalho. Neste caso, o Bitdefender deteta automaticamente a sua atividade e aplica definições de otimização do produto e do sistema.

Para permitir que o Bitdefender ative perfis:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Selecione o separador **PERFIS**.

3. Utilize o botão correspondente para ligar **Ativar perfis automaticamente**.

Caso não queira que os perfis sejam ativados automaticamente, desligue o botão.

Para ativar manualmente um perfil, clique no botão ON/OFF correspondente. Só é possível ativar manualmente um perfil de cada vez.

Para mais informações sobre Perfis, aceda a"*Perfis*" (p. 180)

2.1.5. Definições de proteção da palavra-passe de Bitdefender

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

Para configurar a proteção por palavra-passe para as definições do Bitdefender:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Na janela **GERAL**, ative a **Proteção por palavra-passe** ao clicar no botão correspondente.
3. Digite a palavra-passe nos dois campos e, em seguida, clique em **OK**. A palavra-passe tem de ter pelo menos 8 caracteres.

Depois de definir uma palavra-passe, se alguém tentar mudar as definições do Bitdefender terá primeiro de fornecer a palavra-passe.

Importante

Não se esqueça da sua palavra-passe e registe-a num local seguro. Se esquecer a palavra-passe, terá de reinstalar o programa ou contactar o apoio do Bitdefender.

Para remover a proteção por palavra-passe:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Na janela **GERAL**, desligue a proteção por palavra-passe ao clicar no botão correspondente.
3. Digite a palavra-passe e, em seguida, clique em **OK**.

Nota
Para alterar a palavra-passe para o seu produto, clique na hiperligação **Alterar palavra-passe**. Digite a palavra-passe atual e, de seguida, clique *OK*. Na nova janela que aparece, digite a palavra-passe que pretende utilizar a partir deste momento para restringir o acesso às definições do seu Bitdefender.

2.1.6. Relatórios anónimos de utilização

Por defeito, o Bitdefender envia relatórios que contêm informação sobre como o usar nos servidores Bitdefender. Esta informação é essencial para melhorar o produto e pode ajudar-nos a oferecer-lhe uma experiência melhor no futuro. Tenha em atenção que estes relatórios não contêm dados confidenciais, tais como o seu nome, endereço de IP ou outros, e que não serão usados para fins comerciais.

Caso pretenda parar de enviar Relatórios anónimos:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Selecione o separador **AVANÇADO**.
3. Clique no botão ON/OFF correspondente.

2.1.7. Notificações de ofertas especiais

Quando as ofertas promocionais forem disponibilizadas, o produto Bitdefender está configurado para notificá-lo através de uma janela pop-up. Isto dar-lhe-á a oportunidade de aproveitar os preços vantajosos e manter os dispositivos protegidos por um período mais longo.

Para ativar ou desativar notificações de ofertas especiais:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Na janela **GERAL**, clique no botão ON/OFF correspondente.

As opções de ofertas especiais e de notificações do produto estão ativadas por defeito.

2.2. Interface Bitdefender

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

Vá à interface do Bitdefender, encontra-se exibido no canto superior esquerdo um assistente de introdução que contém detalhes sobre como interagir com o produto e como o configurar. Selecione **SEGUINTE** para continuar a ser guiado ou **Ignorar** para fechar o assistente.

Para ver o estado do produto e realizar tarefas essenciais, encontra-se disponível o ícone na área de notificação do sistema do Bitdefender a qualquer momento.

A janela principal permite que gira o comportamento do produto utilizando o Autopilot, permite realizar tarefas comuns e dá acesso a informações importantes sobre o produto. Na barra lateral esquerda, pode aceder à sua conta Bitdefender e às secções do Bitdefender para definições detalhadas e tarefas administrativas avançadas.

Se deseja manter uma vigilância constante na informação essencial de segurança e ter um acesso rápido a definições chave, adicione o Dispositivo Segurança ao seu ambiente de trabalho.

2.2.1. Ícone na área de notificação

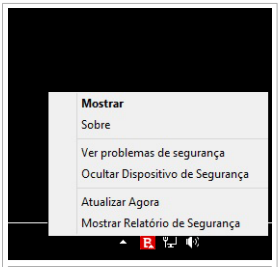
Para gerir todo o produto mais rapidamente, pode usar o ícone da Bitdefender que se encontra na barra de tarefas.

Nota

O ícone do Bitdefender poderá não estar visível a toda a hora. Para fazer o ícone aparecer permanentemente:

- No **Windows 7, Windows 8 e Windows 8.1**:
  1. Clique na seta no canto inferior direito do écran.
  2. Clique **Personalizar...** para abrir a janela de ícones da Área de Notificação.
  3. Selecione a opção **Mostrar ícones e notificações** para o ícone do **Agente do Bitdefender**.
- No **Windows 10**:
  1. Clique com o botão direito do rato na barra de tarefas e seleccione **Propriedades**.
  2. Clique em **Personalizar** na janela da barra de tarefas.
  3. Clique no link de **Selecione quais ícones aparecem na barra de ferramentas** na janela de **Notificações e ações**.
  4. Ative o botão ao lado do **Agente do Bitdefender**.

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



Ícone Tray

- **Mostrar** - abre a janela principal do Bitdefender.
- **Sobre** — abre uma janela onde pode consultar informações sobre Bitdefender, onde procurar ajuda se acontecer algo inesperado, onde visualizar o Contrato de Subscrição, os Componentes de Terceiros e a Política de Privacidade.
- **Ver problemas de segurança** - ajuda-o a remover as vulnerabilidades de segurança. Se a opção não está disponível, é porque não há incidências a reparar. Para informação detalhada dirija-se a "*A reparar problemas*" (p. 13).
- **Ocultar / Mostrar Dispositivo Segurança** - ativa / desativa Dispositivo Segurança.
- **Atualizar agora** - executa uma atualização imediata. Pode seguir o estado das atualizações no painel de Atualizações da janela principal do Bitdefender.
- **Mostrar Relatório de Segurança** - abre uma janela onde pode visualizar o estado semanal e recomendações para o seu sistema. Pode seguir as recomendações para melhorar a segurança do seu sistema.

O ícone do Bitdefender na área de notificação do sistema, informa quando há incidências a afetar o seu computador ou a forma como o produto funciona, exibindo um símbolo especial, como o que se segue:

Problemas críticos estão a afetar a segurança do seu sistema. Eles requerem atenção imediata e devem ser reparados o mais breve possível.
Incidências não críticas estão a afetar a segurança do seu sistema. Deve verificar e repará-las quando tiver oportunidade.
O Autopilot do Bitdefender está ligado.

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

2.2.2. Janela Principal

A janela principal do Bitdefender permite-lhe realizar tarefas comuns, corrigir rapidamente problemas de segurança, visualizar informações sobre o funcionamento do produto e aceder a painéis de onde configurar as definições do produto. Tudo se encontra a apenas uns cliques de distância.

A janela está organizada em quatro áreas principais:

Área de Estado
: Aqui é onde pode verificar o estado de segurança do seu computador, executar uma atualização e configurar o Autopilot.

Barra lateral esquerda
: Este menu permite que aceda e gira a sua conta Bitdefender juntamente com outras funcionalidades online do seu produto ou que altere entre as três principais secções do produto. Neste menu também pode aceder às áreas Notificações, Relatório de Segurança semanal, Definições gerais e Suporte.

Botões de ação e acesso à área de funcionalidades
: Aqui pode executar diferentes tarefas para manter o seu sistema protegido e a funcionar na velocidade ideal. Além disso, pode aceder às funcionalidades do Bitdefender para configurar o produto por si mesmo.

Barra inferior
: Este é o local onde pode instalar o Bitdefender ou outros dispositivos, uma vez que a sua subscrição tem entradas disponíveis suficientes.

Área de Estado

A área de estado contém os seguintes elementos:

- **Estado de Segurança** no lado esquerdo da área, informa se existe qualquer problema a afetar a segurança do seu computador e ajuda a repará-los.

  A cor da área de estado da segurança muda dependendo das incidências detetadas e são apresentadas diferentes mensagens:

  - **A área está colorida de verde.** Não existem incidências para reparar. O seu computador e os seus dados estão protegidos.
  - **A área está colorida de amarelo.** Incidências não críticas estão a afetar a segurança do seu sistema. Deve verificar e repará-las quando tiver oportunidade.

- **A área está colorida de vermelho.** Incidências críticas estão a afectar a segurança do seu sistema. Deve resolver estas incidências imediatamente.

Ao clicar em qualquer lugar na área de estado de segurança, poderá aceder a um assistente que irá ajudar a remover facilmente quaisquer ameaças do seu computador. Para informação detalhada dirija-se a "*A reparar problemas*" (p. 13).

- O **Autopilot** permite que tenha a melhor proteção e que desfrute de uma segurança completamente discreta. Para informação detalhada dirija-se a "*Autopilot*" (p. 16).
- **ATUALIZAR AGORA** permite que execute a atualização de um produto sempre que quiser para garantir que tem a mais recente base de dados de informações sobre ameaças. Para informação detalhada dirija-se a "*Mantenha o seu Bitdefender atualizado.*" (p. 43).
- **Perfil Ativo** exibe o perfil ativo atual no seu produto Bitdefender. Para informação detalhada dirija-se a "*Perfis*" (p. 180).

Barra lateral esquerda

Os ícones sugestivos estão disponíveis no lado esquerdo da barra lateral, dando acesso à conta Bitdefender, a secções do produto, relatório de atividades, notificações, definições gerais e suporte.

Os nomes dos ícones são visíveis ao clicar no ícone ☰, da seguinte forma:

- **Proteção**. Os botões de ação **Análise Rápida** e **Análise de Vulnerabilidades** ficam visíveis no canto inferior esquerdo na interface do Bitdefender. Além disso, as informações sobre aplicações bloqueadas, ameaças detetadas e ataques ficam visíveis. Clique na hiperligação **VER FUNCIONALIDADES** para aceder à área de configuração.
- **Privacidade**. Os botões de ação **Safepay** e **VPN** ficam visíveis no canto inferior esquerdo da interface do Bitdefender. Além disso, são apresentadas as informações sobre carteiras e cofres de ficheiros. Clique na hiperligação **VER FUNCIONALIDADES** para aceder à área de configuração.
- **Ferramentas**. Os botões de ação **OneClick Optimizer** e **Startup Optimizer** ficam visíveis no canto inferior esquerdo da interface do Bitdefender. Além disso, pode aceder à função Antirroubo e a função

Limpeza de Disco pode ser executada para libertar mais espaço para dados novos apagando ficheiros desnecessários.

- **Atividade**. Daqui, pode visualizar a atividade do produto nos últimos 30 dias e aceder ao relatório de segurança que é gerado a cada sete dias.
- **Notificações**. A partir daqui pode aceder às notificações geradas.
- **Conta**. Os detalhes sobre a conta Bitdefender e assinatura em utilização estão disponíveis. Aceda à sua conta Bitdefender para verificar as suas subscrições e realizar tarefas de segurança nos dispositivos que controla.
- **Definições**. A partir daqui pode aceder às definições gerais.
- **Suporte**. Aqui é possível entrar em contato com o departamento de Suporte Técnico da Bitdefender sempre que for necessária assistência para resolver um problema com seu Bitdefender Total Security.

Botões de ação e acesso à área de funcionalidades

Pode realizar tarefas importantes de forma rápida utilizando os botões de ação. Os botões de ação ficam visíveis no canto inferior esquerdo da interface do Bitdefender quando selecionar uma das três secções: **Proteção**, **Privacidade** ou **Ferramentas** a partir da barra lateral esquerda.

Dependendo da secção que você escolher, os botões de ação visíveis na área podem ser:

- **Análise Rápida**. Execute uma análise rápida para garantir que o seu computador está livre de ameaças.
- **Ver Vulnerabilidades**. Verifique o seu computador para identificar vulnerabilidades e garantir que todas as aplicações instaladas, para além do sistema operativo, estão atualizadas e a funcionar corretamente.
- **Safepay**. Abra o Bitdefender Safepay™ para proteger os seus dados pessoais enquanto efetua transações online.
- **VPN**. Abra o Bitdefender VPN para adicionar uma camada extra de proteção enquanto está ligado à Internet.
- **Otimizador de Um Clique**. Liberte espaço no disco, corrija erros de registo e proteja a sua privacidade ao eliminar ficheiros que já não são úteis com um simples clicar no botão.
- **Otimizador de Arranque**. Diminua o tempo de arranque do seu sistema excluindo a execução de aplicações desnecessárias durante o arranque.

Barra inferior

Para começar a proteger mais dispositivos:

1. Clique na ligação **INSTALAR NOUTRO DISPOSITIVO**.

   Será redirecionado para a página Web da conta Bitdefender. Certifique-se de que tem sessão iniciada com as suas credênciais

2. Na janela que aparece selecione o sistema de funcionamento pretendido e, de seguida, clique **CONTINUAR**.

3. Introduza o endereço de e-mail para o qual devemos enviar a ligação de transferência da instalação da plataforma escolhida.

Dependendo da sua escolha, serão instalados os seguintes produtos do Bitdefender:

- Bitdefender Total Security nos dispositivos Windows.
- Bitdefender Antivirus for Mac em dispositivos macOS.
- Bitdefender Mobile Security nos dispositivos Android.
- Bitdefender Mobile Security em dispositivos iOS.
- Controlo Parental do Bitdefender em dispositivos macOS, iOS e Android.

2.2.3. As secções do Bitdefender

O Bitdefender tem três secções diferentes divididas em funcionalidades úteis para ajudá-lo a permanecer protegido enquanto trabalha, navega na Internet, realiza pagamentos online, além de melhorar a velocidade do seu sistema, etc.

Sempre que pretender aceder às funcionalidades para uma secção específica ou para começar a configurar o seu produto, clique nos seguintes ícones localizados na barra lateral da interface do Bitdefender:

- Proteção
- Privacidade
- Ferramentas

Proteção

Na secção Proteção, é possível configurar as definições avançadas de segurança, gerir amigos e spammers, ver e editar as definições da ligação

de rede, configurar as funções de Proteção na Web e Safe Files, verificar e reparar potenciais vulnerabilidades do sistema e avaliar as ligações sem fios às quais se liga.

As funcionalidades que pode gerir na secção Proteção são:

ANTIVIRUS

A protecção antivirus é a base da sua segurança. O Bitdefender protege-o em tempo real e a pedido contra todos os tipos de ameaças, tais como malware, trojans, spyware, adware, etc.

A partir da funcionalidade Antivírus, pode aceder facilmente às seguintes tarefas de análise:

- Análise Rápida
- Análise do Sistema
- Gerir Análises
- Modo de Recuperação (ambiente de recuperação no Windows 10)

Para mais informações sobre tarefas de análise e como configurar a proteção antivírus, consulte "*Proteção Antivírus*" (p. 85).

PROTEÇÃO DA WEB

A proteção da Web ajuda-lhe a manter-se protegido contra ataques de phishing, tentativas de fraude e fugas de dados pessoais enquanto navega na internet.

Para mais informações sobre como configurar o Bitdefender para proteger a sua atividade Web, consulte "*Proteção da Internet*" (p. 109).

FIREWALL

A firewall protege-o enquanto está ligado às redes e à Internet, através da filtragem de todas as tentativas de ligação.

Para mais informações sobre configuração de firewall, consulte "*Firewall*" (p. 120).

ADVANCED THREAT DEFENSE

O Advanced Threat Defense protege ativamente o sistema contra ameaças tal como ransomware, spyware e cavalos de Tróia ao analisar o comportamento de todas as aplicações instaladas. Os processos suspeitos são identificados e, quando necessário, bloqueados.

Para mais informações sobre como manter o sistema protegido contra ameaças, consulte "*Advanced Threat Defense*" (p. 107).

ANTISPAM

A funcionalidade antispam do Bitdefender garante que a sua Caixa de Entrada permanece livre de e-mails indesejados através da filtragem do tráfego de e-mail POP3.

Para mais informações sobre a proteção antispam, consulte "*Antispam*" (p. 111).

VULNERABILIDADE

A funcionalidade Vulnerabilidade ajuda a manter o seu sistema operativo e as aplicações que utiliza regularmente atualizados e a identificar as redes sem fios não protegidas às quais se liga.

Clique em **Análise de Vulnerabilidades** na funcionalidade Vulnerabilidade para começar a identificar as atualizações críticas do Windows, atualizações de aplicações, palavras-passe fracas em contas do Windows e redes sem fios que não são seguras.

Clique em **Consultor de Segurança do Wi-Fi** para ver uma lista das redes sem fio às quais se liga, além da nossa avaliação de reputação para cada uma delas e as ações que pode tomar para continuar protegido contra potenciais espiões.

Para mais informações sobre como configurar a proteção de vulnerabilidade, consulte "*Vulnerabilidade*" (p. 125).

SAFE FILES

A funcionalidade Safe Files garante que os seus ficheiros pessoais ficam protegidos contra ataques de ransomware.

Para obter mais informações sobre como configurar Safe Files para proteger os seus ficheiros pessoais contra ataques de ransomware, consulte "*Safe Files*" (p. 135).

Privacidade

Na secção Privacidade, pode abrir a aplicação do Bitdefender VPN, encriptar os seus dados privados, proteger as suas transações online, manter a sua webcam e navegação seguras e proteger os seus filhos ao restringir a sua atividade online.

As funcionalidades que pode gerir na secção Privacidade são:

VPN

A VPN protege as suas atividades online e esconde o seu endereço IP sempre que se ligar a redes sem fios não seguras em aeroportos, shoppings, cafés ou hotéis. Além disso, pode aceder a conteúdos que normalmente são restritos em certas áreas.

Para mais informações sobre esta funcionalidade, consulte "*VPN*" (p. 151).

ENCRIPTAÇÃO

Criar drives lógicas encriptadas e protegidas por palavra-passe (ou cofres) no seu computador onde pode armazenar em segurança os seus documentos confidenciais e sensíveis.

Para obter mais informações sobre como criar unidades lógicas (ou cofres) protegidas por palavra-passe e encriptadas no seu computador, consulte "*Encriptação de ficheiro*" (p. 138).

PROTEÇÃO DA CÂMARA WEB

A Proteção da Câmara Web do Bitdefender mantém a câmara Web fora de perigo ao bloquear o acesso de aplicações não fidedignas.

Para mais informações sobre como manter o sistema protegido contra acesso indesejado, consulte "*Proteção da Webcam*" (p. 133).

GESTOR DE SENHAS

O Gestor de palavras-passe do Bitdefender ajuda-o a controlar as suas palavras-passe, protege a sua privacidade e proporciona uma experiência de navegação segura.

Para mais informações sobre como configurar o Gestor de palavras-passe, consulte "*Proteção do Gestor de palavras-passe para as suas credenciais*" (p. 144).

SAFEPAY

O navegador Bitdefender Safepay™ ajuda a manter a sua atividade bancária online, compras online e qualquer outro tipo de transação online, privada e segura.

Clique no botão de ação **Safepay** na interface do Bitdefender para começar a realizar transações online num ambiente seguro.

Para mais informações sobre o Bitdefender Safepay™, consulte "*Segurança Safepay para transações online*" (p. 154).

CONSULTOR PARENTAL

O Consultor Parental do Bitdefender permite monitorizar o que o seu filho está a fazer no computador. Caso haja conteúdo inapropriado, pode decidir restringir o seu acesso à Internet ou às aplicações específicas.

Clique em **Configurar** no painel do Controlo Parental para iniciar a configuração dos dispositivos dos seus filhos e monitorizar a sua atividade onde quer que esteja.

Para mais informações sobre como configurar o Gestor de palavras-passe, consulte "*Consultor Parental*" (p. 159).

PROTEÇÃO DE DADOS

A funcionalidade Proteção de Dados permite apagar ficheiros permanentemente.
Clique em **Destruidor de Ficheiros** no painel Proteção de Dados para iniciar um assistente que permitirá eliminar completamente os ficheiros do seu sistema.

Para mais informações sobre como configurar a Proteção de Dados, consulte "*Proteção de dados*" (p. 158).

Ferramentas

Na secção Ferramentas, é possível melhorar a velocidade do sistema e gerir os seus dispositivos.

Optimizador

Bitdefender Total Security oferece não apenas segurança, também ajuda a manter um bom desempenho do seu sistema.

Na funcionalidade Otimização, pode aceder a uma variedade de ferramentas úteis:

- Otimizador de Um Clique
- Otimizador de Arranque
- Limpeza do disco

Para mais informações sobre o desempenho das ferramentas de otimização, por favor consulte "*Ferramentas*" (p. 176).

Anti-Theft

O Antirroubo do Bitdefender protege o seu computador e os seus dados contra roubo ou perda. No caso de tal evento, isto permite-lhe localizar remotamente ou bloquear o seu computador. Pode também limpar todos os dados presentes no seu sistema.

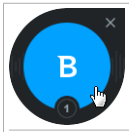
O Antirroubo do Bitdefender oferece as seguintes funcionalidades:
- Localização Remota
- Bloqueio Remoto
- Limpeza Remota
- Alerta Remoto

Para mais informações sobre como pode manter o seu sistema longe das mãos erradas, consulte "*Dispositivo Anti-Roubo*" (p. 172).

2.2.4. Dispositivo de Segurança

Dispositivo Segurança é a forma rápido e fácil de controlar o Bitdefender Total Security. Adicionar este dispositivo pequeno e não intrusivo ao seu ambiente de trabalho deixa-o ver informação critica e levar a cabo tarefas chave em qualquer altura:

- abrir a janela principal do Bitdefender.
- monitorizar a atividade de análise em tempo-real.
- monitorizar o estado de segurança do seu sistema e reparar qualquer incidência que exista.
- ver quando uma atualização está em curso.
- ver os avisos e obter acesso aos mais recentes eventos reportados pelo Bitdefender.
- analisar ficheiros ou pastas ao arrastar e largar um ou vários itens sobre o dispositivo.



Dispositivo de Segurança

O estado geral de segurança do seu computador é mostrado **no centro** do dispositivo. O estado é indicado pela cor e forma do ícone que é mostrado nessa área.

Incidências críticas estão a afectar a segurança do seu sistema.

Eles requerem a sua atenção máxima e devem ser corrigidos o mais rapidamente possível. Clique no ícone do estado para começar a reparar as incidências reportadas.

Incidências não críticas estão a afetar a segurança do seu sistema. Deve verificar e repará-las quando tiver oportunidade. Clique no ícone do estado para começar a reparar as incidências reportadas.

O seu sistema está protegido.

Quando uma tarefa de análise a-pedido está em progresso, este ícone animado é apresentado.

Quando são reportadas incidências, clique no ícone de estado para ativar o assistente de Reparação de Incidências.

O lado inferior do dispositivo apresenta o contador de eventos não lidos (o número de eventos importantes comunicados pelo Bitdefender, caso haja algum). Clique no contador de eventos, por exemplo 1 para um evento não lido, para abrir a janela de notificações. Para mais informação, dirija-se a "*Notificações*" (p. 15).

Analisar ficheiros e pastas

Pode usar o Dispositivo de Segurança para analisar rapidamente ficheiros e pastas. Arraste qualquer ficheiro ou pasta que deseje analisar e largue-o sobre o **Dispositivo Segurança**.

O Assistente de Análise Antivírus irá surgir e guiá-lo através do processo de análise. As opções de análise estão pré-configuradas para obter os melhores resultados de deteção e não podem ser alterados. Se forem detectados ficheiros infectados, o Bitdefender irá tentar desinfectá-los (remover o código malicioso). Se a desinfecção falha, o assistente de análise antivírus irá permitir-lhe definir outras acções a serem levadas a cabo sobre os ficheiros infectados.

Ocultar / mostrar Dispositivo de Segurança

Quando não desejar mais ver o dispositivo, clique em ⊗.

Para restaurar o Widget de Segurança, utilize um dos seguintes métodos:

- Do tabuleiro do sistema:

1. Clique com o botão direito do rato no ícone do Bitdefender no ícone do tabuleiro do sistema.
2. Clique em **Mostrar Dispositivo Segurança** no menu contextual que aparece.

- A partir da interface do Bitdefender:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Selecione o separador **GERAL**.
3. Ligar **Exibir Widget de Segurança** ao clicar no botão correspondente.

O Widget de segurança Bitdefender está desativado por predefinição.

2.2.5. Actividade

A janela de Atividade exibe informações sobre as ações tomadas pelo Bitdefender no seu dispositivo nos últimos 30 dias. Aqui pode verificar quais aplicações, ameaças e ataques foram bloqueados durante esse período, e se quaisquer tentativas de ransomware foram feitas.

Além disso, é possível aceder ao painel de atividade da Bitdefender Central clicando na hiperligação correspondente.

O Relatório de Segurança, que fornece um estado semanal para o seu produto e várias dicas para melhorar a proteção do sistema, pode ser acedido também clicando na hiperligação correspondente. Estas dicas são importantes para gerir a proteção geral e poderá facilmente identificar as ações que pode tomar para o seu sistema.

O relatório é gerado uma vez por semana e resume informações relevantes sobre as atividades do produto para que possa facilmente compreender o que ocorreu durante este período.

As informações oferecidas pelo Relatório de Segurança estão divididas em três categorias:

- Área de **Proteção** - veja as informações relacionadas com a proteção do seu sistema.
  - **Ficheiros analisados**

    Permite-lhe visualizar os ficheiros analisados pelo Bitdefender durante a semana. Pode ver detalhes como o número de ficheiros analisados e o número de ficheiros limpos pelo Bitdefender.

Para obter mais informações sobre a proteção antivírus, consulte "*Proteção Antivírus*" (p. 85).

- **Páginas Web analisadas**

  Permite-lhe verificar o número de páginas Web analisadas e bloqueadas pelo Bitdefender. Para o proteger da divulgação de informações pessoais durante a navegação, o Bitdefender protege o seu tráfego na Internet.

  Para mais informações sobre a Proteção da Internet, consulte "*Proteção da Internet*" (p. 109).

- **Vulnerabilidades**

  Permite identificar e corrigir facilmente as vulnerabilidades do sistema, para tornar o computador mais seguro contra ameaças e hackers.

  Para obter mais informações sobre a análise de vulnerabilidade, consulte "*Vulnerabilidade*" (p. 125).

- **Linha Cronológica de Eventos**

  Permite que tenha uma imagem geral de todos os processos de análise e problemas corrigidos pelo Bitdefender durante a semana. Os eventos são separados por dias.

  Para mais informações sobre um registo detalhado de eventos relativos à atividade no seu computador, consulte "*Notificações*" (p. 15).

- Área **Privada** - veja informações relacionadas com a privacidade do seu sistema.

  - **Ficheiros no Cofre**

    Permite visualizar quantos ficheiros estão protegidos contra o acesso indesejado.

    Para obter mais informações sobre como criar unidades lógicas (ou cofres) protegidas por palavra-passe e encriptadas no seu computador, consulte "*Encriptação de ficheiro*" (p. 138).

- Área de **Otimização** - veja informações relacionadas com o espaço libertado, aplicações otimizadas e quanta bateria do computador economizou utilizando o Modo de Bateria.

  - **Espaço limpo**

Permite-lhe ver quanto espaço foi libertado durante o processo de otimização do sistema. O Bitdefender utiliza a Otimização para ajudar a aumentar a velocidade do seu sistema.

Para mais informações sobre Otimização, consulte "*Ferramentas*" (p. 176).

- **Bateria economizada**

  Permite-lhe ver quanta bateria economizou enquanto o sistema funcionou em Modo de Bateria.

  Para mais informações sobre o Modo de Bateria, consulte "*Perfil do Modo de Bateria*" (p. 185).

- **Aplicações otimizadas**

  Permite ver o número de aplicações que utilizou com os Perfis.

  Para mais informações sobre Perfis, aceda a "*Perfis*" (p. 180).

A verificar o Relatório de Segurança

O Relatório de Segurança utiliza um sistema de rastreio de problemas para detectar e o informar sobre os eventos que podem afetar a segurança do seu computador e dados. As incidências detetadas incluem definições de proteção importantes que estão desligadas e outras condições que podem representar um risco de segurança. Ao utilizar o relatório, pode configurar componentes específicos do Bitdefender ou tomar ações preventivas para proteger o seu computador e dados privados.

Para verificar o Relatório de Segurança:

1. Aceder ao relatório:

   - Clique no ícone na barra lateral esquerda da interface do Bitdefender.

     Clique na hiperligação **Relatório de Segurança** localizado no canto inferior direito da janela Relatório de Atividade.

   - Clique com o botão direito do rato no ícone do Bitdefender no tabuleiro do sistema e selecione **Mostrar relatório de segurança**.

   - Após a conclusão de um relatório receberá uma notificação pop-up. Clique em **Mostrar** para aceder ao relatório de atividade.

     Abrir-se-á uma página Web no navegador Web onde pode visualizar o relatório gerado.

2. Observe a parte superior da janela para visualizar o estado geral de segurança.
3. Verifique as nossas recomendações na parte inferior da página.

A cor da área de estado da segurança muda dependendo das incidências detetadas e são apresentadas diferentes mensagens:

- **A área está verde.** Não existem problemas a corrigir. O seu computador e os seus dados estão protegidos.
- **A área está laranja.** A segurança do seu sistema está a ser afetada por problemas não críticos. Deve verificar e repará-las quando tiver oportunidade.
- **A área está vermelha.** A segurança do seu sistema está a ser afetada por problemas críticos. Deve resolver estas incidências imediatamente.

Ativar ou desativar a notificação do Relatório de Segurança

Para ativar ou desativar a notificação do Relatório de Segurança

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Na janela **GERAL**, clique no botão ON/OFF correspondente.

   A notificação do Relatório de Segurança está ativada por defeito.

2.3. Bitdefender Central

Bitdefender Central é a plataforma Web onde tem acesso às funcionalidades e serviços online do produto, e pode realizar remotamente tarefas importantes nos dispositivos em que o Bitdefender estiver instalado. Pode iniciar sessão na sua conta Bitdefender a partir de qualquer computador ou dispositivo móvel ligado à internet através https://central.bitdefender.com. Assim que iniciar sessão, pode começar a fazer o seguinte:

- Transfira e instale o Bitdefender nos sistemas operativos Windows, macOS, iOS e Android. Os produtos disponíveis para download são:
  - Bitdefender Total Security
  - O Antivírus Bitdefender para Mac
  - Bitdefender Mobile Security para Android
  - Bitdefender Mobile Security for iOS

- Consultor Parental Bitdefender
- Gerir e renovar as suas subscrições do Bitdefender.
- Adicionar novos dispositivos à sua rede e gerir as suas funcionalidades onde quer que esteja.
- Proteja os dispositivos de rede e os seus dados contra roubo ou perda com o Anti-Roubo.
- Configurar as definições do Parental Advisor para as contas das suas crianças e monitorizar a sua atividade onde quer que eles estejam.
- Aceda ao relatório Atividade para ver o estado da sua subscrição atual e os dispositivos adicionados à sua rede e, quando necessário, melhore remotamente o desempenho dos seus dispositivos Windows.

A aceder Bitdefender Central

Existem diversas formas de aceder à Bitdefender Central. Dependendo da tarefa que quiser realizar, pode utilizar qualquer uma das seguintes opções:

- A partir da interface principal do Bitdefender:
  1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
  2. Selecione a ligação **Ir para a Central do Bitdefender**.
  3. Inicie sessão na sua conta Bitdefender utilizando o seu endereço de e-mail e palavra-passe.
- Do seu navegador Web:
  1. Abrir um navegador em qualquer dispositivo com acesso à internet.
  2. Vá para: https://central.bitdefender.com.
  3. Inicie sessão na sua conta Bitdefender utilizando o seu endereço de e-mail e palavra-passe.

2.3.1. As minhas subscrições

A plataforma da Bitdefender Central possibilita-lhe controlar facilmente as subscrições que possui para todos os seus dispositivos.

Verificar subscrições disponíveis

Para verificar as suas subscrições disponíveis:

1. Aceda Bitdefender Central.
2. Selecione o painel **As Minhas Subscrições**.

Aqui pode aceder às informações sobre a disponibilidade das subscrições que possui e o número de dispositivos a utilizar cada uma delas.

Pode adicionar um novo dispositivo a uma subscrição ou renová-la selecionando um cartão de subscrição.

Nota
Pode ter uma ou mais subscrições na sua conta desde que sejam para diferentes plataformas (Windows, macOS, iOS ou Android).

Adicionar um novo dispositivo

Caso a sua subscrição cubra mais do que um dispositivo, pode adicionar um novo dispositivo e instalar o seu Bitdefender Total Security no mesmo, conforme descrito abaixo:

1. Aceda Bitdefender Central.
2. Selecione o painel **Os meus dispositivos**, e clique em **INSTALAR PROTEÇÃO LOCAL**.
3. Escolha uma das duas opções disponíveis:
   - **DOWNLOAD**

     Clique no botão e guarde o ficheiro de instalação.
   - **Noutro dispositivo**

     Selecione **Windows** para transferir o produto Bitdefender e, em seguida, clique em **CONTINUAR**. Escreva um endereço de e-mail no campo correspondente e clique em **ENVIAR**.
4. Aguarde pela conclusão da transferência, em seguida, execute o instalador:

Renovar subscrição

Caso não tenha escolhido renovar automaticamente a sua subscrição do Bitdefender, pode renová-la manualmente seguindo estas instruções:

1. Aceda Bitdefender Central.
2. Selecione o painel **As Minhas Subscrições**.
3. Selecione o cartão de subscrição pretendido.

4. Clique em **RENOVAR** para continuar.

Uma página abrirá no seu navegador onde poderá renovar a sua subscrição do Bitdefender.

Ativar subscrição

Uma subscrição pode ser ativada durante o processo de instalação utilizando a sua conta Bitdefender. Com o processo de ativação, o período de validade da subscrição começa a contar.

Caso tenha adquirido um código de ativação de um dos nossos revendedores ou ganho como presente, poderá prolongar a duração de qualquer subscrição do Bitdefender existente disponível na conta, desde que sejam do mesmo produto.

Para ativar uma assinatura utilizando um código de ativação:

1. Aceda Bitdefender Central.
2. Selecione o painel **As Minhas Subscrições**.
3. Clique no botão **CÓDIGO DE ATIVAÇÃO** e, em seguida, escreva o código no campo correspondente.
4. Clique em **ATIVAR** para continuar.

A subscrição está ativada agora. Vá ao painel **Os Meus dispositivos** e selecione **INSTALAR PROTEÇÃO LOCAL** para instalar o produto num dos seus dispositivos.

2.3.2. Meus dispositivos

A área **Os Meus Dispositivos** na Bitdefender Central dá-lhe a possibilidade de instalar, gerir e realizar ações remotas no seu produto Bitdefender em qualquer dispositivo, desde que esteja ligado e com ligação à Internet. Os cartões de dispositivos exibem o nome do dispositivo, o estado da proteção e se há algum risco de segurança afetando a proteção dos seus dispositivos.

Para ver uma lista dos seus dispositivos ordenados de acordo com o seu estado ou utilizadores, clique na seta pendente no canto superior direito do ecrã.

Para identificar facilmente os seus dispositivos, pode personalizar o nome de cada um:

1. Aceda Bitdefender Central.

2. Selecione o painel **Os Meus Dispositivos**.
3. Clique no cartão de dispositivo pretendido e, em seguida, o ícone ⋮ no canto superior direito do ecrã.
4. Selecione **Definições**.
5. Digite um novo nome no campo **Nome do dispositivo** e clique **GUARDAR**.

Caso o Autopilot esteja desligado, pode ligá-lo clicando no botão. Clique em **Guardar** para aplicar as definições.

Pode criar e atribuir um proprietário a cada um dos seus dispositivos para uma melhor gestão:

1. Aceda Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.
3. Clique no cartão de dispositivo pretendido e, em seguida, o ícone ⋮ no canto superior direito do ecrã.
4. Selecione **Perfil**.
5. Clique em **Add owner** e, em seguida, preencha os respetivos campos. Personalize o perfil adicionando uma fotografia e selecionando a data de nascimento.
6. Clique em **ADICIONAR** para guardar o perfil.
7. Selecione o proprietário pretendido na lista **Proprietário do dispositivo** e, em seguida, clique em **ATRIBUIR**.

Para atualizar o Bitdefender remotamente no dispositivo:

1. Aceda Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.
3. Clique no cartão de dispositivo pretendido e, em seguida, o ícone ⋮ no canto superior direito do ecrã.
4. Selecione **Atualizar**.

Para mais ações remotas e informações sobre o seu produto Bitdefender num dispositivo específico, clique no cartão de dispositivo pretendido.

Quando clicar no cartão de dispositivo, ficam disponíveis os seguintes separadores:

- **Painel**. Nesta janela, pode visualizar os detalhes sobre o dispositivo selecionado, verificar o seu estado de proteção, o estado do Bitdefender VPN e quantas ameaças foram bloqueadas nos últimos sete dias. O estado de proteção pode estar verde, quando não houver problemas a afetar o seu dispositivo, amarelo, quando o dispositivo exigir a sua atenção, ou vermelho, quando o dispositivo estiver em risco. Quando houver problemas a afetar o seu dispositivo, clique no seta pendente na área de estado acima para saber mais detalhes. A partir daqui poderá resolver manualmente os problemas que afetam a segurança dos seus dispositivos.
- **Proteção**. Desta janela pode executar uma Verificação Rápida ou do Sistema remotamente nos seus dispositivos. Clique no botão **VERIFICAR** para iniciar o processo. Também pode conferir quando é que a última verificação foi realizada no dispositivo e aceder a um relatório da última verificação, contendo as informações mais importantes.Para mais informações sobre estes dois processos de verificação, consulte "*Executar uma Análise do Sistema*" (p. 92) e "*Executar uma Análise Rápida*" (p. 92).
- **Otimizador**. Aqui pode melhorar remotamente o desempenho de um dispositivo com a verificação, deteção e limpeza remota de ficheiros inúteis. Clique no botão **INICIAR** e, em seguida, selecione as áreas que deseja otimizar. Clique novamente no botão **INICIAR** para iniciar o processo de otimização. Clique na ligação **Mais detalhes** para aceder a um relatório detalhado sobre os problemas resolvidos.

  Além disso, é possível melhorar a inicialização do seu dispositivo ao identificar as aplicações que consomem muitos recursos do sistema. Clique no botão **MAIS DETALHES** e, em seguida, escolha o que deseja fazer com as aplicações detectadas. Para mais detalhes sobre estas funções, consulte "*A otimizar a velocidade do seu sistema com apenas um clique*" (p. 176) e "*A otimizar o tempo de arranque do seu PC.*" (p. 177).
- **Antirroubo**. Em caso de deslocação, roubo ou perda, pode localizar e realizar ações remotas no seu dispositivo com a função Anti-furto. Clique em **LOCALIZAR** para descobrir a localização do seu dispositivo. A última localização conhecida será exibida, juntamente com a hora e com a data. Para mais detalhes sobre esta função, aceda a "*Dispositivo Anti-Roubo*" (p. 172).
- **Vulnerabilidade**. Para verificar um dispositivo e identificar vulnerabilidades, como a falta de atualizações do Windows, aplicações desatualizadas ou palavras-passe fracas, clique no botão **VERIFICAR** no separador Vulnerabilidade. Vulnerabilidades não podem ser corrigidas remotamente.

Caso qualquer vulnerabilidade seja detetada, é necessário executar uma nova verificação no dispositivo e, em seguida, tomar as providências recomendadas. Clique em **Mais detalhes** para aceder a um relatório detalhado sobre os problemas encontrados. Para mais detalhes sobre esta função, aceda a "*Vulnerabilidade*" (p. 125).

2.3.3. Actividade

A área de Atividade na Bitdefender Central está disponível apenas para os utilizadores que têm uma subscrição Bitdefender Family Pack 2018 ou Bitdefender Total Security 2018 vinculada às suas contas. A sua função é informar como o Bitdefender protegeu nos últimos sete dias os dispositivos nos quais está instalado e exibir informações sobre a subscrição incluída.

Ao aceder à janela **ATIVIDADE**, os seguintes cartões são disponibilizados:

- **Proteção**. Aqui é possível visualizar informações sobre os ficheiros, aplicações e URLs que foram bloqueados devido a comportamentos suspeitos. Para mostrar-lhe quando ocorrerem problemas, são disponibilizados gráficos exibindo os dados recolhidos, divididos em dias e número de ameaças detetadas. Além disso, é possível mover o rato sobre os dados exibidos para descobrir o número de ameaças detetadas.

  Na parte inferior do cartão, pode ver o nome do dispositivo com o maior número de ameaças.

- **Otimizar**. Aqui é possível otimizar o desempenho dos dispositivos do Windows nos quais instalou o produto Bitdefender Total Security. As informações apresentadas são baseadas na funcionalidade Otimizador de Arranque que apresenta as aplicações que estão em execução durante o arranque do sistema e permite que administre o comportamento das mesmas neste passo. Dependendo das decisões tomadas pela comunidade ao aplicar o comando **Atrasar**, somente os três primeiros dispositivos são exibidos. Clique em **Aplicar** para aplicar as alterações sugeridas no dispositivo selecionado.

  Para ver as decisões de outros utilizadores do Bitdefender, clique na hiperligação que exibe o número de aplicações detetadas e o tempo economizado. São exibidos detalhes sobre o tempo que o seu sistema precisa para iniciar, o tempo que as aplicações precisam na inicialização e o tempo otimizado. Selecione **ATRASAR TODOS** se deseja que as aplicações parem de ser executadas na inicialização. Para mais

informações sobre a funcionalidade Otimizador de Arranque do Bitdefender, consulte "*A otimizar o tempo de arranque do seu PC.*" (p. 177).

> **Nota**
> Se nenhuma proteção do Bitdefender estiver instalada nos seus dispositivos do Windows, o cartão **Tune Up** não irá conter informações.

- **Subscrição**. Aqui, é possível visualizar quantos dispositivos estão incluídos na sua subscrição e quantos dispositivos têm a proteção Bitdefender instalada. Para instalar o Bitdefender em outros dispositivos, clique no botão **INSTALAR** no sistema operativo desejado e siga os passos necessários.

  O nome da subscrição em utilização é exibido junto de um ponto colorido:

  - Roxo - a sua subscrição está ativa.
  - Vermelho - a sua subscrição está prestes a expirar. Recomendamos que renove o mais rapidamente possível para continuar a manter os seus dispositivos protegidos.

  Clique na hiperligação **Mais detalhes** para ser redirecionado para a página de **Subscrições**, onde é possível ver informações detalhadas sobre a sua subscrição ativa.

2.3.4. Minha Conta

Na área **A minha conta** tem a possibilidade de personalizar o seu perfil, alterar a palavra-passe associada à sua conta, gerir os inícios de sessão e as mensagens de ajuda da Bitdefender Central.

Assim que clicar no ícone no canto superior direito do ecrã e escolher **A minha conta**, surgem os seguintes separadores:

- **Perfil** - onde pode adicionar e editar as informações da conta.
- **Alterar a palavra-passe** - a partir de onde pode alterar a palavra-passe associada à sua conta.
- **Gestão de sessão** - onde pode ver e gerir os últimos inícios de sessão ativos a funcionar em dispositivos associados à sua conta.
- **Definições** - onde pode ligar e desligar as mensagens de ajuda da Bitdefender Central e decida se quer ser notificado ou não quando são tiradas fotografias nos seus dispositivos Android.

2.3.5. Notificações

Para o ajudar a manter-se informado sobre o que se passa com os dispositivos associados à sua conta, o ícone é útil. Quando clicar sobre este ícone, terá uma imagem global que é composta pelas informações sobre a atividade dos produtos do Bitdefender instalados nos seus dispositivos.

2.4. Mantenha o seu Bitdefender atualizado.

Todos os dias são encontradas e identificadas novas ameaças. Por isso é muito importante manter o Bitdefender atualizado com a base de dados de informações de ameaças mais recente.

Se está ligado à Internet através de banda larga ou ADSL, o Bitdefender executa esta operação sozinho. Por defeito, quando liga o computador verifica se há actualizações e depois disso fá-lo a cada **hora** . Se forem detectadas actualizações, serão automaticamente descarregadas e instaladas no seu computador.

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

Importante
Para estar protegido contra as mais recentes ameaças mantenha a Atualização Automática ativada.

Nalgumas situações particulares, a sua intervenção é necessária para manter a proteção do Bitdefender atualizada:

- Se o seu computador se ligar a Internet através de um servidor proxy, você deve configurar as definições do proxy conforme escrito em "*Como posso configurar Bitdefender para usar um proxy de ligação à Internet?*" (p. 79).
- Podem ocorrer erros ao descarregar atualizações com uma ligação lenta à Internet. Para saber mais sobre como superar esses erros, consulte "*Como atualizar o Bitdefender numa ligação à Internet lenta*" (p. 198).
- Se está ligado à Internet através de uma ligação dial-up, então é uma boa ideia adquirir o hábito de atualizar o Bitdefender a seu pedido. Para mais informação, dirija-se a "*A efetuar uma atualização*" (p. 44).

2.4.1. Verifique se o Bitdefender está atualizado

Para verificar quando foi a última atualização do seu Bitdefender, verifique o **Estado de Segurança**, no lado esquerdo da área de Estado.

Para informações mais detalhadas acerca das mais recentes actualizações, verifique os eventos de actualização:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. No separador **Todas**, selecione a notificação referente à última atualização.

Você pode saber quando foram iniciadas as atualizações e obter informações sobre as mesmas (se foram bem sucedidas ou não, se é necessário reiniciar para concluir a instalação). Se necessário, reinicie o sistema quando lhe convier.

2.4.2. A efetuar uma atualização

Para realizar actualizações, é necessária uma ligação à Internet.

Para iniciar uma atualização, faça o seguinte:

- Abra a interface do Bitdefender e clique na ligação **Atualizar agora** localizado abaixo do estado do seu programa.
- Clique com o botão direito no ícone do Bitdefender na barra de sistema e selecione **Atualizar Agora**.

A funcionalidade Atualização irá ligar-se ao servidor de atualização de Bitdefender e verificará se existem atualizações. Se uma atualização é detetada, poderá ser notificado para confirmar a atualização ou a mesma é realizada automaticamente, dependendo das definições de atualização.

Importante
Poderá ser necessário reiniciar o computador quando a actualização tiver terminado. Recomendamos que o faça assim que seja possível.

Também pode realizar atualizações remotamente nos seus dispositivos, desde que estejam ativados e ligados à Internet.

Para atualizar o Bitdefender remotamente no dispositivo:

1. Aceda Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.

3. Clique no cartão de dispositivo pretendido e, em seguida, o ícone ⋮ no canto superior direito do ecrã.
4. Selecione **Atualizar**.

2.4.3. Ligar ou desligar a atualização automática

Para desativar a atualização automática:

1. Clique no ícone ⚙ na barra lateral esquerda da interface do Bitdefender.
2. Selecione o separador **ATUALIZAR**.
3. Clique no botão ON/OFF correspondente.
4. Aparece uma janela de aviso. Tem de confirmar a sua escolha selecionando no menu durante quanto tempo pretende desativar a atualização automática. Pode desativar a atualização automática durante 5, 15 ou 30 minutos, por uma hora, permanentemente ou até ao reinício do sistema.

Atenção
Esta é uma incidência de segurança critica. Recomendamos que desative a atualização automática o menos tempo possível. Se o Bitdefender não for atualizado regularmente, não será capaz de o proteger contra as ameaças mais recentes.

2.4.4. Ajuste das configurações da atualização

As atualizações podem ser executadas através da rede local, da Internet, diretamente ou através de um servidor proxy. Por defeito, o Bitdefender verificará as atualizações a cada hora, via Internet, e instalará as que estejam disponíveis sem o avisar.

As definições de atualização por defeito são adequadas à maioria dos utilizadores e normalmente não tem de as alterar.

Para ajustar as definições de atualização:

1. Clique no ícone ⚙ na barra lateral esquerda da interface do Bitdefender.
2. Selecione o separador **ATUALIZAR** e ajuste as definições de acordo com as suas preferências.

Frequência de atualização

O Bitdefender está configurado para procurar por atualizações a cada hora. Para alterar a frequência de atualização, arraste o marcador pela barra de frequência para definir o intervalo em que as atualizações devem ocorrer.

Atualizar localização

Bitdefender está configurado para ser atualizado a partir dos servidores de atualização de Bitdefender na Internet. A localização de atualização é um endereço genérico da Internet que é automaticamente redireccionado para o servidor de atualização da Bitdefender mais próximo da sua região.

Não altere a localização da atualização exceto se tiver sido aconselhado por um representante da Bitdefender ou pelo administrador da sua rede (se estiver ligado a uma rede no escritório).

Pode voltar à localização de atualização genérica da Internet clicando em **PREDEFINIÇÃO**.

Regras de atualização

Pode escolher entre três formas para descarregar e instalar atualizações:

- **Atualização silenciosa** - O Bitdefender faz automaticamente o download e a implementação da atualização.
- **Avisar antes de descarregar** - sempre que uma atualização está disponível, será consultado antes do download ser feito.
- **Avisar antes de instalar** - cada vez que uma atualização for descarregada, será consultado antes da instalação ser feita.

Algumas atualizações exigem o reinício para concluir a instalação. Por defeito, se for necessário reiniciar após uma actualização, o Bitdefender continuará a trabalhar com os ficheiros antigos até que o utilizador reinicie voluntariamente o computador. Isto serve para evitar que o processo de actualização de Bitdefender interfira com o trabalho do utilizador.

Se quiser ser avisado quando uma atualização requere um reinício, desligue a opção **Adiar reiniciar** clicando no botão correspondente.

2.4.5. Atualizações contínuas

Para garantir que está a utilizar a versão mais recente, o Bitdefender verifica automaticamente a existência de produtos. Estas atualizações podem

apresentar novas funcionalidades e melhorias, corrigir problemas de produto ou atualizar automaticamente para uma nova versão. Quando a nova versão de Bitdefender é fornecida por atualização, as definições personalizadas são guardadas e o procedimento de desinstalação e reinstalação é ignorado.

Estas atualizações exigem um reinício do sistema para iniciar a instalação de ficheiros novos. Quando uma atualização do produto é concluída, uma janela pop-up irá informar para reiniciar o sistema. Se perder esta notificação, pode clicar em **REINICIAR AGORA** na janela Notificações onde é indicada a atualização mais recente ou reiniciar manualmente o sistema.

Nota

As atualizações que incluem novas funcionalidades e melhorias serão entregues apenas aos utilizadores com o Bitdefender 2017 instalado.

3. COMO

3.1. Instalação

3.1.1. Como instalo o Bitdefender num segundo computador?

Caso a subscrição que comprou cubra mais do que um computador, pode utilizar a sua conta Bitdefender para ativar um segundo PC.

Para instalar o Bitdefender num segundo computador:

1. Clique na hiperligação **INSTALAR NOUTRO DISPOSITIVO** no canto inferior direito da interface do Bitdefender.

   Será redirecionado para a página Web da conta Bitdefender. Certifique-se de que tem sessão iniciada com as suas credênciais

2. Na janela que aparece selecione o sistema de funcionamento pretendido e, de seguida, clique **CONTINUAR**.

3. Introduza o endereço de e-mail para o qual devemos enviar a ligação de transferência da instalação da plataforma escolhida.

4. Execute o Bitdefender que transferiu. Aguarde até que o processo de instalação esteja concluído e feche a janela.

O novo dispositivo em que instalou o Bitdefender aparecerá no painel de controlo da Bitdefender Central.

3.1.2. Como posso reinstalar Bitdefender?

As situações típicas em que deve reinstalar Bitdefender são as seguintes:

- você reinstalou o sistema operativo.
- pretende corrigir problemas que causaram abrandamentos e falhas.
- o seu produto Bitdefender não começa ou funciona corretamente.

Caso uma das situações mencionadas seja o seu caso, siga estes passos:

- No **Windows 7**:

  1. Clique em **Iniciar** e vá para **Todos os Programas**.
  2. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
  3. Clique em **REINSTALAR** na janela que aparece.

4. Necessita de reiniciar o computador para concluir o processo.

- No **Windows 8 e Windows 8.1**:
  1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
  2. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
  3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
  4. Clique em **REINSTALAR** na janela que aparece.
  5. Necessita de reiniciar o computador para concluir o processo.
- No **Windows 10**:
  1. Clique em **Iniciar**, em seguida, clique em Definições.
  2. Clique no ícone **Sistema** na área das Definições, em seguida, selecione **Aplicações e funcionalidades**.
  3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
  4. Clique em **Desinstalar** novamente para confirmar a sua escolha.
  5. Clique em **REINSTALAR**.
  6. Necessita de reiniciar o computador para concluir o processo.

> **Nota**
> Ao seguir este procedimento de reinstalação, as definições personalizadas são guardadas e estão disponíveis no novo produto instalado. As outras definições podem ser alteradas novamente para a configuração predefinida.

3.1.3. Onde posso transferir o meu produto Bitdefender?

Pode instalar o Bitdefender do disco de instalação ou através do instalador transferido no seu computador da plataforma Bitdefender Central.

> **Nota**
> Antes de executar o kit, é recomendada a remoção de qualquer solução de segurança instalada no seu sistema. Quando utiliza mais do que uma solução de segurança no mesmo computador, o sistema torna-se instável.

Para instalar o Bitdefender da Bitdefender Central:

1. Aceda Bitdefender Central.

2. Selecione o painel **Os meus dispositivos**, e clique em **INSTALAR PROTEÇÃO LOCAL**.
3. Escolha uma das duas opções disponíveis:
   - **DOWNLOAD**

     Clique no botão e guarde o ficheiro de instalação.
   - **Noutro dispositivo**

     Selecione **Windows** para transferir o produto Bitdefender e, em seguida, clique em **CONTINUAR**. Escreva um endereço de e-mail no campo correspondente e clique em **ENVIAR**.
4. Execute o Bitdefender que transferiu.

3.1.4. Como é que posso alterar o idioma do meu produto Bitdefender?

Se pretender utilizar o Bitdefender noutro idioma, terá que reinstalar o produto com o idioma apropriado.

Para utilizar o Bitdefender noutro idioma:

1. Remova o Bitdefender seguindo estes passos:
   - No **Windows 7**:
     a. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
     b. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
     c. Clique em **REMOVER** na janela que aparece.
     d. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.
   - No **Windows 8 e Windows 8.1**:
     a. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
     b. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
     c. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
     d. Clique em **REMOVER** na janela que aparece.

e. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

- No **Windows 10**:

  a. Clique em **Iniciar**, em seguida, clique em Definições.

  b. Clique no ícone **Sistema** na área das Definições, em seguida, selecione **Aplicações instaladas**.

  c. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.

  d. Clique em **Desinstalar** novamente para confirmar a sua escolha.

  e. Clique em **REMOVER** na janela que aparece.

  f. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

2. Altere o idioma da Bitdefender Central:

   a. Aceda Bitdefender Central.

   b. Clique no ícone no canto superior direito do ecrã.

   c. Clique em **A Minha Conta** no menu deslizante.

   d. Selecione o separador **Perfil**.

   e. Selecione um idioma da caixa da lista suspensa **Idioma** e, em seguida, clique em **GUARDAR**.

3. Transfira o ficheiro de instalação:

   a. Selecione o painel **Os meus dispositivos**, e clique em **INSTALAR PROTEÇÃO LOCAL**.

   b. Escolha uma das duas opções disponíveis:

   - **DOWNLOAD**

     Clique no botão e guarde o ficheiro de instalação.

   - **Noutro dispositivo**

     Selecione **Windows** para transferir o produto Bitdefender e, em seguida, clique em **CONTINUAR**. Escreva um endereço de e-mail no campo correspondente e clique em **ENVIAR**.

4. Execute o Bitdefender que transferiu.

Nota
Este procedimento de reinstalação irá eliminar permanentemente as definições personalizadas.

3.1.5. Como utilizo a minha subscrição do Bitdefender após uma atualização do Windows?

Esta situação ocorre quando atualiza o sistema operativo e pretende continuar a utilizar a subscrição do Bitdefender.

Se estiver a utilizar uma versão anterior do Bitdefender, pode atualizar, gratuitamente para a versão mais recente do Bitdefender, da seguinte forma:

- Da versão anterior do Bitdefender Antivirus para a versão mais recente doBitdefender Antivirus.
- Da versão anterior do Bitdefender Internet Security para a versão mais recente do Bitdefender Internet Security.
- Da versão anterior do Bitdefender Total Security para a versão mais recente do Bitdefender Total Security.

Existem dois casos que podem aparecer:

- Atualizou o sistema operativo utilizando o Windows Update e constata que o Bitdefender já não funciona.

  Neste caso, é necessário reinstalar o produto ao seguir estes passos:

  - No **Windows 7**:

    1. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
    2. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
    3. Clique em **REINSTALAR** na janela que aparece.
    4. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

       Abra a interface do produto Bitdefender recentemente instalado para ter acesso às respetivas funcionalidades.

  - No **Windows 8 e Windows 8.1**:

1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
2. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
4. Clique em **REINSTALAR** na janela que aparece.
5. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

   Abra a interface do produto Bitdefender recentemente instalado para ter acesso às respetivas funcionalidades.

- No **Windows 10**:
  1. Clique em **Iniciar**, em seguida, clique em Definições.
  2. Clique no ícone **Sistema** na área das Definições, em seguida, selecione **Aplicações instaladas**.
  3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
  4. Clique em **Desinstalar** novamente para confirmar a sua escolha.
  5. Clique em **REINSTALAR** na janela que aparece.
  6. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

     Abra a interface do produto Bitdefender recentemente instalado para ter acesso às respetivas funcionalidades.

> **Nota**
> Ao seguir este procedimento de reinstalação, as definições personalizadas são guardadas e estão disponíveis no novo produto instalado. As outras definições podem ser alteradas novamente para a configuração predefinida.

- Alterou o seu sistema e pretende continuar a utilizar a proteção Bitdefender. Portanto, será necessário reinstalar o produto utilizando a versão mais recente.

  Para resolver este problema:

  1. Transfira o ficheiro de instalação:
     a. Aceda Bitdefender Central.

b. Selecione o painel **Os meus dispositivos**, e clique em **INSTALAR PROTEÇÃO LOCAL**.

c. Escolha uma das duas opções disponíveis:

- **DOWNLOAD**

  Clique no botão e guarde o ficheiro de instalação.

- **Noutro dispositivo**

  Selecione **Windows** para transferir o produto Bitdefender e, em seguida, clique em **CONTINUAR**. Escreva um endereço de e-mail no campo correspondente e clique em **ENVIAR**.

2. Execute o Bitdefender que transferiu.

Para obter mais informações sobre o processo de instalação do Bitdefender, consulte "*A instalar Bitdefender Antivirus for Mac*" (p. 222).

3.1.6. Como posso atualizar para a mais recente versão de Bitdefender?

A começar com Bitdefender 2018, a atualização para a versão mais recente é possível sem seguir o procedimento manual de desinstalação e reinstalação. Mais exatamente, o novo produto que inclui novas funcionalidades e melhorias de produto importantes é fornecido por atualização do produto e, se já tiver uma subscrição de Bitdefender ativa, o produto é ativado automaticamente.

Se estiver a utilizar a versão de 2017, é possível atualizar para a versão mais recente ao seguir estes passos:

1. Clique em **REINICIAR AGORA** na notificação recebida com as informações sobre a atualização. Se a perder, aceda à janela Notificações, aponte para a atualização mais recente e clique no botão **REINICIAR AGORA**. Aguarde pelo reinício do computador.

   É apresentada a janela **Novidades** com informações sobre as novas e melhoradas funcionalidades.

2. Clique nas hiperligações **Ler mais** para ser redirecionado para a nossa página dedicada com mais detalhes e artigos úteis.

3. Feche a janela **Novidades** para aceder à interface da nova versão instalada.

Os utilizadores que pretendem atualizar gratuitamente do Bitdefender 2016 ou uma versão inferior para a versão mais recente do Bitdefender têm de remover a versão atual do Painel de Controlo e transferir o ficheiro de instalação mais recente do site Web do Bitdefender no seguinte endereço: https://www.bitdefender.com/Downloads/. A ativação só é possível com uma subscrição válida.

3.2. Assinaturas

3.2.1. Como é que ativo a minha subscrição do Bitdefender através da chave de licença?

Se tiver uma chave de licença e desejar utilizá-la para ativar uma subscrição do Bitdefender Total Security, há dois possíveis casos que podem ser aplicáveis:

- Atualizou uma versão anterior do Bitdefender para a mais recente:
  1. Assim que a atualização para o Bitdefender Total Security estiver concluída, será solicitado que aceda à sua conta Bitdefender.
  2. Clique em **Iniciar Sessão** e depois digite o endereço de e-mail e a palava-passe da sua conta Bitdefender.
  3. Clique em **INICIAR SESSÃO** para continuar.
  4. Uma notificação a informar-lhe de que uma assinatura foi criada aparece no ecrã da sua conta. A subscrição criada será válida pelo número de dias restantes na sua chave de licença e para o mesmo número de utilizadores.

     Dispositivos que utilizem versões anteriores do Bitdefender e que estiverem registadas com a chave de licença que converteu para uma subscrição necessitam de ativar o produto na mesma conta Bitdefender.
- O Bitdefender não foi instalado anteriormente no sistema:
  1. Assim que o processo de instalação estiver concluído, será solicitado que aceda à sua conta Bitdefender.
  2. Clique em **Iniciar Sessão** e depois digite o endereço de e-mail e a palava-passe da sua conta Bitdefender.
  3. Clique em **ENTRAR** para continuar e, em seguida, o botão **CONCLUIR** para aceder à interface Bitdefender Total Security.

4. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
5. Clique na hiperligação **Código de Ativação**.

   Aparece uma nova janela.
6. Clique na ligação **Obtenha a sua atualização GRATUITA agora!**.
7. Introduza a chave de licença no campo correspondente e clique em **ATUALIZAR O MEU PRODUTO**. Uma subscrição com a mesma validade e número de utilizadores da sua chave de licença está associada à sua conta.

3.3. Bitdefender Central

3.3.1. Como é que é inicio sessão na Bitdefender Central utilizando outra conta online?

Criou uma nova conta Bitdefender e pretende utilizá-la de agora em diante.

Para utilizar outra conta com sucesso:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique no botão **ALTERNAR CONTA** para alterar a conta vinculada ao computador.
3. Escreva o endereço de e-mail e a palavra-passe da sua conta nos campos correspondentes, em seguida, clique em **ENTRAR**.

> **Nota**
> O produto Bitdefender do seu dispositivo muda automaticamente de acordo com a subscrição associada à nova conta Bitdefender.
> Se não houver uma subscrição associada à nova conta Bitdefender ou caso pretenda transferi-la da conta anterior, pode contatar o Bitdefender para obter suporte, como descrito na secção "*Pedir Ajuda*" (p. 325).

3.3.2. Como é que desativo as mensagens de ajuda da Bitdefender Central?

As mensagens de ajuda são exibidas no painel para ajudá-lo a entender como cada opção na Bitdefender Central é útil.

Se pretender deixar de ver este tipo de mensagens:

1. Aceda Bitdefender Central.
2. Clique no ícone no canto superior direito do ecrã.
3. Clique em **A Minha Conta** no menu deslizante.
4. Selecione o separador **Definições**.
5. Desative a opção **Ativar/desativar mensagens de ajuda**.

3.3.3. Esqueci-me da palavra-passe que defini para a minha conta Bitdefender. Como é que a reponho?

Existem duas possibilidades para definir uma nova palavra-passe para a sua conta do Bitdefender:

- A partir da interface do Bitdefender:
  1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
  2. Clique no botão **ALTERNAR CONTA**.

     Aparece uma nova janela.
  3. Clique na hiperligação **Esqueci-me da palavra-passe**.
  4. Escreva o endereço de e-mail utilizado para criar a sua conta Bitdefender e, em seguida, clique no botão **ESQUECI-ME DA PALAVRA-PASSE**.
  5. Verifique o seu e-mail e clique no botão fornecido.

     A janela REINICIAR PALAVRA-PASSE do Bitdefender abre.
  6. Digite o seu endereço de e-mail e a nova palavra-passe no campo correspondente. A palavra-passe tem de ter, pelo menos, 8 carateres e incluir números.
  7. Clique no botão **REDEFINIR PALAVRA-PASSE**.
- Do seu navegador Web:
  1. Vá para: https://central.bitdefender.com.
  2. Clique na hiperligação **Esqueci-me da palavra-passe**.
  3. Digite o seu endereço de e-mail e clique no botão **ESQUECI-ME DA PALAVRA-PASSE**.
  4. Verifique a sua conta de e-mail e siga as instruções fornecidas para definir a nova palavra-passe da sua conta Bitdefender.

A partir de agora, para aceder à sua conta Bitdefender, escreva o seu endereço de e-mail e a nova palavra-passe que acabou de definir.

3.3.4. Como posso gerir os inícios de sessão associados à minha conta do Bitdefender?

Na sua conta do Bitdefender tem a possibilidade de ver os últimos inícios de sessão inativos e ativos a funcionar em dispositivos associados à sua conta. Além disso, pode terminar sessão remotamente seguindo os seguintes passos:

1. Aceda Bitdefender Central.
2. Clique no ícone no canto superior direito do ecrã.
3. Clique em **A Minha Conta** no menu deslizante.
4. Selecione o separador **Gestão de sessão**.
5. Na área **Sessões ativas**, selecione a opção **TERMINAR SESSÃO** junto ao dispositivo que pretende terminar a sessão.

3.4. A analisar com Bitdefender

3.4.1. Como posso analisar um ficheiro ou uma pasta?

A forma mais fácil para analisar um ficheiro ou pasta é clicar com o botão direito do rato no objeto a analisar, apontar para o Bitdefender e selecionar **Analisar com o Bitdefender** a partir do menu.

Para concluir a análise, siga o assistente de Análise Antivírus. O Bitdefender tomará automaticamente as ações recomendadas nos ficheiros detetados.

Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas.

Situações típicas em que deve de usar este método de análise são as seguintes:

- Suspeita que um determinado ficheiro ou pasta está infectado.
- Sempre que descarrega ficheiros da Internet que julga serem perigosos.
- Quer analisar uma partilha de rede antes de copiar os ficheiros para o seu computador.

3.4.2. Como posso analisar o seu sistema?

Para realizar uma análise completa no sistema:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **ANTIVÍRUS**, clique em **Análise do sistema**.
4. Siga as instruções do assistente de Verificação do Sistema para concluir a verificação. O Bitdefender tomará automaticamente as ações recomendadas nos ficheiros detetados.

   Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas. Para mais informação, dirija-se a "*Assistente de Análise Antivírus*" (p. 96).

3.4.3. Como programar uma verificação?

Pode configurar o seu produto Bitdefender para iniciar a verificação de locais importantes do sistema quando não estiver a utilizar o computador.

Para agendar uma análise:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **ANTIVÍRUS**, clique em **Gerir análises**.
4. Escolha o tipo de análise que pretende agendar, Análise completa do sistema pu Análise rápida e, de seguida, clique **Opções de análise**.

   Como alternativa, pode criar um tipo de verificação que corresponda às suas necessidades clicando em **Nova tarefa personalizada**.
5. Ativar o botão **Programar**.

   Selecione uma das opções correspondentes para definir uma agenda:

   - No iniciar do sistema
   - Uma vez
   - Periodicamente

Na janela **Verificar alvos**, pode selecionar os locais que pretenda verificar.

3.4.4. Como posso criar uma tarefa de análise personalizada?

Se quer analisar localizações específicas no seu computador ou configurar as opções de análise, pode configurar e executar uma tarefa personalizada.

Para criar uma tarefa de análise personalizada, proceda da seguinte forma:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **ANTIVÍRUS**, clique em **Gerir análises**.
4. Clique em **Nova tarefa personalizada**. Insira um nome para a análise na aba **Básico** e selecione as localizações a serem analisadas.
5. Se desejar configurar detalhadamente as opções de análise, selecione o separador **Avançado**.

   Pode facilmente configurar as opções de análise ajustando o nível de análise. Arraste o cursor pela escala para definir o nível de análise pretendido.

   Também pode optar por desligar o computador sempre que a análise termina, se não forem encontradas ameaças. Lembre-se de que esta será a ação por defeito sempre que executar esta tarefa.
6. Clique em **OK** para guardar as alterações e fechar a janela.
7. Utilize o botão correspondente se pretender definir uma agenda para a sua tarefa de verificação.
8. Clique em **Iniciar Análise** e siga o assistente de análise para a concluir. No final da análise, será notificado para escolher as ações que devem ser tomadas nos ficheiros detetados, caso os haja.
9. Se quiser, pode voltar a executar rapidamente uma análise personalizada anterior ao clicar na entrada correspondente na lista disponível.

3.4.5. Como posso excluir uma pasta da análise?

O Bitdefender permite excluir ficheiros, pastas ou extensões de ficheiros específicos da análise.

As exceções devem ser usadas pelos utilizadores que possuem conhecimento informáticos avançados e apenas nas seguintes situações:

- Você tem uma pasta grande no seu sistema onde guarda filmes e música.
- Você tem um ficheiro grande no seu sistema onde guarda diferentes dados.
- Você tem uma pasta onde instala diferentes tipos de software e aplicações para testar. A análise da pasta pode resultar na perda de alguns dados.

Para adicionar uma pasta à lista de exclusões:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **ANTIVÍRUS**.
4. Clique no separador **EXCLUSÕES**.
5. Clique no menu em acordeão **Lista de ficheiros e pastas excluídas da análise** e no botão **ADICIONAR**.
6. Clique em **Procurar**, selecione a pasta que pretende excluir da análise e escolha o tipo de análise da qual deve ser excluída.
7. Clique em **Adicionar** para guardar as alterações e fechar a janela.

3.4.6. O que fazer se o Bitdefender identificar um ficheiro limpo como infectado?

Pode haver casos em que o Bitdefender assinala erradamente um ficheiro legítimo como sendo uma ameaça (um falso positivo). Para corrigir este erro, adicione o ficheiro à área de Exceções do Bitdefender:

1. Desative a proteção antivírus em tempo real do Bitdefender:
   a. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
   b. Clique na hiperligação **VER FUNCIONALIDADES**.
   c. Clique no ícone no canto inferior direito do painel **ANTIVÍRUS**.
   d. Na janela **PROTEÇÃO**, clique no botão LIGAR/DESLIGAR.

      Aparece uma janela de aviso. Tem de confirmar a sua escolha seleccionando no menu durante quanto tempo pretende desactivar a protecção em tempo real. Pode desativar a sua proteção em tempo

real durante 5, 15 ou 30 minutos, por uma hora, permanentemente ou até ao reinício do sistema.

2. Mostrar objetos ocultos no Windows. Para saber como o fazer, consulte "*Como posso mostrar objetos ocultos no Windows?*" (p. 81).
3. Restaurar o ficheiro da área de Quarentena:
   a. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
   b. Clique na hiperligação **VER FUNCIONALIDADES**.
   c. No painel **ANTIVÍRUS**, clique em **Quarantena**.
   d. Selecione o ficheiro e, em seguida, clique em **RESTAURAR**.
4. Adicionar o ficheiro à lista de Exceções. Para saber como o fazer, consulte "*Como posso excluir uma pasta da análise?*" (p. 60).
5. Ligue a proteção antivírus em tempo real do Bitdefender.
6. Contacte os nossos representantes do suporte para que possamos remover a deteção de atualizações de informações sobre ameaças. Para saber como o fazer, consulte "*Pedir Ajuda*" (p. 325).

3.4.7. Como posso saber que ameaças o Bitdefender detetou?

Cada vez que uma análise é levada a cabo, um registo de análise é criado e o Bitdefender regista as incidências detetadas.

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.

Pode abrir o relatório diretamente no assistente de análise, assim que esta terminar, clicando em **MOSTRAR RELATÓRIO**.

Para verificar um registo de análise ou qualquer infeção detetada posteriormente:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. No separador **Todas**, selecione a notificação referente à última análise.

   Aqui poderá encontrar todos os eventos de análise de ameaças, incluindo ameaças detectadas na análise no acesso, análises iniciadas pelo utilizador e alterações de estado para as análises automáticas.

3. Na lista de notificações, pode ver as análises que foram recentemente efectuadas. Clique numa notificação para visualizar detalhes sobre o mesmo.
4. Para abrir um relatório da análise, clique em **VER RELATÓRIO**.

3.5. Consultor Parental

3.5.1. Como posso proteger os meus filhos de ameaças online?

O Consultor Parental do Bitdefender permite-lhe restringir o acesso à Internet e a determinadas aplicações, impedindo os seus filhos de visualizarem conteúdos inapropriados sempre que não está por perto.

Para configurar o Consultor Parental:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **CONTROLO PARENTAL**, clique em **Configurar**.

   Será redirecionado para a página Web da conta Bitdefender. Certifique-se de que tem sessão iniciada com as suas credênciais
4. O painel do Consultor Parental abre. Aqui é onde poderá verificar e configurar as definições do Consultor Parental.
5. Clique em **ADICIONAR PERFIL** no lado direito da janela **OS MEUS FILHOS**.
6. Preencha os campos correspondentes com as informações específicas, tais como: nome e data de nascimento. Para adicionar uma foto de perfil, clique na ligação **Escolher um ficheiro**. Clique em **SEGUINTE** para continuar.

   Com base no desenvolvimento infantil, definir a idade da criança carrega automaticamente as definições para pesquisar na Web consideradas apropriadas para a sua faixa etária.
7. Caso o dispositivo do seu filho já possua o Bitdefender Total Security instalado, selecione o dispositivo da lista disponível e selecione a conta que pretende monitorizar. Clique em **GUARDAR**.

   Se o seu filho utilizar um dispositivo Android e a aplicação Controlo Parental do Bitdefender não estiver instalada, clique em **ADICIONAR**

DISPOSITIVO. Se o seu filho utilizar um dispositivo Mac e a aplicação Bitdefender Antivirus for Mac não estiver instalada, clique no mesmo botão. Selecione o sistema operativo onde pretende instalar a aplicação e clique em **PRÓXIMO PASSO** para continuar.

8. Digite o endereço de e-mail para onde devemos enviar a hiperligação de transferência de instalação da aplicação Bitdefender e clique em **ENVIAR HIPERLIGAÇÃO DE INSTALAÇÃO**.

Verifique a atividade dos seus filhos e altere as definições do Consultor Parental utilizando a conta Bitdefender a partir de qualquer computador ou dispositivo móvel ligado à Internet.

Importante
Em dispositivos com Windows, o Bitdefender Total Security que incluir na sua subscrição tem de ser transferido e instalado.
Em dispositivos macOS, o produto Bitdefender Antivirus for Mac tem de ser transferido e instalado.
Em dispositivos Android e iOS, a aplicação Controlo Parental do Bitdefender tem de ser transferida e instalada.

3.5.2. Como bloqueio o acesso do meu filho a um website?

O Consultor Parental do Bitdefender permite-lhe controlar o conteúdo acedido pelos seus filhos nos seus dispositivos, permitindo-lhe bloquear igualmente o acesso a determinados sites.

Para bloquear o acesso a um site Web, necessita de adicioná-lo à lista de Exceções, conforme se segue:

1. Vá para: https://central.bitdefender.com.
2. Inicie sessão na sua conta Bitdefender utilizando o seu endereço de e-mail e palavra-passe.
3. Clique em **Consultor Parental** para aceder ao painel.
4. Selecione o perfil do seu filho na janela **OS MEUS FILHOS**.
5. Selecione a barra **Websites**.
6. Clique no botão **GERIR**.
7. Escreva o endereço da página que deseja bloquear no campo correspondente.
8. Selecione **Permitir** ou **Bloquear**.

9. Clique em **TERMINAR** para guardar as alterações.

> **Nota**
> As restrições só podem ser definidas para dispositivos Android e Windows.

3.5.3. Como impeço o meu filho de jogar um jogo?

O Consultor Parental do Bitdefender permite-lhe controlar o conteúdo a que o seu filho acede quando usa o computador.

Para bloquear o acesso a um jogo:

1. Vá para: https://central.bitdefender.com.
2. Inicie sessão na sua conta Bitdefender utilizando o seu endereço de e-mail e palavra-passe.
3. Clique em **Consultor Parental** para aceder ao painel.
4. Selecione o perfil do seu filho na janela **OS MEUS FILHOS**.
5. Selecione no separador **Aplicações**.

   Uma lista com cartões será exibida. Os cartões representam as aplicações que o seu filho utiliza.
6. Selecione o cartão com a aplicação que pretende que o seu filho pare de utilizar.

   O símbolo de marcação que aparecerá indica que o seu filho não poderá utilizar a aplicação.

3.5.4. Como previno que os meus filhos entrem em contato com pessoas desconhecidas?

O Consultor Parental do Bitdefender possibilita-lhe bloquear as chamadas de números desconhecidos ou de amigos na lista de contatos do seu filho.

Para bloquear um contacto específico num dispositivo Android que tem a aplicação Controlo Parental do Bitdefender instalada:

1. Vá para: https://central.bitdefender.com.
2. Inicie sessão na sua conta Bitdefender utilizando o seu endereço de e-mail e palavra-passe.
3. Clique em **Consultor Parental** para aceder ao painel.

4. Selecione o perfil da criança que pretenda estabelecer restrições.
5. Selecione o separador **Contactos telefónicos**.

   Uma lista com cartões será exibida. Os cartões representam os contatos do telefone do seu filho.
6. Selecione o cartão com o número de telefone que pretende bloquear.

   O símbolo de marcação que aparecerá indica que o seu filho não poderá ser contatado pelo número de telefone selecionado.

Para bloquear um contacto específico num dispositivo Android que não tem a aplicação Controlo Parental do Bitdefender instalada:

1. Vá para: https://central.bitdefender.com.
2. Inicie sessão na sua conta Bitdefender utilizando o seu endereço de e-mail e palavra-passe.
3. Clique em **Consultor Parental** para aceder ao painel.
4. Selecione o perfil da criança que pretenda estabelecer restrições.
5. Clique na ligação **Instale Parental Advisor num dispositivo** no cartão pretendido.
6. Clique em **ADICIONAR O DISPOSITIVO** na janela que aparece.
7. A opção **Parental Advisor DO Bitdefender para Android** é seleciona por predefinição. Clique em **SEGUINTE** para continuar e, de seguida, instale a aplicação no dispositivo pretendido.
8. Selecione o separador **Contactos telefónicos**.

   Uma lista com cartões será exibida. Os cartões representam os contactos do smartphone Android do seu filho.
9. Selecione o cartão com o número de telefone que pretende bloquear.

   O símbolo de marcação que aparecerá indica que o seu filho não poderá ser contatado pelo número de telefone selecionado.

Para bloquear números desconhecidos, ative o botão **Bloquear interações com números desconhecidos**.

Nota

As restrições de chamadas telefónicas só podem ser definidas para dispositivos Android adicionados ao perfil do seu filho.

3.5.5. Como posso definir um local como seguro ou restrito para o meu filho?

O Consultor Parental do Bitdefender permite-lhe definir um local como seguro ou restrito para o seu filho.

Para definir uma localização:

1. Vá para: https://central.bitdefender.com.
2. Inicie sessão na sua conta Bitdefender utilizando o seu endereço de e-mail e palavra-passe.
3. Clique em **Consultor Parental** para aceder ao painel.
4. Selecione o perfil do seu filho na janela **OS MEUS FILHOS**.
5. Selecione no separador **Local da criança**.
6. Clique em **Dispositivos** dentro da janela **Localização da criança**.
7. Clique em **ESCOLHER DISPOSITIVOS** e, em seguida, selecione o dispositivo que pretende configurar.
8. Na janela **Áreas**, clique no botão **ADICIONAR ÁREA**.
9. Escolha o tipo de local, **SEGURO** ou **RESTRITO**.
10. Escreva um nome válido para a área onde o seu filho tenha ou não permissão para aceder.
11. Defina a distância que deverá ser utilizada para monitorização na barra **Raio**.
12. Clique em **ADICIONAR ÁREA** para guardar as suas definições.

Sempre que quiser marcar uma região restrita como segura, ou uma segura como restrita, clique na mesma e, em seguida, clique no botão **EDITAR ÁREA**. Dependendo da mudança que desejar realizar, selecione a opção **SEGURO** ou **RESTRITO** e clique em **ATUALIZAR ÁREA**.

3.5.6. Como posso bloquear o acesso do meu filho a dispositivos atribuídos durante os dias de escola?

Bitdefender Parental Advisor permite-lhe limitar o acesso do seu filho a dispositivos atribuídos durante as horas da escola e quando os trabalhos de casa devem ser feitos.

Para configurar as restrições:

1. Aceda ao painel do Consultor Parental a partir da Bitdefender Central.
2. Na janela **O MEU FILHO** selecione o perfil da criança no qual pretende definir as restrições.
3. Selecione o separador **Programação**.
4. Na área **LIMITES DIÁRIOS**, clique **ESPECÍFICO**.
5. Selecione a caixa de verificação **Limites de tempo em dias de escola**.
6. Selecione na grelha os intervalos de tempo durante os quais o acesso deve estar bloqueado.

Nota
As restrições só podem ser definidas para dispositivos Android e Windows.

3.5.7. Como posso bloquear o acesso do meu filho a dispositivos atribuídos durante as noites de escola?

Bitdefender Parental Advisor permite-lhe limitar o acesso do seu filho aos dispositivos atribuídos durante as noites de escola.

Para configurar as restrições:

1. Aceda ao painel do Consultor Parental a partir da Bitdefender Central.
2. Na janela **O MEU FILHO** selecione o perfil da criança no qual pretende definir as restrições.
3. Selecione o separador **Programação**.
4. Na área **Hora de dormir**, selecione a caixa de verificação **Noites de escola**.
5. Utilize as setas para cima e para baixo das caixas correspondentes para definir os intervalos de tempo durante os quais o acesso deve ser bloqueado.

Nota
As restrições só podem ser definidas para dispositivos Android e Windows.

3.5.8. Como posso bloquear o acesso do meu filho a dispositivos atribuídos durante os fins de semana?

Bitdefender Parental Advisor permite-lhe limitar o acesso do seu filho aos dispositivos atribuídos durante os dias e noites do fim de semana.

Para configurar as restrições:

1. Aceda ao painel do Consultor Parental a partir da Bitdefender Central.
2. Na janela **O MEU FILHO** selecione o perfil da criança no qual pretende definir as restrições.
3. Selecione o separador **Programação**.
4. Na área **Hora de dormir**, selecione a caixa de verificação **Noites de fim de semana**.
5. Utilize as setas para cima e para baixo das caixas correspondentes para definir os intervalos de tempo durante os quais o acesso deve ser bloqueado.
6. Na área de **LIMITES DIÁRIOS** tem as seguintes opções:
   - **CUMULATIVO**
     a. Selecione a caixa de verificação **Limites de tempo em dias de fim de semana**.
     b. Arraste o cursor ao longo da escala para definir durante quanto tempo o acesso aos dispositivos é permitido.
   - **ESPECÍFICO**
     a. Selecione a caixa de verificação **Limites de tempo em dias de fim de semana**.
     b. Selecione na grelha os intervalos de tempo durante os quais o acesso deve estar bloqueado.

   note que as definições **CUMULATIVO** e **ESPECÍFICO** são concebidas para não funcionarem em conjunto.

Nota
As restrições só podem ser definidas para dispositivos Android e Windows.

3.5.9. Como remover um perfil de criança

Se pretender remover um perfil infantil existente:

1. Vá para: https://central.bitdefender.com.
2. Inicie sessão na sua conta Bitdefender utilizando o seu endereço de e-mail e palavra-passe.
3. Clique em **Consultor Parental** para aceder ao painel.
4. Clique no ícone ⋮ do perfil da criança que prtende eliminar e, em seguida, selecione **Remover**.

3.6. Protecção de Privacidade

3.6.1. Como posso ter a certeza de que a minha transação online é segura?

Para ter a certeza de que as suas operações online se mantém privadas, pode usar o browser fornecido pelo Bitdefender para proteger as suas transações e as suas aplicações bancárias.

O Bitdefender Safepay™ é um navegador desenhado para proteger as informações do seu cartão de crédito, número de conta ou qualquer outro dado pessoal que possa utilizar enquanto acede a diferentes localizações online.

Para manter a sua atividade online segura e privada:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique no botão de ação **Safepay**.
3. Clique no ícone para aceder ao **Teclado Virtual**.

   Use o **Teclado Virtual** quando inserir informação sensível tal como palavras-passe.

3.6.2. O que posso fazer se o meu dispositivo tiver sido roubado?

O roubo de dispositivos móveis, seja um smartphone, um tablet ou um portátil é um dos principais problemas que afetam os indivíduos e as organizações de todo o mundo nos dias de hoje.

O Anti-Roubo do Bitdefender permite não só localizar e bloquear o dispositivo roubado, como também apagar todos os dados para garantir que não será utilizado pelo ladrão.

Para aceder às funções anti-furto da sua conta:

1. Aceda Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.
3. Clique no cartão do dispositivo pretendido e, em seguida, selecione **Anti-furto**.
4. Selecione a funcionalidade que deseja usar:
   - **LOCALIZAR** - exibe a localização do seu dispositivo no Google Maps.
   - **Alerta** - emite um alerta no dispositivo.
   - **Bloquear** - bloqueie o seu computador e defina um código numérico PIN para o desbloquear. Alternativamente, ative a opção correspondente para permitir que o Bitdefender tire fotos da pessoa que está a tentar aceder ao seu dispositivo.
   - **Apagar** - apaga toda a informação do seu computador.

     Importante
     Após apagar toda a informação de um dispositivo, todas as funcionalidades Anti-Roubo deixam de funcionar.

   - **Mostrar IP** - exibe o último endereço de IP para o dispositivo selecionado.

3.6.3. Como posso usar os cofres de ficheiros?

O Cofre de Ficheiros Bitdefender permite-lhe criar unidades lógicas encriptadas, e protegidas por palavra-passe (cofres) no seu computador onde pode armazenar em segurança os seus documentos confidenciais e sensíveis. Fisicamente, o cofre é um ficheiros armazenado no seu disco rígido local com a extensão .bvd.

Ao criar um cofre de ficheiros, há dois coisas importantes: o tamanho e a palavra-passe. O tamanho predefinido de 100 MB deve ser o suficiente para os seus documentos privados, ficheiros Excel e outros dados semelhantes. No entanto, para vídeos ou ficheiros de grandes dimensões, poderá precisar de mais espaço.

Para proteger totalmente os ficheiros ou pastas confidenciais ou sensíveis nos cofres de ficheiros do Bitdefender:

- **Crie um cofre de ficheiros e defina uma palavra-passe forte para ele.**

  Para criar um cofre, clique com o botão direito numa área vazia do ambiente de trabalho ou numa pasta no seu computador, aponte para o **Bitdefender** > **Cofre de Ficheiros do Bitdefender** e selecione **Criar Cofre de Ficheiros**.

  Aparece uma nova janela. Proceder da seguinte forma:

  1. Clique em **Explorar** para selecionar a localização do cofre e guarde o cofre de ficheiros sob o nome desejado.
  2. Escolha a letra da drive a partir do menu. Quando abre o cofre, um disco virtual com a letra selecionada aparecerá em **O Meu Computador**.
  3. Insira a palavra-passe do cofre nos campos **Palavra-passe** e **Confirmar**.
  4. Se deseja mudar o tamanho por defeito (100 MB) do cofre, utilize as setas para cima e para baixo na caixa **Tamanho do Cofre (MB)**.
  5. Clique em **Criar**.

  > **Nota**
  > Quando abre o cofre, um disco virtual aparece em **O Meu Computador**. A drive tem a denominação da letra que atribuiu ao cofre.

- **Adicione os ficheiros e as pastas que deseja proteger no cofre.**

  Para adicionar um ficheiro a um cofre, tem de abrir o cofre primeiro.

  1. Procure o ficheiro de cofre .bvd.
  2. Clique com o botão direito no ficheiro do cofre, aponte para Cofre de Ficheiros Bitdefender e selecione **Abrir**.
  3. Na janela que aparecer, introduza a palavra-passe, selecione uma letra de unidade atribuir ao cofre e clique em **OK**.

  Agora, pode efetuar operações na unidade que corresponde ao cofre de ficheiros pretendido com o Explorador do Windows, tal como faria com qualquer outra unidade. Para adicionar um ficheiro a um cofre aberto, também pode clicar com o botão direito no ficheiro, apontar para o Cofre de Ficheiros Bitdefender e selecione **Adicionar ao cofre de ficheiros**.

- **Mantenha o cofre sempre fechado.**

Só abra os cofres quando precisar de aceder ou gerir o conteúdo. Para fechar um cofre, clique com o botão-direito do rato no correspondente disco virtual no **Meu Computador**, aponte para **Cofre de Ficheiros Bitdefender** e selecione **Fechar**.

- **Certifique-se que não elimina o ficheiro de cofre .bvd.**

  Eliminar o ficheiro também elimina o conteúdo do cofre.

Para mais informações sobre como trabalhar com cofres de ficheiros, por favor consulte "*Encriptação de ficheiro*" (p. 138).

3.6.4. Como removo um ficheiro permanentemente com o Bitdefender?

Se deseja remover um ficheiro permanentemente do seu sistema, necessita de apagar a informação fisicamente do seu disco duro.

O Destruidor de Ficheiros do Bitdefender pode ajudá-lo a rapidamente destruir ficheiros ou pastas do seu computador usando o menu contextual Windows, seguindo os seguintes passos:

1. Clique com o botão direito do rato no ficheiro ou pasta que deseja apagar permanentemente, aponte para o Bitdefender e selecione **Destruidor de Ficheiros**.
2. Aparece uma janela de confirmação. Clique em **SIM, ELIMINAR** para iniciar o assistente de destruidora de papel.

   Aguarde que o Bitdefender termine a destruição dos ficheiros.
3. Os resultados são apresentados. Clique em **TERMINAR** para sair do assistente.

3.6.5. Como protejo a minha câmara Web contra hacking?

Pode configurar o produto Bitdefender para permitir ou negar o acesso das aplicações instaladas à sua câmara Web ao seguir estes passos:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **PROTEÇÃO DA CÂMARA WEB**, clique em **Acesso à câmara Web**.

   É apresentada a lista com as aplicações que pediram acesso à sua câmara.

4. Aponte para a aplicação cujo acesso pretende permitir ou recusar e clique no botão correspondente.

   Para ver o que os outros utilizadores do Bitdefender optaram por fazer com a aplicação selecionada, clique no ícone . Será notificado sempre que uma aplicação das aplicações listadas for bloqueada pelos utilizadores do Bitdefender, independentemente do estado do Piloto Automático.

Para adicionar manualmente aplicações a esta lista, clique na hiperligação **Adicionar uma nova aplicação à lista**.

3.7. Ferramentas de Otimização

3.7.1. Como posso usar melhorar o desempenho do meu sistema?

O desempenho do sistema não depende apenas das características do hardware, tais como a capacidade do CPU, a memória disponível e o espaço no disco rígido. Está, também, diretamente relacionada com a configuração do software e com a gestão dos dados.

Estas são as ações principais que pode efetuar com o Bitdefender para melhorar a velocidade e o desempenho do seu sistema:

- "*Otimize o desempenho do seu sistema com um único clique*" (p. 74)
- "*Analise o seu sistema periodicamente*" (p. 75)

Otimize o desempenho do seu sistema com um único clique

A opção Otimizador de Um Clique poupa-lhe quando quer uma maneira rápida de melhorar o desempenho do sistema ao analisar, detectar e limpar rapidamente ficheiros inúteis.

Para iniciar o processo do OneClick Optimizer:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique no botão de ação **OneClick Optimizer**.
3. Deixe que o Bitdefender procure ficheiros que possam ser eliminados, depois clique no botão **OTIMIZAR** para concluir o processo.

Para mais informações sobre como pode melhorar a velocidade do seu computador com um único clique, consulte "*A otimizar a velocidade do seu sistema com apenas um clique*" (p. 176).

Analise o seu sistema periodicamente

A velocidade do seu sistema e o seu comportamento geral também podem ser afetados pelas ameaças.

Certifique-se de que analisa o seu sistema periodicamente, pelo menos uma vez por semana.

Recomenda-se a utilização da Análise do Sistema pois a mesma analisa todos os tipos de ameaças que prejudicam a segurança do seu sistema e também analisa dentro dos ficheiros.

Para iniciar a Verificação do Sistema:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **ANTIVÍRUS**, clique em **Análise do sistema**.
4. Siga os passos do assistente.

3.7.2. Como posso melhorar o tempo de arranque do meu sistema?

As aplicações desnecessárias que deixam o tempo de inicialização irritantemente mais lento quando abre o seu PC podem ter a sua abertura desativada ou adiada com o Otimizador de Inicialização, poupando-lhe, assim, tempo valioso.

Para utilizar o Startup Optimizer:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique no botão de ação **Startup Optimizer**.
3. Selecione as aplicações que quer adiar no arranque do sistema.

Para mais informações sobre como otimizar o tempo de arranque do seu PC, consulte "*A otimizar o tempo de arranque do seu PC.*" (p. 177).

3.8. Informações Úteis

3.8.1. Como posso testar a minha solução de segurança?

Para garantir que o seu produto Bitdefender está a funcionar corretamente, recomendamos a utilização do teste Eicar.

O teste Eicar permite que verifique a sua solução de segurança utilizando um ficheiro de segurança desenvolvido para este fim.

Para testar a sua solução de segurança:

1. Transfira o teste da página Web oficial da organização EICAR http://www.eicar.org/.
2. Clique no separador **Ficheiro de teste antimalware**.
3. Clique em **Transferir** no menu do lado esquerdo.
4. A partir da **área de transferência utilizando o protocolo padrão http** clique no ficheiro de teste **eicar.com**.
5. Receberá informações de que a página a que está a tentar aceder contém o Ficheiro de Teste EICAR (não é uma ameaça).

   Caso clique em **Compreendo os riscos, leve-me até lá mesmo assim**, a transferência do teste irá iniciar e um pop-up do Bitdefender irá informá-lo da deteção de uma ameaça.

   Clique em **Mais Detalhes** para obter mais informações sobre esta ação.

Caso não receba qualquer alerta de Bitdefender, recomendamos que entre em contacto com Bitdefender para suporte conforme descrito na secção "*Pedir Ajuda*" (p. 325).

3.8.2. Como posso remover o Bitdefender?

Se pretender remover o seu Bitdefender Total Security:

- No **Windows 7**:
  1. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
  2. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
  3. Clique em **REMOVER** na janela que aparece.

4. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

- No **Windows 8 e Windows 8.1**:

1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
2. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
4. Clique em **REMOVER** na janela que aparece.
5. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

- No **Windows 10**:

1. Clique em **Iniciar**, em seguida, clique em Definições.
2. Clique no ícone **Sistema** na área das Definições, em seguida, selecione **Aplicações instaladas**.
3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
4. Clique em **Desinstalar** novamente para confirmar a sua escolha.
5. Clique em **REMOVER** na janela que aparece.
6. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

Nota
Este procedimento de reinstalação irá eliminar permanentemente as definições personalizadas.

3.8.3. Como removo o Bitdefender VPN?

O procedimento de remoção do Bitdefender VPN é semelhante ao que utiliza para remover outros programas do seu computador

- No **Windows 7**:

1. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
2. Encontre **Bitdefender VPN** e selecione **Desinstalar**.

Aguarde até que o processo de desinstalação seja concluído.

- No **Windows 8 e Windows 8.1**:
  1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
  2. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
  3. Encontre **Bitdefender VPN** e selecione **Desinstalar**.

     Aguarde até que o processo de desinstalação seja concluído.
- No **Windows 10**:
  1. Clique em **Iniciar**, em seguida, clique em Definições.
  2. Clique no ícone **Sistema** na área das Definições, em seguida, selecione **Aplicações instaladas**.
  3. Encontre **Bitdefender VPN** e selecione **Desinstalar**.
  4. Clique em **Desinstalar** novamente para confirmar a sua escolha.

     Aguarde até que o processo de desinstalação seja concluído.

3.8.4. Como desligo automaticamente o meu computador após terminar a análise?

O Bitdefender oferece múltiplas tarefas de análise que pode usar para se certificar que o seu sistema não está infectado com ameaças. Analisar todo o computador pode levar muito mais tempo a completar dependendo do hardware do seu sistema e da configuração do seu software.

Por este motivo, o Bitdefender permite-lhe configurar o produto para desligar o computador assim que a análise terminar.

Por exemplo: terminou de trabalhar no seu computador e deseja ir dormir. Gostaria que o seu sistema fosse completamente analisado quanto a ameaças pelo Bitdefender.

Eis como define o Bitdefender para desligar o seu computador no final da análise:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.

3. No painel **ANTIVÍRUS**, clique em **Gerir análises**.
4. Na janela **GERIR TAREFAS DE ANÁLISE**, clique em **Nova tarefa personalizada** para introduzir um nome para a análise e selecione os locais a serem analisados.
5. Se desejar configurar detalhadamente as opções de análise, selecione o separador **Avançado**.
6. Opte por desligar o computador sempre que a análise terminar e se não forem encontradas ameaças.
7. Clique em **OK** para guardar as alterações e fechar a janela.
8. Clique no botão **Iniciar Análise** para verificar o seu sistema.

Se não forem encontradas ameaças, o computador desliga-se.

Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas. Para mais informação, dirija-se a "*Assistente de Análise Antivírus*" (p. 96).

3.8.5. Como posso configurar Bitdefender para usar um proxy de ligação à Internet?

Se o seu computador se ligar a Internet através de um servidor proxy, você deve configurar as definições do proxy do Bitdefender. Normalmente, o Bitdefender deteta e importa automaticamente as definições proxy do seu sistema.

> **Importante**
> As ligações à Internet domésticas normalmente não usam um servidor proxy. Como regra de ouro, verifique e configure as definições da ligação proxy do seu programa Bitdefender quando as atualizações não funcionam. Se o Bitdefender atualizar, então está corretamente configurado à Internet.

Para gerir as definições de proxy:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Selecione o separador **AVANÇADO**.
3. Ative a utilização de proxy ao clicar no botão correspondente.
4. Clique na ligação **Gerir proxies**.
5. Existem duas opções para as definições do proxy:

- **Importe as definições de proxy do navegador por defeito** - as definições de proxy do utilizador actual, extraídas do explorador por defeito. Se o servidor proxy requer um nome de utilizador e uma palavra-passe, deverá inseri-los nos campos correspondentes.

  Nota
  O Bitdefender pode importar definições de proxy dos browsers mais populares, incluindo as mais recentes versões do Microsoft Edge, Internet Explorer, Mozilla Firefox e Google Chrome.

- **Definições de proxy personalizadas** - definições de proxy que você pode configurar. As seguintes definições devem ser especificadas:
  - **Endereço** - introduza o IP do servidor proxy.
  - **Porta** - insira a porta que o Bitdefender usa para se ligar ao servidor proxy.
  - **Nome de Utilizador** - introduza um nome de utilizador reconhecido pelo proxy.
  - **Palavra-passe** - introduza uma palavra-passe válida para o utilizador previamente definido.

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

O Bitdefender usará as definições de proxy disponíveis até conseguir ligar à Internet.

3.8.6. Estou a utilizar uma versão de 32 ou 64 Bit do Windows?

Para descobrir se possui sistema operativo de 32 bits ou 64 bits:

- No **Windows 7**:
  1. Clique em **Iniciar**.
  2. Localize o **Computador** no menu **Iniciar**.
  3. Clique com o botão direito em **Computador** e selecione **Propriedades**.
  4. Procure na secção **Sistema** a informação sobre o seu sistema.
- No **Windows 8**:
  1. A partir do ecrã Iniciar do Windows, localize **Computador** (por exemplo, pode começar a digitar "Computador" diretamente no menu Iniciar) e, em seguida, clique com o botão direito do rato no seu ícone.

No **Windows 8.1**, localize **Este PC**.

2. Selecione **Propriedades** no menu inferior.
3. Procure na área do Sistema o seu tipo de sistema.

- No **Windows 10**:

1. Introduza "Sistema" na caixa de pesquisa da barra de tarefas e, em seguida, clique no ícone correspondente.
2. Procure por informações sobre o tipo do sistema na área do Sistema.

3.8.7. Como posso mostrar objetos ocultos no Windows?

Estes passos são úteis nos casos de ameaças e se tiver de encontrar e remover os ficheiros infectados, que poderão estar ocultos.

Siga os seguintes passos para mostrar objetos ocultos no Windows:

1. Clique em **Iniciar**, aceda ao **Painel de Controlo**.

   No **Windows 8 e Windows 8.1**: a partir do ecrã Iniciar do Windows, localize o **Painel de Controlo** (por exemplo, introduza "Painel de Controlo" no ecrã Iniciar) e, em seguida, clique no ícone correspondente.
2. Selecione **Opções de Pastas**.
3. Abra o separador **Ver**.
4. Selecione **Mostrar ficheiros e pastas ocultos**.
5. Desmarque **Ocultar extensões nos tipos de ficheiro conhecidos**.
6. Desmarque **Ocultar ficheiros protegidos do sistema operativo**.
7. Clique em **Aplicar**, em seguida, clique em **OK**.

No **Windows 10**:

1. Introduza "Mostrar ficheiros e pastas ocultos" na caixa de pesquisa da barra de tarefas e, em seguida, clique no ícone correspondente.
2. Selecione **Mostrar ficheiros, pastas e unidades ocultos**.
3. Desmarque **Ocultar extensões nos tipos de ficheiro conhecidos**.
4. Desmarque **Ocultar ficheiros protegidos do sistema operativo**.
5. Clique em **Aplicar**, em seguida, clique em **OK**.

3.8.8. Como posso remover outras soluções de segurança?

A principal razão para utilizar uma solução de segurança é proporcionar proteção e segurança aos seus dados. Mas o que acontece quando tem mais do que um produto de segurança no mesmo sistema?

Quando utiliza mais do que uma solução de segurança no mesmo computador, o sistema torna-se instável. O instalador do Bitdefender Total Security deteta automaticamente outros programas de segurança e oferece-lhe a opção de os desinstalar.

Se não tiver removido as outras soluções de segurança durante a instalação inicial:

- No **Windows 7**:
  1. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
  2. Aguarde alguns momentos até que a lista do software instalado seja apresentada.
  3. Encontre o nome do programa que pretende remover e selecione **Desinstalar**.
  4. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.
- No **Windows 8 e Windows 8.1**:
  1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
  2. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
  3. Aguarde alguns momentos até que a lista do software instalado seja apresentada.
  4. Encontre o nome do programa que pretende remover e selecione **Desinstalar**.
  5. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.
- No **Windows 10**:
  1. Clique em **Iniciar**, em seguida, clique em Definições.

2. Clique no ícone **Sistema** na área das Definições, em seguida, selecione **Aplicações instaladas**.
3. Encontre o nome do programa que pretende remover e selecione **Desinstalar**.
4. Clique em **Desinstalar** novamente para confirmar a sua escolha.
5. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

Se não conseguir remover as outras soluções de segurança do seu sistema, obtenha a ferramenta de desinstalação do site Internet do fornecedor ou contacte-o diretamente para receber instruções de desinstalação.

3.8.9. Como posso reiniciar no Modo de Segurança?

O Modo de Segurança é um modo operativo de diagnóstico, utilizado principalmente para detetar e resolver problemas que estejam a afetar o funcionamento normal do Windows. As causas destes problemas vão desde a incompatibilidade de controladores a ameaças que impedem o arranque normal do Windows. No Modo de Segurança funcionam apenas algumas aplicações e o Windows só carrega os controladores básicos e os componentes mínimos do sistema operativo. É por isso que a maioria das ameaças está inativa quando o Windows está no Modo de Segurança e podem ser facilmente removidos.

Para iniciar o Windows no Modo de Segurança:

- No **Windows 7**:
  1. Reinicie o computador.
  2. Prima a tecla **F8** várias vezes antes de o Windows iniciar para aceder ao menu de arranque.
  3. Selecione **Modo Seguro** no menu de inicialização ou **Modo Seguro com Rede** se quiser ter acesso à Internet.
  4. Prima em **Enter** e aguarde enquanto o Windows carrega o Modo Seguro.
  5. Este processo termina com uma mensagem de confirmação. Clique em **OK** para aceitar.
  6. Para iniciar o Windows normalmente, basta reiniciar o sistema.
- No **Windows 8, Windows 8.1 e Windows 10**:

1. Execute a **Configuração do Sistema** no Windows pressionando simultaneamente as teclas **Windows + R** no seu teclado.
2. Escreva **msconfig**na caixa de diálogo **Abrir** ,depois clique em **OK**.
3. Selecione o separador **Arranque**.
4. Na área **Opções de arranque** selecione a caixa **Arranque seguro**.
5. Clique em **Rede** e depois em **OK**.
6. Clique em **OK** na janela **Configuração do Sistema**, que o informa de que o sistema necessita de ser reiniciado para as mudanças serem aplicadsa.

   O seu sistema será reiniciado no Modo Seguro com rede.

Para reiniciar no modo normal, reverta as definições executando novamente a **Operação do Sistema** e desmarcando a caixa **Arranque seguro**. Clique em **OK** e depois em **Reiniciar**. Aguarde para que as novas definições sejam aplicadas.

4. GERIR A SUA SEGURANÇA

4.1. Proteção Antivírus

Bitdefender protege o seu computador de todo o tipo de ameaças (malware, Trojans, spyware, rootkits, etc.). A proteção que Bitdefender oferece está dividida em duas categorias:

- Análise no acesso - previne que novas ameaças entrem no seu sistema. Poe exemplo, Bitdefender irá analisar um documento word em busca de ameaças conhecidas quando você o abrir, e uma mensagem de e-mail quando recebe uma.

  A análise no acesso garante proteção em tempo real contra ameaças, sendo um componente essencial de qualquer programa informático de segurança.

  > **Importante**
  > Para prevenir a infeção de ameaças no seu computador, mantenha ativada a **análise no acesso**.

- Análise a pedido - permite detetar e remover ameaças que já se encontram no sistema. Esta é uma análise clássica iniciada pelo utilizador – você escolhe qual a drive, pasta ou ficheiro o Bitdefender deverá analisar, e o mesmo é analisado – a-pedido.

O Bitdefender analisa automaticamente qualquer média removível que esteja ligado ao computador para garantir um acesso em segurança. Para mais informação, dirija-se a "*Análise automática de média removíveis*" (p. 100).

Os utilizadores avançados podem configurar as exceções da análise se não quiserem que certos ficheiros ou tipos de ficheiros sejam analisados. Para mais informação, dirija-se a "*Configurar exceções da análise*" (p. 102).

Quando deteta uma ameaça, o Bitdefender irá tentar remover automaticamente o código malicioso do ficheiro e reconstruir o ficheiro original. Esta operação é designada por desinfecção. Os ficheiros que não podem ser desinfectados são movidos para a quarentena de modo a conter a infecção. Para mais informação, dirija-se a "*Gerir ficheiros da quarentena*" (p. 105).

Se o seu computador estiver infectado com ameaças, consulte "*Remover ameaças do seu sistema*" (p. 210). Para o ajudar a limpar as ameaças do computador que não podem ser removidas no sistema operativo Windows, o Bitdefender proporciona-lhe o "*Modo de Recuperação Bitdefender (ambiente de recuperação no Windows 10)*" (p. 210). Este é um ambiente fiável, concebido sobretudo para a remoção de ameaças, que lhe permite arrancar o seu computador independentemente do Windows. Quando o computador estiver a ser executado no Modo de Recuperação (ambiente de recuperação no Windows 10), as ameaças do Windows estão inativas, tornando fácil removê-las.

4.1.1. Análise no acesso (proteção em tempo real)

O Bitdefender fornece uma proteção contínua e em tempo real contra uma gama de ameaças ao analisar todos os ficheiros acedidos e mensagens de e-mail.

Ligar ou desligar a proteção em tempo real

Para ativar ou desativar a proteção contra ameaças em tempo real:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **ANTIVÍRUS**.
4. Na janela **PROTEÇÃO**, clique no botão LIGAR/DESLIGAR.
5. Se pretender desativar a proteção em tempo real, aparece uma janela de aviso. Tem de confirmar a sua escolha seleccionando no menu durante quanto tempo pretende desactivar a protecção em tempo real. Pode desativar a sua proteção em tempo real durante 5, 15 ou 30 minutos, por uma hora, permanentemente ou até ao reinício do sistema. A proteção em tempo real será ativada automaticamente quando o tempo selecionado expirar.

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

Configuração das definições avançadas de proteção em tempo real

Os utilizadores avançados podem aproveitar as definições que o Bitdefender oferece. Pode configurar as definições da proteção em tempo real criando um nível de proteção personalizado.

Para configurar as definições avançadas de proteção em tempo real:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **ANTIVÍRUS**.
4. Na janela **PROTEÇÃO**, clique no menu **EXIBIR DEFINIÇÕES AVANÇADAS**.

   Um janela será exibida.
5. Desloque a página para baixo para configurar as definições de verificação, conforme necessário.

Informação sobre as opções de análise

Poderá achar esta informação útil:

- Se não está familiarizado com alguns dos termos, procure-os no glossário. Pode também encontrar informação útil pesquisando a Internet.
- **Opções de análise para ficheiros acedidos.** Pode configurar o Bitdefender para analisar todos os ficheiros ou apenas aplicações (ficheiros de programas) acedidos. A análise de todos os ficheiros acedidos proporciona uma maior segurança, enquanto a análise apenas das aplicações pode ser utilizada para melhorar o desempenho do sistema.

  Por defeito, ambas as pastas locais e partilhas de rede são sujeitas a análise no acesso. Para um melhor desempenho do sistema, pode excluir os locais de rede da análise no acesso.

  As aplicações (ou ficheiros de programa) são muito mais vulneráveis a ataques de ameaças do que qualquer outro tipo de ficheiros. Esta categoria inclui as seguintes extensões de ficheiro:

  386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms;

hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Analisar dentro dos arquivos.** Analisar o interior de arquivos é um processo lento e que consome muitos recursos, não sendo, por isso recomendado para a proteção em tempo real. Os arquivos que contém ficheiros infectados não são uma ameaça imediata à segurança do seu sistema. A ameaça só pode afetar o seu sistema se o ficheiro infetado for extraído do arquivo e executado sem que a proteção em tempo real esteja ativada.

  Se decidir utilizar esta opção, ligue-a e, em seguida, arraste o marcador pela escala para determinar um limite de tamanho máximo (em MB) dos ficheiros a serem verificados ao aceder.

- **Analisar e-mails.** Para impedir que sejam transferidas ameaças para o seu computador, o Bitdefender analisa os e-mails de entrada e de saída.

  Apesar de não ser recomendado, pode desativar a análise de ameaas de e-mail para aumentar o desempenho do sistema. Se desativar as respetivas opções de análise, as mensagens eletrónicas e os ficheiros recebidos não serão analisados, permitindo que ficheiros infectados sejam guardados no seu computador. Esta não é uma ameaça grave pois a proteção em tempo real vai bloquear a ameaça quando os ficheiros infetados forem acedidos (abertos, movidos, copiados ou executados).

- **Analisar sectores de arranque.** Pode definir o Bitdefenderpara analisar os sectores de saída do seu disco rígido. Este sector do disco rígido contém o código do computadores necessário para iniciar o processo de reinício. Quando uma ameaça infe ta o setor de saída, a unidade pode tornar-se inacessível ou poderá não conseguir iniciar o seu sistema e aceder aos seus dados.

- **Analisar só ficheiros alterados.** Ao analisar apenas ficheiros novos e modificados, pode melhorar significativamente o desempenho do seu sistema sem comprometer a sua segurança.

- **Analisar em busca de keyloggers.** Selecione esta opção para analisar o seu sistema em busca de aplicações keylogger. Os keyloggers gravam o que você digita no seu teclado e enviam relatórios pela 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.
- **Verificar no arranque do sistema.** Selecione a opção **Verificação de inicialização antecipada** para verificar o seu sistema na inicialização assim que todos os serviços essenciais tenham sido carregados. A finalidade desta funcionalidade é melhorar a deteção de ameaças no arranque do sistema e o tempo de inicialização do sistema.

Ações tomadas em ameaças detetadas

Pode configurar as ações a serem levadas a cabo pela proteção em tempo-real, seguindo estes passos:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **ANTIVÍRUS**.
4. Na janela **PROTEÇÃO**, clique no menu **EXIBIR DEFINIÇÕES AVANÇADAS**.

   Um janela será exibida.
5. Desloque a janela para abaixo até ver a opção **Ações após concluir a análise**.
6. Configure as definições de análise como necessário.

As seguintes ações podem ser levadas a cabo pela proteção em tempo real do Bitdefender:

Tomar acções adequadas

Bitdefender tomará as ações recomendadas dependendo do tipo de ficheiro detetado:

- **Ficheiros infectados.** Os ficheiros detetados como infetados correspondem a parte das informações de ameaças encontrada na Base de Dados de Informações de Ameaças do Bitdefender. Bitdefender tentará automaticamente remover o código malicioso do ficheiro infetado e reconstruir o ficheiro original. Esta operação é designada por desinfecção.

Os ficheiros que não podem ser desinfectados são movidos para a quarentena de modo a conter a infecção. O ficheiros em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece. Para mais informação, dirija-se a "*Gerir ficheiros da quarentena*" (p. 105).

> **Importante**
> Para determinados tipos de ameaças, a desinfeção não é possível por o ficheiro detetado ser totalmente malicioso. Nestes casos, o ficheiro infectado é eliminado do disco.

- **Ficheiros suspeitos.** Os ficheiros são detectados como suspeitos pela análise heurística. Não foi possível desinfectar os ficheiros suspeitos por não estar disponível uma rotina de desinfecção. Serão movidos para a quarentena para evitar uma potencial infeção.

  Por defeito, os ficheiros da quarentena são automaticamente enviados para os Laboratórios Bitdefender para serem analisados pelos investigadores de ameaças da Bitdefender. Se a presença de uma ameaça for confirmada, uma atualização de informações de ameaças é lançada para permitir a sua remoção.

- **Aquivos que contêm ficheiros infetados.**
  - Os arquivos que contêm apenas ficheiros infectados são eliminados automaticamente.
  - Se um arquivo tiver ficheiros infectados e limpos, o Bitdefender tentará eliminar os ficheiros infectados desde que possa reconstruir o arquivo com os ficheiros limpos. Se não for possível a reconstrução do arquivo, será informado de que não pode ser tomada qualquer ação, de forma a evitar perder ficheiros limpos.

Mover ficheiros para a quarentena

Move os ficheiros infectados para a quarentena. O ficheiros em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece. Para mais informação, dirija-se a "*Gerir ficheiros da quarentena*" (p. 105).

Negar acesso

Será negado o acesso de um ficheiro que se encontre infectado.

Restaurar as predefinições

As predefinições da proteção em tempo real asseguram uma ótima proteção contra ameaças, com um impacto mínimo no desempenho do seu sistema.

Para restaurar as definições da protecção em tempo real:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **ANTIVÍRUS**.
4. Na janela **PROTEÇÃO**, clique no menu **EXIBIR DEFINIÇÕES AVANÇADAS**.

   Um janela será exibida.
5. Desloque a janela para baixo até ver a opção **Repor definições**. Selecione esta opção para repor as predefinições do antivírus.

4.1.2. Verificação por ordem

O objectivo principal do Bitdefender é manter o seu computador livre de ameaças. Isto é feito ao manter as novas ameaças fora do seu computador e ao analisar as suas mensagens de e-mail e quaisquer novos ficheiros transferidos ou copiados para o seu sistema.

Há o risco de a ameaça já ter acedido ao seu sistema, antes mesmo de ter instalado o Bitdefender. Este é o motivo pelo qual é uma excelente ideia verificar ameaças residentes no seu computador depois de instalar o Bitdefender. E é definitivamente uma boa ideia analisar frequentemente o seu computador quanto a ameaças.

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 quiser executar as tarefas por defeito ou as suas próprias tarefas de análise (tarefas definidas pelo utilizador). Se quer analisar localizações específicas no seu computador ou configurar as opções de análise, pode configurar e executar uma análise personalizada.

Procurar ameaças num ficheiro ou pasta

Deve analisar os ficheiros e as pastas sempre que suspeitar de uma infecção. Clique com o botão direito do rato sobre o ficheiro ou pasta que pretende analisar, aponte para o **Bitdefender** e selecione **Analisar com o Bitdefender**.

O Assistente de Análise Antivírus irá surgir e guiá-lo através do processo de análise. No final da análise, será notificado para escolher as ações que devem ser tomadas nos ficheiros detetados, caso os haja.

Executar uma Análise Rápida

A Análise Rápida utiliza a análise nas nuvens para detetar ameaças em execução no seu sistema. Normalmente, a realização de uma Análise Rápida demora menos de um minuto e utiliza uma fração dos recursos do sistema necessários para uma análise antivírus normal.

Para realizar uma análise rápida:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **ANTIVÍRUS**, clique em **Análise rápida**.
4. Siga o assistente de Análise Antivírus para completar a análise. O Bitdefender tomará automaticamente as ações recomendadas nos ficheiros detetados. Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas.

Ou, de forma mais rápida, clique no ícone na barra lateral esquerda da interface do Bitdefender e depois clique no botão de ação **Análise Rápida**.

Executar uma Análise do Sistema

A tarefa de Análise do Sistema procura em todo o computador todos os tipos de ameaças que prejudicam a sua segurança, tais como malware, spyware, adware, rookits, etc.

Nota

Porque a **Análise do Sistema** leva a cabo uma análise minuciosa de todo o seu computador, a mesma poderá levar algum tempo. Portanto, recomenda-se que execute esta tarefa quando não estiver a usar o seu computador.

Antes de executar uma Análise do Sistema, recomendamos o seguinte:

- Certifique-se de que o Bitdefender está atualizado com a sua base de dados de informações de ameaças. Analisar o seu computador usando uma base de dados de informações de ameaças desatualizada pode impedir que o Bitdefender detecte novas ameaças encontradas desde a

última actualização. Para mais informação, dirija-se a "*Mantenha o seu Bitdefender atualizado.*" (p. 43).

- Encerre todos os programas abertos.

Se quer analisar localizações específicas no seu computador ou configurar as opções de análise, pode configurar e executar uma análise personalizada. Para mais informação, dirija-se a "*Configurar uma análise personalizada*" (p. 93).

Para realizar uma análise do sistema:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **ANTIVÍRUS**, clique em **Análise do sistema**.
4. A primeira vez que executar uma Análise do Sistema, verá uma apresentação da função. Clique em **OK, ENTENDI** para continuar.
5. Siga o assistente de Análise Antivírus para completar a análise. O Bitdefender tomará automaticamente as ações recomendadas nos ficheiros detetados. Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas.

Configurar uma análise personalizada

Para configurar detalhadamente uma análise personalizada e depois executá-la:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **ANTIVÍRUS**, clique em **Gerir análises**.
4. Clique no botão **Nova tarefa personalizada**. Insira um nome para a análise na aba **Básico** e selecione as localizações a serem analisadas.
5. Se desejar configurar detalhadamente as opções de análise, selecione o separador **Avançado**. Aparece uma nova janela. Siga os seguintes passos:
   a. Pode facilmente configurar as opções de análise ajustando o nível de análise. Arraste o cursor pela escala para definir o nível de análise pretendido. Utilize a descrição do lado direito da escala para escolher o nível de análise que melhor se adequa às suas necessidades.

Os utilizadores avançados podem aproveitar as definições que o Bitdefender oferece. Para configurar as opções de análise em pormenor, clique em **Personalizar**. Pode encontrar informação sobre as mesmas no final desta secção.

b. Também pode configurar as seguintes opções gerais:

- **Executar a tarefa com prioridade baixa .** Diminui a prioridade do processo de análise. Irá permitir que outros programas funcionem com maior rapidez e aumenta o tempo necessário para terminar o processo da análise.
- **Minimizar a janela da análise para a área de notificação .** Minimiza a janela da análise para a área de notificação. Faça duplo-clique sobre o ícone Bitdefender para o abrir.
- Especifique a ação a aplicar se não forem encontradas ameaças.

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

6. Se quiser programar a sua tarefa de verificação, utilize o botão **Programar** na janela **Básico**. Selecione uma das opções correspondentes para definir uma agenda:
   - No iniciar do sistema
   - Uma vez
   - Periodicamente
7. Clique em **Iniciar Análise** e siga o assistente de Análise Antivírus para completar a análise. Dependendo das localizações a serem analisadas, a análise pode demorar um pouco. No final da análise, será notificado para escolher as ações que devem ser tomadas nos ficheiros detetados, caso os haja.
8. Se quiser, pode voltar a executar rapidamente uma análise personalizada anterior ao clicar na entrada correspondente na lista disponível.

Informação sobre as opções de análise

Poderá achar esta informação útil:

- Se não está familiarizado com alguns dos termos, procure-os no glossário. Pode também encontrar informação útil pesquisando a Internet.
- **Análise de ficheiros.** Pode configurar o Bitdefender para analisar todos os tipos de ficheiros ou apenas as aplicações (ficheiros de programas).

A análise de todos os ficheiros proporciona uma maior segurança, enquanto a análise das aplicações só pode ser utilizada numa análise mais rápida.

As aplicações (ou ficheiros de programa) são muito mais vulneráveis a ataques de ameaças do que qualquer outro tipo de ficheiros. Esta categoria inclui as seguintes extensões de ficheiro: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Opções de análise para ficheiros.** Os arquivos que contém ficheiros infectados não são uma ameaça imediata à segurança do seu sistema. A ameaça só pode afetar o seu sistema se o ficheiro infetado for extraído do arquivo e executado sem que a proteção em tempo real esteja ativada. No entanto, é recomendado que utilize esta opção para detetar e remover qualquer ameaça potencial, mesmo se não for imediata.

  > **Nota**
  > Analisar ficheiros arquivados aumenta o tempo da análise e requer mais recursos do sistema.

- **Analisar sectores de arranque.** Pode definir o Bitdefenderpara analisar os sectores de saída do seu disco rígido. Este sector do disco rígido contém o código do computadores necessário para iniciar o processo de reinício. Quando uma ameaça infe ta o setor de saída, a unidade pode tornar-se inacessível ou poderá não conseguir iniciar o seu sistema e aceder aos seus dados.
- **Analisar memória.** Selecione esta opção para analisar programas executados na memória do seu sistema.

- **Analisar registo.** Selecione esta opção para analisar as chaves de registo. O Registo do Windows é uma base de dados que armazena as definições da configuração e as opções para os componentes do sistema operativo Windows, bem como para as aplicações instaladas.
- **Analisar cookies.** Selecione esta opção para analisar os cookies armazenados pelos navegadores no seu computador.
- **Analisar só ficheiros alterados.** Ao analisar apenas ficheiros novos e modificados, pode melhorar significativamente o desempenho do seu sistema sem comprometer a sua segurança.
- **Ignorar keyloggers comerciais.** Selecione esta opção se tiver instalado e usar programas de controlo e registo comerciais no seu computador. Os programas de controlo e registo comerciais são software legítimo de monitorização do computador cuja função mais básica é registar tudo o que é digitado no teclado.
- **Analisar em busca de rootkits.** Selecione esta opção para analisar rootkits e objetos ocultos usando tal software.

Assistente de Análise Antivírus

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

Nota

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

Passo 1 - Realizar Análise

Bitdefender iniciará a análise dos objetos selecionados. Pode ver informação em tempo real sobre o estado da análise e as estatísticas (incluindo o tempo decorrido, uma estimativa do tempo restante e o número de ameaças detetadas).

Espere que o Bitdefender termine a análise. O processo de análise pode demorar algum tempo, dependendo da complexidade da mesma.

Parar ou pausar a análise. Pode interromper a análise a qualquer altura que quiser clicando em **PARAR**. Irá directamente para o último passo do assistente. Para parar temporariamente o processo de análise, clique em **PAUSA**. Terá de clicar em**RETOMAR** para retomar a análise.

Arquivos protegidos com palavra-passe. Quando é detectado um arquivo protegido por palavra-passe, dependendo das definições da análise, poderá ter de indicar a palavra-passe. Os arquivos protegidos por palavra-passe não podem ser analisados a não ser que forneça a palavra-passe. Estão disponíveis as seguintes opções:

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

Escolha a opção desejada e clique em **OK** para continuar a analisar.

Passo 2 - Escolher Ações

No final da análise, será notificado para escolher as ações que devem ser tomadas nos ficheiros detetados, caso os haja.

Nota

Quando realiza uma verificação rápida ou do sistema, o Bitdefender automaticamente aplica as ações recomendadas nos ficheiros detetados durante a verificação. Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas.

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

Pode escolher uma ação geral a ser levada a cabo para todas as incidências ou pode escolher ações separadas para cada grupo de incidências. Uma ou várias das seguintes opções poderão aparecer no menu:

Tomar acções adequadas

Bitdefender tomará as ações recomendadas dependendo do tipo de ficheiro detetado:

- **Ficheiros infectados.** Os ficheiros detetados como infetados correspondem a parte das informações de ameaças encontrada na Base de Dados de Informações de Ameaças do Bitdefender. Bitdefender tentará automaticamente remover o código malicioso do ficheiro infetado e reconstruir o ficheiro original. Esta operação é designada por desinfecção.

  Os ficheiros que não podem ser desinfectados são movidos para a quarentena de modo a conter a infecção. O ficheiros em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece. Para mais informação, dirija-se a "*Gerir ficheiros da quarentena*" (p. 105).

  > **Importante**
  > Para determinados tipos de ameaças, a desinfeção não é possível por o ficheiro detetado ser totalmente malicioso. Nestes casos, o ficheiro infectado é eliminado do disco.

- **Ficheiros suspeitos.** Os ficheiros são detectados como suspeitos pela análise heurística. Não foi possível desinfectar os ficheiros suspeitos por não estar disponível uma rotina de desinfecção. Serão movidos para a quarentena para evitar uma potencial infeção.

  Por defeito, os ficheiros da quarentena são automaticamente enviados para os Laboratórios Bitdefender para serem analisados pelos investigadores de ameaças da Bitdefender. Se a presença de uma ameaça for confirmada, uma atualização de informações é lançada para permitir a sua remoção.

- **Aquivos que contêm ficheiros infetados.**
  - Os arquivos que contêm apenas ficheiros infectados são eliminados automaticamente.
  - Se um arquivo tiver ficheiros infectados e limpos, o Bitdefender tentará eliminar os ficheiros infectados desde que possa reconstruir o arquivo com os ficheiros limpos. Se não for possível a reconstrução do arquivo, será informado de que não pode ser tomada qualquer ação, de forma a evitar perder ficheiros limpos.

Apagar
Remove os ficheiros detectados do disco.

Se os ficheiros infectados estiverem armazenados num arquivo junto com ficheiros limpos, o Bitdefender tentará eliminar os ficheiros infectados e reconstruir o arquivo com ficheiros limpos. Se não for possível a reconstrução do arquivo, será informado de que não pode ser tomada qualquer ação, de forma a evitar perder ficheiros limpos.

Não Tomar Acção
Nenhuma acção será levada a cabo sobre os ficheiros detectados. Após a analisar terminar, pode abrir o relatório da análise para ver informação sobres esses ficheiros.

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

Passo 3 - Resumo

Quando o Bitdefender termina de reparar estas incidências, o resultado da análise aparecerá numa nova janela. Se deseja uma informação completa sobre o processo de análise, clique em **MOSTRAR RELATÓRIO** para ver o relatório da análise. O registo é fornecido no formato .xml e pode ser guardado localmente ao clicar no botão **Guardar registo** e escolher uma localização

Importante

Na maioria dos casos o Bitdefender desinfecta com sucesso o ficheiro infectado ou isola a infecção. No entanto, há incidências que não podem ser automaticamente resolvidas. Se necessário, ser-lhe-à solicitado que reinicie o seu computador, para que o processo de limpeza seja completado. Para mais informações e instruções sobre como remover manualmente uma ameaça, consulte "*Remover ameaças do seu sistema*" (p. 210).

Ver os relatórios da análise

Sempre que uma análise for efetuada, é criado um registo de análise e o Bitdefender regista as incidências detectadas na janela Antivírus. 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.

Pode abrir o relatório diretamente no assistente de análise, assim que esta terminar, clicando em **MOSTRAR RELATÓRIO**.

Para verificar um registo de análise ou qualquer infeção detetada posteriormente:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. No separador **Todas**, selecione a notificação referente à última análise.

   Aqui poderá encontrar todos os eventos de análise de ameaças, incluindo ameaças detectadas na análise no acesso, análises iniciadas pelo utilizador e alterações de estado para as análises automáticas.
3. Na lista de notificações, pode ver as análises que foram recentemente efectuadas. Clique numa notificação para visualizar detalhes sobre o mesmo.
4. Para abrir o registo de verificação, clique em **VER REGISTO**.

4.1.3. Análise automática de média removíveis

O Bitdefender deteta automaticamente quando um dispositivo de armazenamento removível é ligado ao computador e analisa-o em segundo plano quando a opção de Análise automática está ativada. Isto é recomendado para evitar que ameaças infetem o seu computador.

Os dispositivos detetados encaixam-se numa destas categorias:

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

Você pode configurar a análise automática separadamente para cada categoria de dispositivos de armazenamento. Análise automática das drives de rede mapeadas está desativada por defeito.

Como funciona?

Quando deteta dispositivos de armazenamento removíveis, o Bitdefender começa a verificar se existem ameaças em segundo plano (desde que a análise automática esteja ativada para aquele tipo de dispositivo). Um ícone de análise do Bitdefender irá aparecer no tabuleiro do sistema Pode clicar nesse ícone para abrir a janela da análise e ver o seu progresso.

Se o Piloto Automático estiver ativado, não será incomodado com a análise. A verificação será apenas registada e as informações adjacentes estarão disponíveis na janela Notificações.

Se o Piloto Automático estiver desativado:

1. Será notificado através de uma janela de pop-up que um novo dispositivo foi detetado e está a ser analisado.
2. Na maioria dos casos, o Bitdefender remove automaticamente as ameaças detetadas ou isola os ficheiros infetados na quarentena. Se houver ameaças não resolvidas depois da análise, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas.

   Nota
   Leve em consideração que não pode ser tomada qualquer acção em ficheiros infectados ou suspeitos detectados em CDs/DVDs. Da mesma forma, não pode ser tomada qualquer acção em ficheiros infectados ou suspeitos detectados em drives de rede mapeadas, caso não tenha os privilégios adequados.

3. Quando a análise estiver concluída, é apresentada a janela dos resultados da análise para o informar se pode aceder em segurança aos ficheiros nos dispositivos removíveis.

Esta informação pode ser útil para si:

- Tenha cuidado ao utilizar um CD/DVD infetado com ameaças porque as ameaças não podem ser removidas do disco (é apenas de leitura). Certifique-se que a proteção em tempo real está ativada para evitar que as ameaças se propaguem no seu sistema. É recomendado copiar quaisquer dados valiosos do disco no seu sistema e depois descartar o disco.
- Em alguns casos, o Bitdefender poderá não conseguir remover as ameaças de ficheiros específicos devido a restrições legais ou técnicas. Exemplo disso são os ficheiros guardados usando uma tecnologia proprietária (isto acontece porque o ficheiro não pode ser correctamente recriado).

  Para saber mais sobre como lidar com ameaças, consulte "*Remover ameaças do seu sistema*" (p. 210).

Gerir análise de média removível

Para gerir a verificação automática de dispositivos multimédia amovíveis:

Para uma melhor proteção, recomenda-se que deixe a opção **Análise automática** selecionada para todos os tipos de dispositivos de armazenamento removíveis.

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **ANTIVÍRUS**.
4. Selecione o separador **DRIVES E DISPOSITIVOS**.

As opções de análise estão pré-configuradas para obter os melhores resultados de deteção. Se forem detctados ficheiros infetados, o Bitdefender tentará desinfetá-los (remover o código malicioso) ou movê-los para a quarentena. Se ambas as acções falharem, o assistente da Análise Antivírus permite especificar outras acções a serem tomadas com ficheiros infectados. As opções de análise são padronizadas e não as pode alterar.

4.1.4. Analisar ficheiro hosts

Os ficheiros anfitrião são fornecidos por predefinição com a instalação do seu sistema operativo e são utilizados para mapear os nomes de anfitrião nos endereços IP sempre que acede a uma nova página Web, ligue um FTP ou outros servidores de Internet. É um ficheiro de texto simples e os programas maliciosos podem modificá-lo. Os utilizadores avançados sabem como utilizá-lo para bloquear anúncios incómodos, separadores, cookies de terceiros ou hijackers.

Para configurar o ficheiro anfitrião de verificação:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Selecione o separador **AVANÇADO**.
3. Clique no botão ON/OFF correspondente.

4.1.5. Configurar exceções da análise

O Bitdefender permite excluir ficheiros, pastas ou extensões de ficheiros específicos da análise. Esta característica visa evitar a interferência com o seu trabalho e também pode ajudar a melhorar o desempenho do sistema.

As exceções devem ser usadas por utilizadores com conhecimentos informáticos avançados ou sob as recomendações de um representante da Bitdefender.

Pode configurar as exceções para aplicar apenas na análise no acesso ou a pedido, ou ambos. Os objetos excluídos da análise a-pedido não serão analisados, independentemente de eles serem acedidos por si ou por uma aplicação.

Nota

As exceções NÃO serão aplicadas à análise contextual e do sistema. A análise do sistema é um analista sob demanda que possibilita analisar todo o sistema em busca de ameaças maliciosas que podem pôr a segurança dos seus dados em perigo. Análise Contextual é um tipo de análise a-pedido: você clica com o botão direito de rato sobre o ficheiro ou pasta que quer analisar e seleciona **Analisar com Bitdefender**.

Excluir ficheiros e pastas da verificação

Para excluir ficheiros e pastas específicos da verificação:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **ANTIVÍRUS**.
4. Selecione o separador **EXCLUSÕES**.
5. Clique no menu em acordeão **Lista de ficheiros e pastas excluídas da análise**. Na janela que surge, pode gerir os ficheiros e pastas excluídos da análise.
6. Adicionar exceções seguindo estes passos:
   a. Clique no botão **ADD**.
   b. Clique em **Pesquisar**, selecione o ficheiro ou pasta que quer eliminar da verificação e, em seguida, clique em **OK**. Alternativamente, pode digitar (ou copiar e colar) o caminho para o ficheiro ou pasta no campo editar.
   c. Por defeito, o ficheiro ou pasta é excluída da análise no acesso e a pedido. Para alterar a aplicação da exclusão, selecione uma das outras opções.

d. Prima **Adicionar**.

Excluir extensões de ficheiros da análise

Quando exclui uma extensão de ficheiro da análise, o Bitdefender deixará de analisar ficheiros com essa extensão, independentemente da sua localização no seu computador. A exclusão também se aplica a ficheiros em média removíveis, tais como CDs, DVDs, dispositivos de armazenamento USB ou drives da rede.

> **Importante**
> Tenha cuidado ao excluir as extensões da análise, porque tais exceções podem tornar o seu computador vulnerável a ameaças.

Para excluir extensões de ficheiro da análise:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **ANTIVÍRUS**.
4. Selecione o separador **EXCLUSÕES**.
5. Clique no respetivo menu **Lista de extensões excluídas da verificação**. Na janela que surge, pode gerir as extensões de ficheiros excluídas da análise.
6. Adicionar exceções seguindo estes passos:
   a. Clique no botão **ADD**.
   b. Digite as extensões que pretende que sejam excluídas da análise, separando-as com ponto e vírgula (;). Eis um exemplo:

      txt;avi;jpg

   c. Por defeito, todos os ficheiros com as extensões especificadas são excluídas na análise no acesso e a pedido. Para alterar a aplicação da exclusão, selecione uma das outras opções.
   d. Prima **Adicionar**.

Gerir exceções da análise

Se as exceções de análise configuradas já não forem necessárias, recomenda-se que elimine ou desative as exceções da análise.

Para gerir as exclusões da análise:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **ANTIVÍRUS**.
4. Selecione o separador **EXCLUSÕES**.
5. Utilize as opções no menu **Lista de ficheiros e pastas excluídos da verificação** para gerir exclusões da verificação.
6. Para remover ou editar exceções da análise, clique numa das ligações disponíveis. Proceder da seguinte forma:
   - Para remover uma entrada da lista, selecione-a e clique no botão **REMOVER**.
   - Para editar uma entrada da lista, clique duas vezes (ou selecione-a e clique no botão **Editar**). Uma nova janela aparece quando muda a extensão ou o caminho a ser excluído e o tipo de verificação que deseja que sejam excluídos, conforme necessário. Faça as alterações necessárias, depois clique em **Modificar**.

4.1.6. Gerir ficheiros da quarentena

O Bitdefender isola os ficheiros infetados por ameaças que não consegue desinfetar numa área segura denominada quarentena. Quando uma ameaça se encontra na quarentena não pode provocar nenhum mal, porque não pode ser nem lida nem executada.

Por defeito, os ficheiros da quarentena são automaticamente enviados para os Laboratórios Bitdefender para serem analisados pelos investigadores de ameaças da Bitdefender. Se a presença de uma ameaça for confirmada, uma atualização de informações é lançada para permitir a sua remoção.

Além disso, o Bitdefender analisa os ficheiros em quarentena sempre que a base de dados de informações de ameaças é atualizada. Os ficheiros limpos são automaticamente repostos no seu local de origem.

Para verificar e gerir os ficheiros em quarentena:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.

3. No painel **ANTIVÍRUS**, clique em **Quarantena**.

   Aqui pode ver o nome dos ficheiros em quarentena, a sua localização original e o nome das ameaças detetadas.

4. Os ficheiros da quarentena são geridos automaticamente pelo Bitdefender de acordo com as predefinições da quarentena.

   Embora não seja recomendado, pode ajustar as definições de quarentena de acordo com as suas preferências clicando em **Ver Definições**.

   Clique nos botões para ligar ou desligar:

   Analisar novamente a quarentena depois da base de dados de assinaturas de malware
   Mantenha esta opção ligada para analisar automaticamente os ficheiros da quarentena após cada atualização da base de dados das informações de ameaças. Os ficheiros limpos são automaticamente repostos no seu local de origem.

   Enviar ficheiros suspeitos da quarentena para análise
   Mantenha esta opção ligada para enviar automaticamente os ficheiros da quarentena para os Laboratórios da Bitdefender. As amostras de ficheiros serão analisados pelos investigadores de ameaças da Bitdefender. Se a presença de uma ameaça for confirmada, uma atualização de informações de ameaças é lançada para permitir a sua remoção.

   Apagar conteúdo com mais de 30 dias
   Os ficheiros em quarentena com mais de 30 dias são eliminados automaticamente.

   Criar exclusão para ficheiros restaurados
   Os ficheiros que restaurar da quarentena são colocados na sua localização original sem que sejam reparados e eliminados automaticamente de análises futuras.

5. Para eliminar um ficheiro da quarentena, selecione-o e clique no botão **ELIMINAR**. Se pretende restaurar um ficheiro da quarentena para a respetiva localização original, selecione-o e clique em **RESTAURAR**.

4.2. Advanced Threat Defense

Bitdefender Advanced Threat Defense é uma tecnologia de deteção proativa inovadora que utiliza métodos heurísticos avançados para detetar ransomware e outras novas ameaças potenciais em tempo real.

Advanced Threat Defense monitoriza continuamente as aplicações executadas no computador, procurando ações tipo ameaças. Cada uma destas acções é classificada e é calculada uma pontuação geral para cada processo.

Como uma medida de segurança, será notificado sempre que um ataque de ransomware for detetado e bloqueado, mesmo se a funcionalidade Piloto Automático estiver ativada.

Ativar ou desativar o Advanced Threat Defense

Para ativar ou desativar o Advanced Threat Defense:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **ADVANCED THREAT DEFENSE**, clique no botão ON/OFF.

Nota
Para manter o sistema protegido contra ransomware e outras ameaças, recomendamos que desative o Advanced Threat Defense o mínimo de tempo possível.

A verificar ataques de ransomware detetados

Para verificar os ataques de ransomware detetados pelo Advanced Threat Defense:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **ADVANCED THREAT DEFENSE**, clique em **Proteção contra Ransomware**.
4. A primeira vez que aceder à Proteção contra Ransomware, verá uma apresentação da função. Clique em **OK, ENTENDI** para continuar.

São apresentados os ataques detetados nos últimos 90 dias. Para obter informações sobre o tipo de um ransomware detetado, o caminho do processo malicioso ou se a desinfeção foi bem-sucedida, basta clicar neste.

A verificar aplicações suspeitas detetadas

Para verificar as aplicações suspeitas detetadas pelo Advanced Threat Defense:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **ADVANCED THREAT DEFENSE**, clique em **Defesa contra Ameaças**.
4. A primeira vez que aceder à Defesa contra Ameaças, verá uma apresentação da função. Clique em **OK, ENTENDI** para continuar.

   São apresentadas as aplicações que foram detetadas como ameaças e bloqueadas nos últimos 90 dias. Para obter informações sobre uma aplicação, o caminho do processo malicioso ou se a desinfeção foi bem-sucedida, basta clicar nesta.

A adicionar processos às exclusões

Pode configurar regras de exclusão para aplicações fidedignas para que o Advanced Threat Defense não as bloqueie se executarem ações tipo ameaças. Advanced Threat Defense irá continuar a monitorizar aplicações excluídas.

Para começar a adicionar processos à lista de exclusões do Advanced Threat Defense:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **ADVANCED THREAT DEFENSE**.
4. Na janela **LISTA DE PERMISSÕES**, clique em **Adicionar aplicações à lista de permissões**.

5. Encontre e selecione a aplicação que pretende excluir e, em seguida, clique em **OK**.

   Para remover uma entrada da lista, clique no botão **Remover** junto da mesma.

4.3. Proteção da Internet

A Proteção na web do Bitdefender garante uma navegação segura ao alertá-lo sobre páginas da web potencialmente maliciosas.

O Bitdefender fornece proteção da Internet em tempo real para:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

Para configurar as definições de proteção na web:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **PROTEÇÃO NA WEB**.

Clique nos botões para ligar ou desligar:

- Verifique ameaças de bloqueio de tráfego HTTP provenientes da Internet, incluindo transferências não autorizadas.
- Consultor de pesquisa, um componente que qualifica os resultados do seu motor de pesquisa e dos links colocados nos websites das redes sociais ao colocar um icone ao lado de cada resultado:

  Não deveria visitar esta página web.

  Esta página web pode conter conteúdo perigoso. Tenha cuidado se decidir visitá-la.

  Esta página é segura.

  O Consultor de Pesquisa qualifica os resultados da pesquisa dos seguintes motores de busca:

- Google
- Yahoo!
- Bing
- Baidu

O Consultor de Pesquisa classifica os links publicados nos seguintes serviços das redes sociais:

- Facebook
- 123

- A analisar SSL.

  Ataques mais sofisticados podem usar tráfego da web seguro para enganar as suas vítimas. É, por isso, recomendado que ative a análise SSL.

- Proteção contra fraudes.

- Proteção contra phishing.

Pode criar uma lista de páginas que não serão analisadas pelos motores antiameaças, antiphishing e antifraude do Bitdefender. A lista deve conter apenas os sites web em que confia plenamente. Por exemplo, adicione os sites da Web onde faz compras online.

Para configurar e gerir os sites Web utilizando a proteção na Web fornecida pelo Bitdefender:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **PROTEÇÃO NA WEB**, clique em **Lista branca**.
4. Na caixa de texto **Adicionar URL**, introduza o nome do site Web que deseja adicionar à lista e, em seguida, clique em **Adicionar**.

   Para remover um site web desta lista, selecione-o na lista e, em seguida, clique na hiperligação **Remover** correspondente.

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

Alertas de Bitdefender no navegador

Sempre que tenta visitar uma página Web classificada como insegura, esta é bloqueada e é apresentada uma página de aviso no seu navegador.

A página contém informações como a URL do site web e a ameaça detetada.

Tem de decidir o que fazer a seguir. Estão disponíveis as seguintes opções:

- Navegue para fora da página web clicando em **Leve-me de volta à segurança**.
- Prosseguir para a página web, apesar do aviso, clicando em **Eu compreendo os riscos, avançar de qualquer forma**.

4.4. Antispam

Spam é o termo utilizado para descrever mensagens eletrónicas não solicitadas. O Spam é um problema crescente, tanto para indivíduos como para organizações. Não é bonito, não desejaria que os seus filhos o vissem, pode fazer com que seja despedido (por desperdiçar muito tempo, ou por receber pornografia no seu mail de trabalho) e não pode impedir que as pessoas o enviem. O melhor a fazer para impedir isso, é, obviamente, parar de o receber. Infelizmente, o Spam vem em muitos formatos e feitios, e é muito abundante.

O Bitdefender Antispam emprega inovações tecnológicas surpreendentes e um conjunto de filtros de antispam standard para limpar o spam antes de o mesmo chegar à caixa de correio A receber do utilizador. Para mais informação, dirija-se a "*Compreender o Antispam*" (p. 112).

A proteção de Antispam do Bitdefender está disponível apenas para clientes de correio eletrónico configurado para receber mensagens de e-mail via protocolo POP3. POP3 é um dos protocolos mais utilizados para fazer o download de mensagens de e-mail a partir de um servidor de correio.

Nota
O Bitdefender não proporciona proteção antispam para contas de correio eletrónico a que acede através de sites Internet (webmail).

As mensagens não solicitadas detetadas pelo Bitdefender são marcadas com o prefixo [SPAM] no campo do assunto. O Bitdefender move automaticamente as mensagens de spam para uma determinada pasta, da seguinte forma:

- No Microsoft Outlook, as mensagens de spam são movidas para a pasta **Spam**, localizada na pasta **Itens Eliminados**. A pasta **Spam** fé criada quando um e-mail é indicado como spam.
- No Mozilla Thunderbird, as mensagens de spam são movidas para a pasta **Spam**, localizada na pasta **Lixo**. A pasta **Spam** fé criada quando um e-mail é indicado como spam.

Se usa outros cliente de e-mail, tem de criar uma regra para mover os e-mails marcados como [spam] pelo Bitdefender para uma pasta de quarentena personalizada. Se os itens Eliminar ou as pastas Lixo forem eliminados, a pasta Spam também é eliminada. Contudo, é criada uma nova pasta Spam assim que um e-mail for indicado como spam.

4.4.1. Compreender o Antispam

Filtros impeditivos da entrada de mails indesejados

O Motor Antispam do Bitdefender inclui proteção na nuvem e outros filtros diferenciados que garantem que a sua Caixa de Entrada fique livre de SPAM, como a Lista de Amigos, Lista de Spammers e Filtro de Carateres.

Lista de Amigos / Lista de Spammers

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

Nota
Recomendamos que adicone os nomes e endereços de e-mail dos seus amigos à **Lista de Amigos**. O Bitdefendernão bloqueia mensagens das pessoas dessa lista; logo, adicionar amigos ajuda a que as mensagens legítimas cheguem a si.

Filtro caracteres

Muitas mensagens de spam estão escritas em Cirílico e/ou caracteres Asiáticos. O filtro de Caracteres detecta este tipo de mensagens e marca-os como SPAM.

Operação Antispam

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

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 de Spammers irá apoderar-se do seu correio electrónico para verificar se o endereço do remetente se encontra na lista. Se for encontrada uma correspondência, a mensagem será marcada como SPAM e movida para a pasta de **Spam**.

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

Nota
Se o e-mail for marcado com SEXUALLY EXPLICIT na linha do sujeito, o Bitdefender irá considerá-lo como SPAM.

Clientes de email e protocolos suportados

A proteção 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 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 e superior

4.4.2. Ligar ou desligar a proteção antispam

A proteção AntiSpam está ativada por defeito.

Para ligar ou desligar a ferramenta Antispam:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **ANTISPAM**, clique no botão LIGAR/DESLIGAR.

4.4.3. Utilizar a barra de ferramentas Antispam na janela do seu cliente de email

No lado superior da janela do seu cliente de mail pode ver a barra de ferramentas do Antispam. A barra de ferramentas do Antispam ajuda-o a gerir a proteção antispam diretamente do seu cliente de e-mail. Pode

facilmente corrigir o Bitdefender se ele marcar uma mensagem legítima como SPAM.

Importante

O BiDefender integra uma barra antispam de facil utilização, nos clientes de email mais comuns. Para ver a lista completa de clientes de e-mail suportados, por favor consulte o "*Clientes de email e protocolos suportados*" (p. 113).

Cada botão é explicado abaixo:

Definições - abre uma janela onde pode configurar as definições da barra de ferramentas e dos filtros antispam.
É Spam - indica que o email selecionado é spam. O email será movido imediatamente para a pasta **Spam**. Se os serviços da nuvem antispam estiverem ativados, a mensagem é enviada para a Nuvem do Bitdefender para análise mais aprofundada.
Não Spam - indica que o email selecionado não é spam e o Bitdefender não o deveria ter identificado. Este e-mail será movido da pasta **Spam** para o diretório **Caixa de Entrada**. Se os serviços da nuvem antispam estiverem ativados, a mensagem é enviada para a Nuvem do Bitdefender para análise mais aprofundada.

Importante

O botão **Não Spam** fica ativo quando selecionar uma mensagem marcada como SPAM pelo Bitdefender (normalmente estas mensagens localizam-se na pasta de **Spam**).

Adicionar Spammer - adiciona o remetente da mensagem de e-mail à lista de Spammers. Pode necessitar de clicar em **OK** para confirmar. As mensagens de e-mail recebidas dos endereços na lista de Spammers são automaticamente marcadas como [spam].
Adicionar Amigo - adiciona o remetente da mensagem de e-mail à lista de Amigos. Pode necessitar de clicar em **OK** para confirmar. Irá sempre receber mensagens de e-mail destes endereços, independentemente do conteúdo da mensagem.
Spammers- abre a **Lista de Spammers** que contém todos os endereços de e-mail, dos quais não quer receber mensagens, independentemente do seu conteúdo. Para mais informação, dirija-se a "*Configurar a lista de Spammers*" (p. 117).
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. Para mais informação, dirija-se a "*Configurar a Lista de Amigos*" (p. 116).

Indicar os erros de deteção

Se estiver a usar um cliente de e-mail suportado, pode facilmente corrigir o filtro antispam (indicando mensagens de correio eletrónico que não deveriam ter sido marcadas como[spam]). Se o fizer, ajuda a melhorar a eficiência do filtro antispam. Siga os seguintes passos:

1. Abra o mail de cliente.
2. Vá à pasta de lixo eletrónico, para onde são movidas as mensagens.
3. Selecione a mensagem legítima incorretamente marcada como [spam] pelo Bitdefender.
4. Clique no botão **Adicionar Amigos** da barra de tarefas antispam do Bitdefender para adicionar o remetente à lista de Amigos. Pode necessitar de clicar em **OK** para confirmar. Irá sempre receber mensagens de e-mail destes endereços, independentemente do conteúdo da mensagem.
5. Clique no botão **Não Spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de mail do cliente). A mensagem de email será movida para a pasta de Entrada.

Indicar mensagens de spam não detetadas

Se estiver a utilizar um cliente de e-mail suportado, pode facilmente indicar quais as mensagens de e-mail que devem ser detectadas como spam. Se o fizer, ajuda a melhorar a eficiência do filtro antispam. Siga os seguintes passos:

1. Abra o mail de cliente.
2. Vá à pasta Caixa de Entrada.
3. Selecione as mensagens spam não detetadas
4. Clique no botão **É Spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de email do cliente). São imediatamente marcadas como [spam] e movidas para a pasta de lixo electrónico.

Configurar definições da barra de ferramentas

Para configurar as definições da barra de ferramentas antispam do seu cliente de email, clique no botão **Definições** na barra e depois no separador **Definições da Barra de Ferramentas**.

Tem as seguintes opções:

- **Marque as mensagens de e-mail indesejadas como 'ler'** - marca as mensagens indesejadas como ler automaticamente, para que não seja perturbador quando chegarem.
- Pode optar por visualizar janelas de confirmação quando clica nos botões **Adicionar Spammer** e **Adicionar Amigo** na barra de ferramentas antispam.

  As janelas de confirmação pode evitar a adição acidental de destinatários de email à lista de Amigos / Spammers.

4.4.4. Configurar a Lista de Amigos

A **Lista de Amigos** é uma lista de todos os endereços de e-mail dos quais deseja sempre receber mensagens, independentemente do seu conteúdo. As mensagens dos seus amigos não são marcadas como spam, mesmo que o conteúdo se assemelhe a spam.

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

Para configurar e gerir a lista de Amigos:

- Se estiver a utilizar o Microsoft Outlook ou Thunderbird, clique no botão **Amigos** na barra de ferramentas antispam do Bitdefender.
- Alternativa:
  1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
  2. Clique na hiperligação **VER FUNCIONALIDADES**.
  3. No painel **ANTISPAM**, clique em **Gerir amigos**.

Para adicionar um endereço de email, selecione a opção **Endereço de e-mail**, digite o endereço e depois clique em **Adicionar**. Sintaxe: nome@dominio.com.

Para adicionar os endereços de e-mail de um domínio específico, selecione a opção **Nome do domínio**, insira o nome do domínio e, em seguida, clique em **Adicionar**. Sintaxe:

- @domain.com e domain.com - todas as mensagens de e-mail recebidas de domain.com chegarão à sua **Caixa de entrada** independentemente do seu conteúdo;
- dominio - todos os mails provenientes de dominio (independentemente dos sufixos de domínio) serão marcados como INDESEJADOS;
- com - todos os mails tendo o sufixo de domínio com serão marcados como INDESEJADOS;

É recomendado que evite adicionar domínios completos, mas isto poderá ser útil em algumas situações. Por exemplo, pode adicionar o domínio do endereço eletrónico da empresa para a qual trabalha ou de parceiros de confiança.

Para eliminar um item da lista, clique na ligação **Remover** correspondente. Para eliminar todas as entradas da lista, clique no botão **Limpar Lista**.

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

Para carregar uma lista de Amigos previamente guardada, clique no botão **Carregar** e abra o ficheiro .bwl correspondente. Para repor o conteúdo da lista existente ao carregar uma lista guardada anteriormente, selecione **Sobrescrever lista atual**.

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

4.4.5. Configurar a lista de Spammers

A **Lista de indesejados** é uma lista de todos os endereços de e-mail, dos quais nunca pretende receber mensagens, independentemente do seu conteúdo. Todo o mail proveniente de um endereço presente na **Lista de indesejados**, será marcado automaticamente com indesejado, sem mais demora.

Para configurar e gerir a lista de Spammers:

- Se estiver a utilizar o Microsoft Outlook ou Thunderbird, clique no botão **Spammers** na barra de ferramentas antispam do Bitdefender integrada no seu cliente de e-mail.

- Alternativa:
  1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
  2. Clique na hiperligação **VER FUNCIONALIDADES**.
  3. No painel **ANTISPAM**, clique em **Gerir spammers**.

Para adicionar um endereço de email, selecione a opção **Endereço de e-mail**, digite o endereço e depois clique em **Adicionar**. Sintaxe: nome@dominio.com.

Para adicionar os endereços de e-mail de um domínio específico, selecione a opção **Nome do domínio**, insira o nome do domínio e, em seguida, clique em **Adicionar**. Sintaxe:

- @domain.come domain.com - todas as mensagens de e-mail recebidas de domain.com chegarão à sua **Caixa de entrada** independentemente do seu conteúdo;
- dominio - todos os mails provenientes de dominio (independentemente dos sufixos de domínio) serão marcados como INDESEJADOS;
- com - todos os mails tendo o sufixo de domínio com serão marcados como INDESEJADOS.

É recomendado que evite adicionar domínios completos, mas isto poderá ser útil em algumas situações.

Atenção

Não adicione domínios de serviços web-mail (tais como o Yahoo, Gmail, Hotmail ou outro) à lista de Spammers. Caso contrário, as mensagens de email recebidas de algum utilizador registado nesses serviços será detectado como spam. Se, por exemplo, adicionar yahoo.com à lista de Spammer, todos as mensagens de e-mais recebidas do endereço yahoo.com, serão marcadas como [spam].

Para eliminar um item da lista, clique na ligação **Remover** correspondente. Para eliminar todas as entradas da lista, clique no botão **Limpar Lista**.

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

Para carregar uma lista de spammers previamente guardada, clique no botão **Carregar** e abra o ficheiro .bwl correspondente. Para repor o conteúdo da lista existente ao carregar uma lista guardada anteriormente, selecione **Sobrescrever lista atual**.

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

4.4.6. A configurar os filtros locais Antispam

Como descrito em "*Compreender o Antispam*" (p. 112), o Bitdefender utiliza um conjunto de diferentes filtros antispam para identificar o spam. Os filtros antispam são pré-configurados para uma proteção eficaz.

> **Importante**
>
> Dependendo se recebe ou não mensagens eletrónicas fiáveis ou não escrita com caracteres asiáticos ou cirílicos, desative ou ative a definição que bloqueia automaticamente estas mensagens. A respetiva definição está desativada nas versões localizadas do programa que utilizam conjuntos de caracteres (por exemplo, na versão russa ou chinesa).

Para configurar os filtros locais antispam:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **ANTISPAM**.
4. Clique nos botões LIGAR/DESLIGAR correspondentes.

Se estiver a usar Microsoft Outlook ou Thunderbird, pode configurar os filtros locais antispam diretamente a partir do seu cliente de e-mail. Clique no botão **Definições** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela do cliente de e-mail) e depois no separador **Filtros Antispam**.

4.4.7. Configurar as definições da nuvem

A deteção na nuvem utiliza os Serviços na Nuvem do Bitdefender para lhe proporcionar uma proteção antispam eficaz e sempre atualizada.

As funções de proteção na nuvem enquanto mantiver o AntiSpam do Bitdefender ativado.

As amostras de emails legítimos ou spam podem ser enviados para a Nuvem Bitdefender quando indica erros de detecção ou emails de spam não detectados. Isto ajuda a melhorar a detecção antispam do Bitdefender.

Configurar o envio de amostra por e-mail para a Nuvem Bitdefender através da seleção das opções pretendidas, seguindo estes passos:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **ANTISPAM**.
4. Na janela **DEFINIÇÕES**, selecione as opções desejadas.

Se estiver a utilizar Microsoft Outlook ou Thunderbird, pode configurar a deteção na nuvem diretamente a partir do seu cliente de e-mail. Clique no botão **Definições** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela do cliente de e-mail) e depois no separador **Definições de Nuvem**.

4.5. Firewall

A Firewall protege o seu computador de tentativas de ligação de saída e entrada não-autorizadas, quer em redes locais quer na Internet. É bastante semelhante a um guarda no seu seu portão - regista as tentativas de ligação e decide quais deve permitir e quais bloquear.

A firewall do Bitdefender usa um conjunto de regras para filtrar dados transmitidos para ou a partir do seu sistema.

Em condições normais, o Bitdefender cria automaticamente uma regra sempre que uma aplicação tenta aceder à Internet. Também pode adicionar ou editar manualmente regras das aplicações.

Como medida de segurança, será notificado sempre que uma aplicação potencialmente maliciosa for bloqueada de aceder à Internet, mesmo se a funcionalidade Piloto Automático estiver ativada.

OBitdefender atribui automaticamente um tipo de rede a cada ligação de rede que deteta. Dependendo do tipo de rede, a proteção firewall é definida para o nível apropriado para cada ligação.

Para saber mais sobre as definições da firewall para cada tipo de rede e como pode editar as definições de rede, por favor consulte "*Gerir definições da ligação*" (p. 124).

Ativar/desativar firewall de proteção

Para ativar ou desativar a proteção por firewall:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.

2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **FIREWALL**, clique no botão ON/OFF.

Atenção

Porque expõe o seu computador a ligações não autorizadas, desligar a firewall deveria ser uma medida temporária. Volte a ligar a firewall assim que possível.

4.5.1. A gerir regras de aplicações

Para visualizar e gerir as regras da firewall de controlo do acesso a aplicações a recursos da rede e à Internet:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **FIREWALL**, clique em **Acesso a aplicações**.
4. A primeira vez que aceder à Firewall, verá uma apresentação da função. Clique em **OK, ENTENDI** para continuar.

Pode ver os últimos 15 programas (processos) que passaram pela Firewall do Bitdefender e a rede de Internet à qual está ligado. Para ver as regras criadas para uma aplicação específica, basta clicar nela e clicar na hiperligação **Ver regras da aplicação**. A janela **REGRAS** é apresentada.

Para cada regra é apresentada a seguinte informação:

- **REDE** - o processo e os tipos de adaptador de rede (doméstico/escritório, público ou todos) aos quais a rede se aplica. As regras são automaticamente criadas para filtrar o acesso à rede ou à Internet através de qualquer adaptador. Por defeito, as regras aplicam-se a qualquer rede. 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).
- **PROTOCOLO** - o protocolo IP ao qual a regra se aplica. Por defeito, as regras aplicam-se a qualquer protocolo.
- **TRÁFEGO** - a regra aplica-se em ambas as direções, entrada e saída.
- **PORTAS** - o protocolo PORTA ao qual a regra se aplica. Por predefinição, as regras aplicam-se a todas as portas.

- **IP** - o protocolo Internet (IP) ao qual a regra se aplica. Por predefinição, as regras aplicam-se a qualquer endereço IP.
- **ACESSO** - se a aplicação permite ou recusa acesso à rede ou Internet em circunstâncias específicas.

Para editar ou eliminar as regras da aplicação selecionada, clique no ícone ⋯.

- **Editar regra** - abre uma janela onde é possível editar a regra atual.
- **Eliminar regra** - é possível optar por remover o conjunto de regras atual para a aplicação selecionada.

A adicionar regras de aplicações

Para adicionar uma regra de aplicação:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **FIREWALL**.
4. Clique na hiperligação **Adicionar regra** na parte superior da janela **REGRAS**.

Na janela **DEFINIÇÕES** pode aplicar as seguintes alterações:

- **Aplicar esta regra a todas as aplicações.** Ative esta opção para aplicar a regra criada a todas as aplicações.
- **Caminho do Programa.** Clique em **Explorar** para selecionar a aplicação à qual a regra se aplica.
- **Permissão.** Selecione uma das seguintes permissões disponíveis:

Permissão	Descrição
Permitir	À aplicação especificada será permitido o acesso à rede / Internet nas circunstâncias determinadas.
Bloquear	À aplicação especificada será negado o acesso à rede / Internet nas circunstâncias determinadas.

- **Tipo de rede.** Selecione o tipo de rede ao qual a regra se aplica. Pode alterar o tipo abrindo o menu pendente **Tipo de Rede** e selecionando um dos tipos disponíveis na lista.

Tipo de rede	Descrição
Qualquer Rede	Permite todo o tráfego entre o seu computador e outros computadores independentemente do tipo de rede.
Casa/Escritório	Permite o tráfego entre o seu computador e os computadores na rede local.
Público	Todo o tráfego é filtrado.

- **Protocolo.** Selecione do menu o protocolo IP ao qual a regra se aplica.
  - Se deseja que a regra se aplique a todos os protocolos, selecione **Todos**.
  - Se deseja que a regra se aplique ao TCP, selecione **TCP**.
  - Se deseja que a regra se aplique ao UDP, selecione **UDP**.
  - Se pretender que a regra se aplique a ICMP, selecione **ICMP**.
  - Se pretender que a regra se aplique a IGMP, selecione **IGMP**.
  - Se quiser que a regra se aplique num protocolo específico, introduza o número atribuído ao protocolo que quiser filtrar no campo de edição em branco.

    Nota

    Os números dos protocolos IP são atribuídos pelo Internet Assigned Numbers Authority (IANA). Pode encontrar a lista completa de números IP atribuidos em http://www.iana.org/assignments/protocol-numbers.

- **Direção.** Selecione do menu a direção do tráfego ao qual a regra se aplica.

Direção	Descrição
Saída	A regra aplica-se apenas ao tráfego de saída.
Entrada	A regra aplica-se apenas ao tráfego de entrada.
Ambos	A regra aplica-se em ambos os sentidos.

Na janela **AVANÇADO** pode personalizar as seguintes definições:

- **Endereço Local Customizado.** Especifique o endereço IP local e a porta aos quais a regra se aplica.

- **Endereço remoto personalizado.** Especifique o endereço IP remoto e a porta aos quais a regra se aplica.

Para remover o conjunto de regras atual e restaurar as predefinições, clique na hiperligação **Repor regras** na parte superior da janela **REGRAS**.

4.5.2. Gerir definições da ligação

Independentemente de se ligar à Internet por Wi-Fi ou adaptador Ethernet, pode configurar as definições que devem ser aplicadas para uma navegação segura. As opções disponíveis são:

- **Dinâmica** – o tipo de rede será definido automaticamente com base no perfil da rede ligada, doméstica/escritório ou pública. Quando isto acontece, só serão aplicadas as regras de firewall do tipo de rede específica ou as definidas para se aplicarem a todos so tipos de rede.
- **Doméstica/escritório** – o tipo de rede será sempre doméstica/escritório, independentemente do perfil da rede ligada. Quando isto acontece, só serão aplicadas as regras de firewall para doméstica/escritório ou as definidas para se aplicarem a todos so tipos de rede.
- **Pública** – o tipo de rede será sempre pública, independentemente do perfil da rede ligada. Quando isto acontece, só serão aplicadas as regras de firewall para pública ou as definidas para se aplicarem a todos so tipos de rede.

Para configurar os adaptadores de rede:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **FIREWALL**.
4. Selecione o separador **TIPO DE REDE**.
5. Selecione as definições que pretende aplicar ao estabelecer ligação com os seguintes adaptadores:
   - Wi-Fi
   - Ethernet

4.5.3. Configurar definições avançadas

Para definições avançadas da firewall:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **FIREWALL**.
4. Selecione o separador **DEFINIÇÕES**.

É possível configurar as seguintes funcionalidades:

- **Bloquear scans das portas na rede** - deteta e bloqueia tentativas de encontrar quais portas encontram-se 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.

- **Modo Paranoico** - são apresentados alertas sempre que uma aplicação tenta estabelecer ligação com a Internet. Selecione **Permitir** ou **Bloquear**. Quando o modo Paranoico está ligado, as funcionalidades Piloto Automático e Perfis são automaticamente desligadas. O Modo Paranoico pode ser utilizado em simultâneo com o **Modo de Bateria**.

- **Modo Stealth** - para não ser detetado por outros computadores. Clique em **Editar definições sigilosas** para escolher quando o seu dispositivo deve ou não ficar visível para outros computadores.

- **Comportamento predefinido da aplicação** - permite que o Bitdefender aplique definições automáticas às aplicações sem regras definidas. Clique em **Editar regras predefinidas** para escolher se as definições automáticas devem ser aplicadas ou não.

  - Automático - o acesso a aplicações será permitido ou recusado com base nas regras automáticas de firewall e utilizadores.
  - Permitir - as aplicações que não têm qualquer regra de firewall definidas serão permitidas automaticamente.
  - Bloquear - as aplicações que não têm qualquer regra de firewall definidas serão bloqueadas automaticamente.

4.6. Vulnerabilidade

Um passo importante na proteção do seu computador contra as pessoas e aplicações maliciosas é manter atualizado o seu sistema operativo e as

aplicações que usa regularmente. Além disso, para impedir o acesso físico não autorizado ao seu computador, devem ser configuradas palavras-passe fortes (palavras-passe que não é possível adivinhar facilmente) para cada conta de utilizador Windows e para as redes Wi-Fi às quais esta ligado.

O Bitdefender verifica automaticamente o seu sistema por vulnerabilidades e alerta-o sobre eles. Verifique o seguinte:

- aplicações desatualizadas no seu computador.
- actualizações do Windows em falta.
- Senhas fracas para as contas de utilizador do Windows.
- routers e redes sem fios não protegidos.

O Bitdefender proporcionar duas formas fáceis de resolver as vulnerabilidades do seu sistema:

- Pode analisar o seu sistema por vulnerabilidades e repará-las passo a passo com a opção **Análise de Vulnerabilidades**.
- Utilizando a monitorização automática de vulnerabilidades, pode verificar e reparar as vulnerabilidades detetadas na janela Notificações.

Deve verificar e resolver as vulnerabilidades do sistema semanal ou quinzenalmente.

4.6.1. Procurar vulnerabilidades no seu sistema

Para corrigir as vulnerabilidades do sistema utilizando a opção Análise de Vulnerabilidade:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique no botão de ação **Análise de vulnerabilidade**.
3. Aguarde para o Bitdefender analisar as vulnerabilidades do seu sistema. Para interromper o processo de análise, clique no botão **Saltar** na parte superior da janela.
   - **Atualizações Críticas do Windows**

     Clique em **Ver detalhes** para ver uma lista de atualizações críticas do Windows que não foram instaladas no seu computador.

     Para iniciar a instalação das atualizações selecionadas, clique em **Instalar atualizações**. Note que a instalação das atualizações poderá

demorar um pouco e poderá ser necessário reiniciar o sistema para concluir a instalação. Se necessário, reinicie o sistema quando lhe convier.

- **Atualização de aplicações**

  Se a aplicação não estiver atualizada, clique na ligação **Transferir a nova versão** para transferir a versão mais recente.

  Clique em **Ver detalhes** para ver informações sobre a aplicação que necessita de ser atualizada.

- **Palavras-passe fracas de contas do Windows**

  Pode ver a lista dos utilizadores de contas Windows configurados no seu computador e o nível de proteção que as suas palavras-passe garantem.

  Clique em **Alterar palavra-passe ao iniciar sessão** para definir uma nova palavra-passe para o seu sistema.

  Clique em **Ver detalhes** para modificar as palavras-passe fracas. Pode escolher entre pedir ao utilizador para alterar a palavra-passe da próxima vez que iniciar sessão ou o próprio alterar a palavra-passe imediatamente. Para obter uma palavra-passe forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).

- **Redes Wi-Fi fracas**

  Clique em **Ver detalhes** para saber mais sobre a rede sem fios à qual está ligado. Se for recomendado utilizar uma palavra-passe forte para a rede da sua casa; clique no link correspondente.

  Quando outras recomendações estiverem disponíveis, siga as instruções fornecidas para garantir que a rede da sua casa fica protegida contra hackers.

No canto superior direito da janela, pode filtrar os resultados de acordo com as suas preferências.

4.6.2. Usar monitorização de vulnerabilidade automática

O Bitdefender verifica o seu sistema quanto a vulnerabilidades regularmente, em segundo plano, e mantém os registos de problemas detetados na janela Notificações.

Para verificar e reparar os problemas detetados:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. No separador **Todas**, selecione a notificação referente à verificação de vulnerabilidades.
3. Pode ver a informação detalhada sobre as vulnerabilidades do sistema detetadas. Dependendo da incidencia, para reparar uma vulnerabilidade específica proceda da seguinte forma:
   - Se as atualizações para o Windows estiverem disponíveis para o Windows, clique em **INSTALAR**.
   - Se as atualizações automáticas do Windows estiverem desativadas, clique em **ATIVAR**.
   - Se uma aplicação estiver desatualizada, clique em **ATUALIZAR AGORA** para obter a hiperligação para a página de Internet do fornecedor a partir da qual pode instalar a versão mais recente dessa aplicação.
   - Se uma conta de utilizador do Windows tiver uma palavra-passe fraca, clique em **ALTERAR PALAVRA-PASSE** para obrigar o utilizador a mudar a palavra-passe no próximo início de sessão ou alterá-la por si mesmo. Para obter uma palavra-passe forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).
   - Se a funcionalidade de Execução Automática do Windows estiver ativada, clique em **REPARAR** para desativá-la.
   - Se o router que tem configurado tiver uma palavra-passe fraca, clique em **ALTERAR PALAVRA-PASSE** para aceder à sua interface a partir da qual é possível definir uma palavra-passe forte.
   - Se a rede à qual está ligado apresentar vulnerabilidades que possam expor o seu sistema a riscos, clique em **ALTERAR DEFINIÇÕES WI-FI**.

Para configurar as definições de monitorização de vulnerabilidades:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **VULNERABILIDADE**, clique no botão ON/OFF.

Importante
Para ser notificado automaticamente sobre vulnerabilidades no sistema ou nas aplicações, mantenha a opção **Vulnerabilidade** ativada.

4. Escolha as vulnerabilidades do sistema que deseja que sejam regularmente verificadas usando os botões correspondentes.

   Atualizações Críticas do Windows
   Verifique se o seu sistema operativo Windows possui as mais recentes e importantes atualizações de segurança da Microsoft.

   Atualização de aplicações
   Verifique se as aplicações instaladas no seu sistema estão atualizadas. As aplicações desatualizadas podem ser exploradas por software malicioso, tornando o PC vulnerável a ataques externos.

   Palavras-passe fracas
   Verifique se as palavras-passe dos routers e contas Windows configuradas no sistema são fáceis de descobrir ou não. A definição de palavras-passe difíceis de descobrir (palavras-passe fortes) torna muito difícil a invasão do seu sistema pelos hackers. Uma palavra-passe forte inclui maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).

   Autorun dispositivos media
   Verifique o estado do recurso Windows Autorun. Esta característica permite que as aplicações se iniciem automaticamente a partir dos CDs, DVDs, drives USB ou outros dispositivos externos.

   Alguns tipos de ameaças utilizam Autorun para se propagar automaticamente dos suportes multimédia removíveis do PC. Por isso, recomenda-se a desactivação desta janela.

   Notificações do Assessor de Segurança de redes Wi-Fi
   Verifique se a rede doméstica sem fios à qual está ligado é segura ou não e se tem vulnerabilidades. Além disso, verifique se a palavra-passe do seu router doméstico é suficientemente e se pode torná-la mais segura.

   A maioria das redes não protegidas não são seguras, permitindo o fácil acesso de hackers às suas atividades privadas.

Nota
Se desativar a monitorização de uma vulnerabilidade específica, os problemas relacionados não serão mais registados na janela de notificações.

4.6.3. Consultor de Segurança Wi-Fi

Enquanto caminha, trabalha num café ou aguarda no aeroporto, ligar-se a uma rede pública sem fios para realizar pagamentos, verificar e-mails ou aceder às contas de redes sociais pode ser a solução mais rápida. Enquanto isso, pessoas curiosas tentam roubar os seus dados pessoais vendo como as informações fluem ao longo da rede.

Dados pessoais consistem em palavras-passe e nomes de utilizadores que utilizar para aceder às suas contas online, tais como e-mails, contas bancárias, contas de redes sociais, mas também mensagens enviadas por si.

Geralmente, as redes públicas sem fios tendem a ser menos seguras uma vez que não necessitam de qualquer palavra-passe para efetuar a ligação ou, caso seja necessária uma palavra-passe, esta é disponibilizada a qualquer pessoa que pretenda ligar-se. Além disso, podem ser redes maliciosas ou "honeypot", que representam um alvo para criminosos informáticos.

Para protegê-lo contra os perigos dos hotspots de ligação sem fios públicos não seguros ou não encriptados, o Consultor de Segurança do Wi-Fi do Bitdefender analisa a segurança de uma rede sem fios e, quando necessário, recomenda que use o Bitdefender VPN.

O Consultor de Segurança Wi-Fi do Bitdefender fornece informações sobre:

- Redes Wi-Fi domésticas
- Redes Wi-Fi públicas

Ativar ou desativar as notificações do Consultor de Segurança Wi-Fi

Para ativar ou desativar as notificações do Consultor de Segurança Wi-Fi:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.

3. Clique no ícone ⚙ no canto inferior direito do painel **VULNERABILIDADE**.
4. Na janela **DEFINIÇÕES**, clique no botão ON/OFF correspondente.

Configurar a rede Wi-Fi doméstica

Para começar a configurar a sua rede doméstica:

1. Clique no ícone Ⓑ na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **VULNERABILIDADE**, clique em **Consultor de Segurança do Wi-Fi**.
4. No separador **WI-FI DOMÉSTICO**, clique no botão **SELECIONAR WI-FI DOMÉSTICO**.

   Uma lista com redes sem fios às quais já esteve ligado é agora exibida.
5. Indique a sua rede doméstica e, em seguida, clique em **SELECIONAR**.

Se uma rede doméstica for considerada insegura ou desprotegida, são exibidas as recomendações de configuração para aumentar a sua segurança.

Para remover a rede sem fios definida como rede doméstica, clique no botão **REMOVER**.

Wi-Fi público

Enquanto está ligado a uma rede sem fios insegura ou desprotegida, o perfil de Wi-Fi pública é ativado. Ao executar neste perfil, o Bitdefender Total Security é definido automaticamente de modo a obter as seguintes definições de programa:

- Advanced Threat Defense ativado
- A Firewall do Bitdefender é ativada e as definições seguintes são aplicadas ao seu adaptador sem fios:
  - Modo Stealth - : LIGADO
  - Tipo de rede- Pública
- As seguintes definições da Proteção na Web estão desativadas:
  - Analisar SSL
  - Proteção contra fraudes
  - Proteção contra phishing

- Está disponível um botão que abre o Bitdefender Safepay™. Neste caso, a proteção Hotspot para redes desprotegidas está ativada por predefinição.

Verificar informações sobre redes Wi-Fi

Para verificar as informações sobre as redes sem fios a que é habitual ligar-se:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **VULNERABILIDADE**, clique em **Consultor de Segurança do Wi-Fi**.
4. Consoante as informações necessárias, selecione um dos dois separadores **WI-FI DOMÉSTICO** ou **WI-FI PÚBLICO**.
5. Clique em **Visualizar detalhes** junto à rede sobre a qual pretende obter mais informações.

Existem três tipos de redes sem fios filtrados por importância, sendo cada tipo indicado com um ícone específico:

Wi-Fi desprotegida - indica que o nível de segurança da rede é reduzido. Isto significa que existe um risco elevado de utilização e não é recomendado realizar pagamentos ou verificar contas bancárias sem uma proteção adicional. Nestas situações, recomendamos a utilização do Bitdefender Safepay™ com a proteção Hotspot para redes desprotegidas ativada.

Wi-Fi desprotegida - indica que o nível de segurança da rede é moderado. Isto significa que podem existir vulnerabilidades e não é recomendado realizar pagamentos ou verificar contas bancárias sem uma proteção adicional. Nestas situações, recomendamos a utilização do Bitdefender Safepay™ com a proteção Hotspot para redes desprotegidas ativada.

Wi-Fi é segura - indica que a rede utilizada é segura. Neste caso, pode utilizados dados confidenciais para realizar operações online.

Ao clicar na ligação **Ver detalhes** na área de cada rede, são apresentados os seguintes detalhes:

- **Segura** - onde pode ver se a rede selecionada está segura ou não. As redes não encriptadas podem deixar os seus dados expostos.
- **Tipo de encriptação** - aqui pode visualizar o tipo de encriptação utilizado pela rede selecionada. Alguns tipos de encriptação podem não ser seguros. Assim, recomendamos vivamente verificar as informações sobre o tipo

de encriptação exibido para garantir que está protegido ao navegar na Web.

- **Canal/Frequência** - aqui pode visualizar a frequência do canal utilizada pela rede selecionada.
- **Força da palavra-passe** - aqui pode visualizar a força da palavra-passe. Observe que as redes que têm palavras-passe fracas definidas representam um alvo para os cibernautas criminosos.
- **Tipo de início de sessão** - aqui pode visualizar se a rede selecionada está ou não protegida com uma palavra-passe. É altamente recomendado ligar-se apenas a redes que possuem palavras-passe fortes definidas.
- **Tipo de autenticação** - aqui pode visualizar o tipo de autenticação utilizado pela rede selecionada.

Mantenha a opção **Notificação** ativada para receber notificações sempre que o seu sistema é ligado a esta rede.

4.7. Proteção da Webcam

O facto de que os hackers podem controlar a sua câmara Web para o espiar já não é uma novidade e as soluções para o proteger, tal como revogar privilégios de aplicações, desativar a câmara integrada do dispositivo ou tapá-la, não são muito práticas. Para evitar futuras tentativas de acesso à sua privacidade, a Proteção da Câmara Web do Bitdefender monitoriza permanentemente as aplicações que tentam aceder à câmara e bloqueiam as que não estão listadas como fidedignas.

Como medida de segurança, será notificado sempre que uma aplicação não fidedigna tentar obter acesso à câmara, mesmo se a funcionalidade Piloto Automático estiver ativada.

Ativar ou desativar a Proteção da Câmara Web

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **PROTEÇÃO DA CÂMARA WEB**, clique no botão ON/OFF.

Configuração da Proteção da Câmara Web

É possível configurar as regras que devem ser aplicadas quando uma aplicação tentar aceder à sua câmara ao seguir estes passos:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **PROTEÇÃO DA CÂMARA WEB**.

Regras de bloqueio de aplicações

- **Bloquear todo o acesso à câmara Web** - nenhuma aplicação pode aceder à sua câmara Web.
- **Bloquear o acesso dos browsers à câmara Web** - nenhum browser exceto Internet Explorer e Microsoft Edge podem aceder à câmara Web. Devido ao procedimentos das aplicações da Loja do Windows em serem executadas num único processo, o Internet Explorer e o Microsoft Edge não podem ser detetados pelo Bitdefender como browsers e são excluídos desta definição.
- **Definir o acesso à câmara Web por aplicações com base na escolha dos utilizadores de Bitdefender** - se a maioria dos utilizadores de Bitdefender considerar uma aplicação popular como sendo inofensiva, o seu acesso à câmara Web é automaticamente definido como Permitir. Se uma aplicação popular for considerada como perigosa por muitas pessoas, o seu acesso será automaticamente definido como Bloqueado.

  Será informado sempre que uma das aplicações instaladas seja listada como bloqueada pela maioria dos utilizadores de Bitdefender, mesmo se a funcionalidade Piloto Automático estiver ativada.

Notificações

- **Notificar-me quando as aplicações permitidas estabelecerem ligação com a câmara Web** - será notificado sempre que uma aplicação autorizada aceder à câmara Web, mesmo se a funcionalidade Piloto Automático estiver ativada.

Adicionar aplicações à lista de Proteção da Câmara Web

As aplicações que tentam estabelecer ligação à sua câmara Web são detetadas automaticamente e, dependendo do respetivo comportamento e da escolha da comunidade, o acesso é permitido ou recusado. No entanto, é possível começar a configurar manualmente a ação que deve ter tomada ao seguir estes passos:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **PROTEÇÃO DA CÂMARA WEB**, clique em **Acesso à câmara Web**.
4. A primeira vez que aceder à Proteção contra Webcam, verá uma apresentação da função.
5. Clique na hiperligação pretendida:
   - **Selecionar aplicações da Loja do Windows para adicionar à lista de permissões** — é apresentada uma lista com aplicações da Loja do Windows detetadas. Ative os botões perto das aplicações que pretende adicionar à lista.
   - **Comece a adicionar aplicações à lista de acesso da câmara Web** — aceda ao ficheiro .exe que pretende adicionar à lista e, em seguida, clique em **OK**.

     Para adicionar aplicações adicionais, clique na hiperligação **Adicionar uma nova aplicação à lista**.

Clique no botão Acesso autorizado/Acesso bloqueado.

Para ver o que os utilizadores do Bitdefender optaram por fazer com a aplicação selecionada, clique no ícone .

As aplicações que pedem acesso à câmara, assim como a hora da última atividade são apresentadas nesta janela.

Será notificado sempre que uma aplicação das aplicações autorizadas for bloqueada pelos utilizadores do Bitdefender, independentemente do estado do Piloto Automático.

4.8. Safe Files

Ransomwares são softwares maliciosos que atacam sistemas vulneráveis bloqueando-os e exigindo dinheiro para permitir que o utilizador volte a ter

controlo do seu sistema. Este software malicioso finge ser inteligente ao exibir mensagens falsas para assustar o utilizador, persuadindo-o a realizar o pagamento solicitado.

A infeção pode espalhar-se através de e-mails de spam, transferência de anexos ou ao visitar sites infetados e instalar aplicações maliciosas sem informar o utilizador sobre o que está a acontecer com o seu sistema.

Ransomwares podem ter um dos seguintes comportamentos, prevenindo que o utilizador aceda ao seu sistema:

- Encriptar dados privados e pessoais sem a possibilidade de desencriptação até que um resgate seja pago pela vítima.
- Bloquear o ecrã do computador e exibir uma mensagem a solicitar dinheiro. Neste caso, nenhum ficheiro é encriptado, mas o utilizador é forçado a realizar o pagamento.
- Bloquear a execução de aplicações.

Com Bitdefender Safe Files, é possível manter os seus ficheiros pessoais, tais como documentos, fotografias ou filmes, protegidos contra ataques de ransomware.

Nota
Advanced Threat Defense e Safe Files são duas camadas de proteção contra ransomware. Advanced Threat Defense é a funcionalidade que impede ataques de ransomware nas áreas fundamentais do sistema, enquanto Safe Files garante que nenhum ficheiro importante no computador é encriptado.

4.8.1. Ativar ou desativar Safe Files

Para ativar ou desativar a funcionalidade Safe Files:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **SAFE FILES**, clique no botão ON/OFF.

Sempre que uma aplicação tentar aceder a um dos ficheiros protegidos, é apresentado um pop-up do Bitdefender. Pode permitir ou bloquear o acesso.

Nota
A funcionalidade Safe Files não está ativada por predefinição.

4.8.2. Proteja os seus ficheiros pessoais contra ataques de ransomwares

Se quiser proteger ficheiros pessoais:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **SAFE FILES**, clique em **Pastas Protegidas**.
4. A primeira vez que aceder à Defesa contra Ameaças, verá uma apresentação da função. Clique em **PROTEGER MAIS PASTAS** para continuar.
5. Selecione a pasta que pretende proteger e clique em **OK**.

   Para adicionar pastas adicionais, clique na hiperligação **Proteger mais pastas**. Em alternativa, arraste pastas para esta janela.

Por predefinição, as pastas Imagens, Vídeos, Música, Ambiente de Trabalho e Transferências estão protegidas contra ataques de ameaças. Dados pessoais armazenados em serviços online de armazenamento de ficheiros, como Box, Dropbox, Google Drive e OneDrive também são adicionados ao ambiente de proteção, desde que as suas aplicações estejam instaladas no sistema.

Para evitar o abrandamento do sistema, recomendamos que adicione no máximo 30 pastas ou guarde vários ficheiros numa única pasta.

> **Nota**
> Pastas personalizadas apenas podem ser protegidas para os utilizadores atuais. Ficheiros de sistema e de aplicações não podem ser adicionados às exceções.

4.8.3. A configurar o acesso de aplicações

As aplicações que tentam mudar ou apagar ficheiros protegidos podem ser sinalizadas como potencialmente inseguras e adicionadas à lista de aplicações bloqueadas. Se uma aplicação como esta estiver bloqueada e não tiver a certeza se o respetivo comportamento é normal, pode autorizá-la ao seguir estes passos:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.

2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **SAFE FILES**, clique em **Acesso a aplicações**.
4. As aplicações que pediram para alterar ficheiros nas suas pastas protegidas são listadas. Clique no botão Permitir junto da aplicação que tem a certeza que é segura.

Na mesma janela, é possível desativar a proteção contra ransomware para aplicações específicas ao clicar no botão Bloquear.

Se pretender adicionar novas aplicações à lista, clique na hiperligação **Adicionar uma nova aplicação à lista**.

4.8.4. Proteção no arranque

Sabe-se que muitas aplicações maliciosas são configuradas para serem executadas no arranque do sistema, o que pode danificar gravemente a máquina. A Proteção no arranque do Bitdefender verifica todas as áreas essenciais do sistema antes que todos os ficheiros sejam carregados, sem impacto no desempenho do sistema.

Para desativar a Proteção na inicialização:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **SAFE FILES**.
4. Clique no botão ON/OFF.

Nota
As aplicações adicionadas às exclusões serão analisadas e tratadas em conformidade.

4.9. Encriptação de ficheiro

O Cofre de Ficheiros Bitdefender permite-lhe criar drives lógicas encriptadas, e protegidas por palavra-passe (cofres) no seu computador onde pode armazenar em segurança os seus documentos confidenciais e sensíveis. Os dados armazenados nos cofres apenas podem ser acedidos pelos utilizadores que sabem a palavra-passe.

A palavra-passe permite-lhe abrir, armazenar dados no cofre e fechá-lo ao mesmo tempo que o mantém seguro. Quando um cofre é aberto, pode adicionar-lhe ficheiros, aceder aos que lá estão ou alterá-los.

Fisicamente, o cofre é um ficheiros armazenado no seu disco duro local com a extensão .bvd. Apesar dos ficheiros físicos que representam as drives de cofre poderem ser acedidos a partir de um sistema operativo diferente (tal como Linux), a informação armazenada não pode ser lida por estar encriptada.

Os cofres de ficheiros podem ser geridos a partir da janela do Bitdefender ou com o menu contextual do Windows e da unidade lógica associada ao cofre.

Gerir os cofres de ficheiros

Para gerir os seus cofres de ficheiros do Bitdefender, clique no ícone na barra lateral esquerda da interface do Bitdefender.

Os cofres de ficheiros existentes aparecem na funcionalidade **Cofres de ficheiros**.

Criar cofres de ficheiros

Para criar um novo cofre:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **ENCRIPTAÇÃO DE FICHEIROS**, clique em **Criar Novo Cofre de Ficheiros**.
4. Especifique o nome e a localização do cofre de ficheiros.
   - Escreva o nome do cofre de ficheiros no campo correspondente.
   - Clique em **Explorar** para selecionar a localização do cofre e guarde o cofre de ficheiros sob o nome desejado.
5. Escolha uma letra do disco no menu correspondente. Quando abre o cofre, um disco virtual com a letra selecionada aparecerá em O Meu Computador.
6. Se deseja mudar o tamanho por defeito (100 MB) do cofre, utilize as setas para cima e para baixo na caixa **Tamanho do Cofre (MB)**.

7. Escreva a palavra-passe pretendida para o cofre nos campos **Palavra-passe** e **Confirmar palavra-passe**. A palavra-passe tem de ter pelo menos 8 caracteres. Qualquer pessoa que tente abrir o cofre e aceder aos seus ficheiros tem de inserir a palavra-passe.
8. Clique em **Criar**.

O Bitdefender informá-lo-á imediatamente do resultado da operação. Se ocorreu um erro, use a mensagem de erro para resolver o problema.

Para criar um cofre de forma mais rápida, clique com o botão direito no seu ambiente de trabalho ou numa pasta no seu computador, aponte para o **Bitdefender** > **Cofre de Ficheiros do Bitdefender** e selecione **Criar Cofre de Ficheiros**.

Nota
Poderá ser conveniente que guarde todos os cofres de ficheiros no mesmo local. Desta forma poderá localizá-los mais rapidamente.

Importar um cofre de ficheiros

Para importar um cofre de ficheiros armazenado localmente:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **ENCRIPTAÇÃO DE FICHEIROS**, clique em **Importar cofre**.
4. Procure a localização do cofre e selecione-o (o ficheiro .bvd).
5. Clique em **Abrir**.

Abrir Cofres de Ficheiros

De forma a poder aceder e trabalhar com os ficheiros armazenados no cofre, tem de o abrir. Quando abre o cofre, um disco virtual aparece em O Meu Computador. A drive tem a denominação da letra que atribuiu ao cofre.

Para abrir um cofre:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.

   Os cofres de ficheiros existentes aparecem na funcionalidade **Cofres de ficheiros**.

2. Clique na hiperligação **Ver cofres** e, em seguida, selecione o cofre que pretende abrir.
3. Clique no botão **Desbloquear** e, em seguida, escreva a palavra-passe necessária.
4. Clique em **OK** e, em seguida, no botão **Abrir** para abrir o seu cofre.

O Bitdefender informá-lo-á imediatamente do resultado da operação. Se ocorreu um erro, use a mensagem de erro para resolver o mesmo.

Para abrir um cofre mais rapidamente, localize no seu computador o ficheiro .bvd que representa o cofre que pretende abrir. Clique com o botão-direito no ficheiro, aponte para **Cofre Ficheiros Bitdefender** e selecione **Abrir**. Introduza a palavra-passe necessária e, em seguida, clique em **OK**.

Adicionar ficheiros aos cofres

Antes que possa adicionar ficheiros ou pastas ao cofre, deve de abri-lo.

Para adicionar ficheiros novos ao seu cofre:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **ENCRIPTAÇÃO DE FICHEIROS**.
4. Na janela **OS MEUS COFRES**, selecione o cofre que pretende abrir.
5. Clique no botão **Desbloquear** e, em seguida, escreva a palavra-passe necessária.
6. Clique no botão **Abrir** para abrir o seu cofre.
7. Adicione ficheiros ou pastas como faria normalmente no Windows (por exemplo, pode utilizar o método de copiar e colar).

Para adicionar ficheiros de forma mais rápida ao seu cofre, clique com o botão direito do rato no ficheiro que pretende copiar para um cofre, selecione **Cofre de Ficheiros do Bitdefender** e clique em **Adicionar ao Cofre de Ficheiros**.

- Se apenas um cofre estiver aberto, o ficheiro ou pasta é copiado diretamente para esse cofre.

- Se vários cofres estiverem abertos, ser-lhe-á solicitado que escolha o cofre para onde deseja copiar o item. Selecione do menu a letra da drive correspondente ao cofre desejado e clique **OK** para o copiar.

Bloquear cofres

Quando terminar de trabalhar sobre um cofre de ficheiros, deve fechá-lo de forma a proteger os seus dados. Ao fechar o cofre, o correspondente disco virtual desaparecerá de O Meu Computador. Logo, o acesso aos dados armazenados no cofre fica completamente bloqueado.

Para bloquear um cofre:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. No painel **Cofres de ficheiros**, clique em **Ver cofres**.
3. Na janela **OS MEUS COFRES**, selecione o cofre que deseja bloquear.
4. Clique no botão **Trancar**.

O Bitdefender informá-lo-á imediatamente do resultado da operação. Se ocorreu um erro, use a mensagem de erro para resolver o problema.

Para trancar um cofre de forma mais rápida, clique com o botão direito do rato no ficheiro .bvd que representa o cofre, selecione **Cofre de Ficheiros do Bitdefender** e clique em **Trancar**.

Remover ficheiros do cofre

De forma a remover os ficheiros ou pastas do cofre, o cofre deve de ser aberto. Para remover ficheiros ou pastas de um cofre:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **ENCRIPTAÇÃO DE FICHEIROS**.
4. Na janela **OS MEUS COFRES**, selecione o cofre de onde pretende remover os ficheiros.
5. Clique no botão **Destrancar**, caso esteja trancado.
6. Clique no botão **Abrir**.

Remover os ficheiros ou pastas como normalmente faz no Windows (por exemplo, clique botão-direito no ficheiro que quer apagar e selecione **Apagar**).

Mudar palavra-passe do Cofre

A palavra-passe protege o conteúdo do cofre contra acessos não-autorizados. Apenas os utilizadores que sabem a palavra-passe podem abrir o cofre e aceder aos documentos e dados armazenados no seu interior.

O cofre tem de ser fechado antes que possa mudar a sua palavra-passe. Para alterar a palavra-passe de um cofre:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **ENCRIPTAÇÃO DE FICHEIROS**.
4. Na janela **OS MEUS COFRES**, selecione o cofre para onde pretende alterar a palavra-passe.
5. Clique no botão **Definições**.
6. Insira a palavra-passe atual do cofre no campo **Palavra-passe antiga** .
7. Insira a nova palavra-passe nos campos **Nova palavra-passe** e **Confirmar nova palavra-passe** .

> **Nota**
> A palavra-passe tem de ter pelo menos 8 caracteres. Para obter uma palavra-passe forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).

O Bitdefender informá-lo-á imediatamente do resultado da operação. Se ocorreu um erro, use a mensagem de erro para resolver o problema.

Para alterar de forma mais rápida a palavra-passe de um cofre, localize no seu computador o ficheiro .bvd que representa o cofre. Clique com o botão-direito do rato no ficheiro, aponte para **Cofre Ficheiros Bitdefender** e selecione **Alterar palavra-passe do cofre**.

4.10. Proteção do Gestor de palavras-passe para as suas credenciais

Utilizamos os nossos computadores para efetuar compras online ou pagar as contas, para nos ligarmos a plataformas de comunicação social ou para iniciar sessão em aplicações de mensagens instantâneas.

Mas como todos sabemos, nem sempre é fácil memorizar a palavra-passe!

E se não formos cuidadosos ao navegar online, as nossas informações privadas, tais como endereço de e-mail, ID de mensagens instantâneas ou os dados do cartão de crédito, podem ficar comprometidas.

Guardar as suas palavras-passe ou os seus dados pessoais numa folha ou no computador pode ser perigoso, pois podem ser acedidos e utilizados por pessoas que pretendam roubar e utilizar essas informações. E memorizar todas as palavras-passe definidas para as suas contas online ou para os seus sites Web favoritos não é uma tarefa fácil.

Portanto, há alguma forma de garantir que encontramos as nossas palavras-passe quando necessitamos das mesmas? E podemos ter a certeza de que as nossas palavras-passe secretas estão sempre seguras?

O Gestor de palavras-passe ajuda-o a controlar as suas palavras-passe, protege a sua privacidade e proporciona uma experiência de navegação segura.

Utilizando uma única palavra-passe principal para aceder às suas credenciais, o Gestor de palavras-passe simplifica a proteção das suas palavras-passe numa Carteira.

Para oferecer a melhor proteção para as suas atividades online, o Gestor de palavras-passe está integrado com o Bitdefender Safepay™ e fornece uma solução única para as várias maneiras com que os seus dados pessoais podem ficar comprometidos.

O Gestor de palavras-passe protege as seguintes informações privadas:

- Informações pessoais, tais como endereço de e-mail e número de telefone
- Credenciais de início de sessão dos sites Web
- Informações de contas bancárias ou o número do cartão de crédito
- Dados de acesso às contas de e-mail
- Palavras-passe para as aplicações

- Palavras-passe das redes Wi-Fi

Criar uma nova base de dados Carteira

A Carteira do Bitdefender é onde pode armazenar os seus dados pessoais. Para uma experiência no navegador, deve criar uma base de dados Carteira conforme o seguinte:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **CARTEIRA**, clique em **Criar nova carteira**.
4. Clique no botão **Criar nova**.
5. Digite as informações solicitadas nos campos correspondentes.
   - Etiqueta da Carteira - introduza um nome personalizado para a sua base de dados da Carteira.
   - Palavra-passe Principal - escreva uma palavra-passe para a sua Carteira.
   - Escrever novamente a Palavra-passe - volte a escrever a palavra-passe que definiu.
   - Sugestão - escreva uma sugestão para lembrar-se da palavra-passe.
6. Clique em **Continuar**.
7. Nesta etapa, pode escolher armazenar as suas informações na nuvem. Se selecionar Sim, as suas informações bancárias irão permanecer armazenadas localmente no seu dispositivo. Escolha a opção pretendida, em seguida, clique em **Continuar**.
8. Selecione o navegador da Internet de onde deseja importar as credenciais.
9. Clique em **Terminar**.

Importar uma base de dados existente

Para importar a base de dados da carteira armazenada localmente:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **CARTEIRA**, clique em **Criar nova carteira**.
4. Clique no botão **A partir do alvo**.

5. Aceda ao local no seu dispositivo onde deseja guardar a base de dados da carteira e escolha um nome.
6. Clique em **Abrir**.
7. Dê um nome à sua Carteira e introduza a palavra-passe atribuída quando foi criada pela primeira vez.
8. Clique em **Importar**.
9. Selecione os programas cujas credenciais pretende que a Carteira importe e, de seguida, o botão **Terminar**.

Exportar a base de dados da Carteira

Para exportar a sua base de dados do portfólio:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **CARTEIRA**, clique em **As minhas carteiras**.
4. Clique no ícone na carteira pretendida e, em seguida, selecione **Exportar**.
5. Procure o local da sua base de dados da carteira e selecione-o (o ficheiro .db).
6. Clique em **Guardar**.

> **Nota**
> A Carteira precisa de ser aberta para que a opção **Exportar** esteja disponível. Se a carteira que precisa de exportar estiver bloqueada, clique no botão **ATIVAR CARTEIRA** e, de seguida, digite a palavra-passe atribuída quando foi criada pela primeira vez.

Sincronize as suas carteiras na nuvem

Para ativar ou desativar a sincronização das carteiras na nuvem:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **CARTEIRA**, clique em **As minhas carteiras**.

4. Clique no ícone ⋮ na carteira pretendida e, em seguida, selecione **Definições**.
5. Escolha a opção pretendida na janela que aparecer, em seguida, clique em **Guardar**.

Nota
A Carteira precisa de ser aberta para que a opção **Exportar** esteja disponível. Se a carteira que precisa de sincronizar estiver bloqueada, clique no botão **ATIVAR CARTEIRA** e, de seguida, digite a palavra-passe atribuída quando foi criada pela primeira vez.

Gerir as suas credenciais da Carteira

Para gerir as suas palavras-passe:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **CARTEIRA**, clique em **As minhas carteiras**.
4. Selecione a base de dados da Carteira pretendida na janela **As Minhas Carteiras** e, em seguida, clique no botão **ATIVAR CARTEIRA**.
5. Introduza a palavra-passe principal e, de seguida, clique em **OK**.

Aparece uma nova janela. Selecione a categoria pretendida na parte superior da janela:

- Identidade
- Websites
- Online banking
- E-mails
- Apps
- Redes Wi-Fi

Adicionar/editar as credenciais

- Para adicionar uma nova palavra-passe, escolha a categoria pretendida acima, clique em **+ Adicionar item**, insira as informações nos campos correspondentes e clique no botão Guardar.

- Para editar uma entrada da lista, selecione-a e clique no botão **Editar**.
- Para eliminar uma entrada, selecione-a e clique no botão **Eliminar**.

Ativar ou desativar a proteção do Gestor de palavras-passe

Para ativar ou desativar a proteção do Gestor de Palavras-passe:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **CARTEIRA**, clique no botão ON/OFF.

Gerir as definições do Gestor de Palavras-passe

Para configurar a palavra-passe principal de forma detalhada:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **CARTEIRA**.
4. Selecione o separador **DEFINIÇÕES DE SEGURANÇA**.

Estão disponíveis as seguintes opções:

- **Solicitar a minha palavra-passe principal sempre que eu aceder ao meu PC** - ser-lhe-á solicitado a introduzir a palavra-passe principal ao aceder ao computador.
- **Solicitar palavra-passe principal quando abro browsers e aplicações** - ser-lhe-á solicitada a introdução da palavra-passe principal quando acede a um browser ou aplicação.
- **Não solicitar a minha palavra-passe principal** — não necessita de introduzir a sua palavra-passe principal ao aceder ao seu computador, um browser ou uma aplicação.
- **Bloquear automaticamente a Carteira quando deixo o meu PC sem supervisão** - ser-lhe-á solicitada a introdução da palavra-passe principal quando regressar ao seu computador após 15 minutos.

Importante
Não se esqueça da sua palavra-passe principal e registe-a num local seguro. Se esquecer a palavra-passe, terá de reinstalar o programa ou contactar o apoio do Bitdefender.

Melhore a sua experiência

Para selecionar os navegadores ou aplicações onde deseja integrar o Gestor de Palavras-passe:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **CARTEIRA**.
4. Selecione o separador **PLUGINS**.

   Marque uma aplicação para utilizar o Gestor de Palavras-passe e melhorar a sua experiência:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Safepay

Configurar o Preenchimento automático

A funcionalidade Preenchimento automático simplifica a ligação aos seus sites Web favoritos ou o início de sessão nas suas contas online. A primeira vez que introduzir as suas credenciais de início de sessão e informações pessoais no navegador da Internet, estes estarão automaticamente protegidos na Carteira.

Para configurar as definições de **Preenchimento automático**:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **CARTEIRA**.
4. Selecione o separador **DEFINIÇÕES DE PREENCHIMENTO AUTOMÁTICO**.

5. Configure as seguintes opções:
   - **Configure como a Carteira protege as suas credenciais**:
     - **Guardar credenciais automaticamente na Carteira** - as credenciais de início de sessão e outras informações pessoais como os detalhes do seu cartão de crédito e detalhes pessoais são guardados e atualizados automaticamente na sua Carteira.
     - **Perguntar-me sempre** - ser-lhe-á sempre perguntado se pretende adicionar as suas credenciais à Carteira.
     - **Não guardar, atualizarei as informações manualmente** - as credenciais só podem ser atualizadas na Carteira manualmente.
   - **Preencher automaticamente as credenciais de início de sessão**:
     - **Preencher automaticamente e sempre as credenciais de início de sessão** - ao credenciais são inseridas automaticamente no browser.
   - **Formulários de preenchimento automático**:
     - **Mostrar as minhas opções de preenchimento quando eu visitar uma página com formulários** - um pop-up com as opções de preenchimento irá aparecer sempre que o Bitdefender detetar que deseja realizar um pagamento online ou iniciar a sessão.

Gerir as informações do Gestor de Palavras-passe a partir do seu navegador

Pode gerir facilmente os detalhes do Gestor de Palavra-passe diretamente do seu navegador para ter todos os dados importantes à mão. O add-on da Carteira do Bitdefender é suportado pelos seguintes navegadores: Google Chrome, Internet Explorer e Mozilla Firefox, e também é integrado com o Safepay.

Para aceder à extensão da Carteira do Bitdefender, abra seu navegador, permita que o add-on seja instalado e clique no ícone na barra de ferramentas.

A extensão da Carteira do Bitdefender contém as seguintes opções:

- Abrir Carteira - abre a Carteira.
- Bloquear Carteira - bloqueia a Carteira.

- Sites Web - abre um submenu com todos os inícios de sessão em sites Web armazenados na Carteira. Clique em **Adicionar sites Web** para adicionar novos sites Web à lista.
- Preencher formulários - abre o submenu que contém as informações que adicionou para uma categoria específica. Aqui pode adicionar novos dados à sua Carteira.
- Gerador de Palavras-passe - permite-lhe gerar palavras-passe aleatórias que pode utilizar para contas novas ou existentes. Clique em **Mostrar definições avançadas** para personalizar a complexidade da palavra-passe.
- Definições - abre a janela de definições do Gestor de Palavras-passe.
- Relatar problema - relata qualquer problema encontrado com o Gestor de Palavras-passe do Bitdefender.

4.11. VPN

A aplicação do VPN pode ser instalada a partir do seu produto Bitdefender e utilizada sempre que desejar adicionar uma camada de proteção extra à sua ligação. A VPN funciona como um túnel entre o seu dispositivo e a rede à qual se liga, protegendo a sua ligação, encriptando os seus dados utilizando uma encriptação de nível bancário e escondendo o seu endereço IP onde quer que esteja. O seu tráfego é redirecionado por meio de um servidor separado, tornando o seu dispositivo quase impossível de ser identificado entre os incontáveis dispositivos que usam os nossos serviços. Além disso, enquanto estiver ligado à Internet com o Bitdefender VPN, pode aceder a conteúdos que normalmente são restritos em áreas específicas.

> **Nota**
> Alguns países censuram a Internet e, portanto, a utilização de VPN nos seus territórios foi banida por lei. Para evitar consequências legais, pode ser apresentada uma mensagem de aviso ao tentar utilizar a aplicação Bitdefender VPN pela primeira vez. Ao continuar a utilizar a funcionalidade, confirma que está ciente dos regulamentos aplicáveis e dos riscos aos quais pode estar exposto.

A instalar a VPN

A aplicação de VPN pode ser instalada a partir da interface do Bitdefender da seguinte forma:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel da **VPN**, clique em **Ativar VPN**.
4. Na janela com a descrição da aplicação da VPN, leia o **Acordo de Subscrição** e depois clique em **ATIVAR O Bitdefender VPN**.

   Aguarde um momento até os ficheiros serem transferidos e instalados.
5. Clique em **ABRIR O VPN BITDEFENDER** para finalizar o processo de instalação.

Nota
O Bitdefender VPN requer o .Net Framework 4.5.2 ou superior para ser instalado. Caso não tenha esse pacote instalado, uma janela de notificação aparecerá. Clique em **instalar o .Net Framework** para ser redirecionado para uma página onde pode transferir a versão mais recente deste software.

A abrir a VPN

Para aceder à interface principal do Bitdefender VPN, use um dos seguintes métodos:

- Do tabuleiro do sistema
  1. Clique com o botão direito no ícone na bandeja do sistema e depois clique em **Exibir**.
- A partir da interface do Bitdefender:
  1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
  2. Clique no botão de ação da **VPN**.

Interface da VPN

A interface do VPN exibe o estado da aplicação, conectado ou desconectado. O local do servidor para utilizadores com a versão gratuita é determinado automaticamente pelo Bitdefender para o servidor mais adequado, enquanto os utilizadores Premium têm a possibilidade de alterar o local do servidor ao qual desejam se ligar. Para mais informações sobre as subscrições de VPN, aceda "*Assinaturas*" (p. 272).

Para conectar ou desconectar, basta clicar no estado exibido no topo do ecrã ou clique com o botão direito na bandeja do sistema. O ícone da bandeja

do sistema exibe um símbolo verde quando a VPN está ligada e vermelho quando a VPN está desligada.

Quando está conectado, o tempo decorrido e o endereço IP designado automaticamente para si exibidos na parte inferior da interface.

Para ter acesso a mais opções, aceda à área do **Menu** ao clicar no ícone no lado superior esquerdo. Tem as seguintes opções:

- **A minha conta** - detalhes sobre a sua conta Bitdefender e a subscrição do VPN são exibidos. Clique em **Trocar conta** se deseja entrar com outra conta.
- **Definições** – dependendo das suas necessidades, pode personalizar o comportamento do seu produto:
  - receba notificações quando a VPN se conectar ou desconectar automaticamente
  - executar a aplicação VPN automaticamente no arranque do Windows
  - executar a aplicação VPN automaticamente quando o seu dispositivo se ligar a redes sem fios não seguras
- **Atualizar para o Premium** - Se estiver a utilizar a versão gratuita, pode atualizar para o plano Premium aqui.
- **Suporte** - é redirecionado para a nossa plataforma do Centro de Apoio onde poderá ler um artigo útil sobre como utilizar o Bitdefender VPN.
- **Sobre** - são apresentadas informações sobre a versão instalada.

Assinaturas

O Bitdefender VPN oferece gratuitamente 200 MB de franquia por dispositivo para proteger a sua ligação sempre que precisar, além de ligá-lo automaticamente ao melhor local de servidor.

Para obter tráfego ilimitado e acesso irrestrito a conteúdos no mundo inteiro escolhendo um local da sua preferência, atualize para a versão Premium.

Pode atualizar para a versão Bitdefender Premium VPN a qualquer momento ao clicar no botão **OBTER TRÁFEGO ILIMITADO** disponível na interface do produto.

A subscrição do Bitdefender Premium VPN é independente da subscrição do Bitdefender Total Security, ou seja, poderá usá-lo durante todo o seu período de disponibilidade, sem importar o estado de subscrição da solução

de segurança. Caso a subscrição do Bitdefender Premium VPN expire, mas Bitdefender Total Security continua ativa, voltará para o plano gratuito.

O Bitdefender VPN é um produto multiplataforma, disponível nos produtos Bitdefender compatíveis com Windows, macOS, Android e iOS. Quando atualizar para o plano Premium, poderá usar a sua subscrição em todos os seus produtos, desde que faça login com a mesma conta Bitdefender.

4.12. Segurança Safepay para transações online

O computador está a tornar-se na principal ferramenta para a realização de compras e operações bancárias. Pagar contas, transferir dinheiro, comprar praticamente qualquer coisa que possa imaginar nunca foi tão fácil e rápido.

Isto engloba enviar informação pessoal, de conta e de cartão de crédito, palavras-passe e outros tipos de informação privada pela Internet, por outras palavras exatamente o tipo de fluxo de informação que os cibercriminosos estão muito interessados em deitar a mão. Os hackers são incansáveis nos seus esforços para roubar esta informação, assim que nunca poderá ser demasiado cuidadoso em manter seguras as suas transações online.

O Bitdefender Safepay™ é, acima de tudo, um navegador protegido, um ambiente desenhado para manter a sua atividade bancária, as suas compras online e qualquer outra transação online privada e segura.

Para a melhor proteção da privacidade, o Gestor de palavras-passe do Bitdefender foi integrada ao Bitdefender Safepay™ para proteger as suas credenciais quando quiser aceder a locais online privados. Para mais informação, dirija-se a "*Proteção do Gestor de palavras-passe para as suas credenciais*" (p. 144).

O Bitdefender Safepay™ oferece as seguintes funcionalidades:

- Bloqueia o acesso ao seu ambiente de trabalho e de qualquer tentativa de tirar fotografias do seu ecran.
- Protege as suas palavras-passe secretas enquanto navega online com o Gestor de palavras-passe.
- Vem com um teclado virtual que, quando usado, torna impossível para os hackers lerem as teclas que usar.
- É completamente independente dos outros navegadores.
- Vem com uma proteção hotspot inbuída para ser usada quando o seu computador se liga a redes Wi-fi não-seguras.

- Suporta bookmarks e permite-lhe navegar entre os seus sites favoritos de bancos/compras.
- Não está só limitado ao banking e às compras online. Qualquer página Web pode ser aberta no Bitdefender Safepay™.

A utilizar o Bitdefender Safepay™

Por defeito, o Bitdefender deteta quando entra numa página de um banco ou de compras em qualquer navegador do seu computador e pergunta se gostaria de utilizar o Bitdefender Safepay™.

Para aceder à interface principal do Bitdefender Safepay™, utilize um dos métodos a seguir:

- A partir da interface do Bitdefender:
  1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
  2. Clique no botão de ação **Safepay**.
- Do Windows:
  - No **Windows 7**:
    1. Clique em **Iniciar** e vá para **Todos os Programas**.
    2. Clique em **Bitdefender**.
    3. Clique em o **Bitdefender Safepay™**.
  - No **Windows 8 e Windows 8.1**:

    Encontre o Bitdefender Safepay™ no Ecrã inicial do Windows (por exemplo, pode introduzir "Bitdefender Safepay™" diretamente no Ecrã Inicial) e, em seguida, clique no ícone.
  - No **Windows 10**:

    Introduza "Bitdefender Safepay™" na caixa de pesquisa da barra de tarefas e, em seguida, clique no ícone correspondente.

> **Nota**
> Se o plug-in do Adobe Flash Player não estiver instalado ou estiver desatualizado, será apresentada um mensagem do Bitdefender. Clique no botão correspondente para continuar.
> Após o processo de instalação, terá que reabrir o navegador Bitdefender Safepay™ manualmente para continuar com o seu trabalho.

Se estiver habituado a navegadores da Internet, não terá nenhum problema em utilizar o Bitdefender Safepay™ - ele parece e comporta-se como um navegador normal:

- insira URLs que deseja ir na barra de endereços.
- adicione separadores para visitar múltiplas páginas na janela do Bitdefender Safepay™ clicando em .
- navegue para a frente e para trás e atualize as páginas usando respetivamente.
- aceda às definições do Bitdefender Safepay™ clicando em e escolhendo **Definições**.
- proteja as suas palavras-passe com o Gestor de palavras-passe clicando em .
- pode gerir os seus bookmarks clicando em ao lado da barra de endereço.
- pode abrir o teclado virtual clicando em .
- aumente ou diminua o tamanho do navegador pressionando as teclas **Ctrl** e **+/-** simultaneamente no teclado numérico.
- veja informações sobre o seu Bitdefender clicando em e escolhendo **Sobre**.
- imprima as informações importantes clicando em .

Nota
Para alternar entre Bitdefender Safepay™ e o ambiente de trabalho Windows, pressione as teclas **Alt+Tab** ou clique no botão **Minimizar**.

Configurar definições

Clique em e escolha **Definições** para configurar o Bitdefender Safepay™:

- Nas **Definições gerais**, é possível configurar o seguinte:

  Comportamento do Bitdefender Safepay™
  Escolha o que deve de ser feito quando acede a um site online de compras ou de bancos no seu navegador habitual:
  - Abrir sites Web automaticamente no Safepay.
  - Recomendar-me a utilizar o Safepay.
  - Não me recomendar a utilização do Safepay.

Lista de domínios

Escolha como o Bitdefender Safepay™ irá comportar-se quando visitar páginas com domínios específicos no seu navegador adicionando-os à lista de domínios e selecionando o comportamento para cada um deles:

- Abrir automaticamente no Bitdefender Safepay™.
- Que o Bitdefender o avise para a ação a tomar.
- Nunca utilizar o Bitdefender Safepay™ ao visitar uma página do domínio num navegador normal.

A bloquear pop-ups

Pode escolher para bloquear pop-ups clicando no botão correspondente.

Também pode criar uma lista de páginas que possa permitir pop-ups. A lista deve conter apenas os sites web em que confia plenamente.

Para adicionar uma página à lista, introduza o seu endereço no campo correspondente e clique em **Adicionar domínio**.

Para remover uma página da web da lista, selecione o X correspondente à entrada pretendida.

- Na área **Definições Avançadas**, estão disponíveis as seguintes opções:

Gerir Plugins

Pode escolher se pretende ativar ou desativar os plug-ins específicos no Bitdefender Safepay™.

Gerir certificados

Pode importar certificados do seu sistema para uma loja de certificados.

Selecione **Importar certificados**e siga o assistente para utilizar os certificados no Bitdefender Safepay™.

Iniciar automaticamente o Teclado Virtual em campos da palavra-passe.

O teclado virtual irá aparecer automaticamente quando o campo de palavra-passe for selecionado.

Utilize o botão correspondente para ativar ou desativar a função.

Solicitar confirmação antes de imprimir

Ative esta opção se pretender dar a sua confirmação antes de iniciar o processo de impressão.

Gerir bookmarks

Se desativou a detecção automática de alguma ou de todas as páginas, ou o Bitdefendersimplesmente não detectar algumas páginas, pode adicionar bookmarks ao Bitdefender Safepay™ para que possa abrir facilmente as suas páginas favoritas no futuro.

Siga estes passos para adicionar um URL aos bookmarks do Bitdefender Safepay™

1. Clique no ícone ao lado da barra de endereços para abrir a página de Marcadores.

   Nota
   A página de Bookmarks abre por defeito quando executa o Bitdefender Safepay™.

2. Clique no botão **+** para adicionar um novo bookmark.
3. Digite o URL e o título do marcador e clique em **Criar**. Marque a opção **Abrir automaticamente no Safepay** se quiser que a página marcada abra com o Bitdefender Safepay™ todas as vezes que acedê-la. O URL é também adicionado à lista de Domínios na página de definições.

4.13. Proteção de dados

Apagar ficheiros permanentemente

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

O Destruidor de Ficheiros do Bitdefender ajuda a eliminar permanentemente dados removendo-os fisicamente do seu disco rígido.

Pode rapidamente destruir ficheiros ou pastas do seu computador usando o menu contextual Windows, seguindo os seguintes passos:

1. Clique botão direito sobre o ficheiro ou pasta que deseja apagar permanentemente.
2. Selecione **Bitdefender** > **Destruidor Ficheiros** no menu contextual que aparece.

3. Aparece uma janela de confirmação. Clique em **SIM, ELIMINAR** para iniciar o assistente de destruidora de papel. Aguarde que o Bitdefender termine a destruição dos ficheiros.
4. Os resultados são apresentados. Clique em **TERMINAR** para sair do assistente.

Alternativamente pode destruir os ficheiros a partir da interface do Bitdefender, conforme o seguinte:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **PROTEÇÃO DE DADOS**, selecione **Triturador de Ficheiros**.
4. Siga o assistente do Destruidor de Ficheiros:
   a. Clique no botão **ADICIONAR PASTAS** para adicionar os ficheiros ou pastas que pretende que sejam permanentemente removidas.

      Alternativamente, arraste estes ficheiros ou pastas para esta janela.

   b. Clique em **ELIMINAR PERMANENTEMENTE** e, de seguida, confirme que pretende continuar com o processo.

      Aguarde que o Bitdefender termine a destruição dos ficheiros.

   c. **Resumo do Resultado**

      Os resultados são apresentados. Clique em **TERMINAR** para sair do assistente.

4.14. Consultor Parental

A função de Consultor Parental permite-lhe controlar o acesso à Internet e às aplicações específicas para cada dispositivo que tenha a funcionalidade instalada. Assim que tiver configurado o Consultor Parental, poderá descobrir facilmente o que o seu filho está a fazer nos dispositivos que utiliza e onde esteve nas últimas 24 horas. Além disso, para ajudá-lo a saber melhor o que seu filho está a fazer, a aplicação apresenta estatísticas sobre as suas atividades e interesses.

Tudo o que precisa é um computador com acesso à Internet e um navegador de Internet.

Pode configurar o Consultor Parental para bloquear:

- Páginas web inapropriadas.
- aplicações tais como: jogos, programas de partilha de ficheiros e outros.
- contatos específicos que estão proibidos de entrar em contato telefónico com o seu filho.

Verifique a atividade dos seus filhos e altere as definições do Consultor Parental utilizando a conta Bitdefender a partir de qualquer computador ou dispositivo móvel ligado à Internet.

4.14.1. A aceder ao Consultor Parental - OS MEUS FILHOS

Quando aceder à secção do Consultor Parental, a janela **OS MEUS FILHOS** fica disponível. Aqui pode visualizar e editar todos os perfis que criou para os seus filhos. Os perfis aparecem como cartões de perfil, permitindo-lhe geri-los com rapidez e verificar o seu estado atual num ápice.

Assim que criar um perfil, poderá personalizar as configurações mais detalhadas para monitorizar e controlar o acesso à Internet e às aplicações específicas para os seus filhos.

Pode aceder às definições do Consultor Parental a partir da sua Bitdefender Central em qualquer computador ou dispositivo móvel ligado à Internet.

Aceda à sua conta Bitdefender:

- Em qualquer dispositivo com acesso à Internet:
  1. Aceda Bitdefender Central.
  2. Inicie sessão na sua conta Bitdefender utilizando o seu endereço de e-mail e palavra-passe.
  3. Selecione a funcionalidade **Controlo Parental**.
  4. Na janela **OS MEUS FILHOS** que aparecer, pode controlar e configurar os perfis do Consultor Parental para cada dispositivo.
- A partir do interface do Bitdefender :
  1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
  2. Clique na hiperligação **VER FUNCIONALIDADES**.
  3. No painel **CONTROLO PARENTAL**, clique em **Configurar**.

     Será redirecionado para a página Web da conta Bitdefender. Certifique-se de que tem sessão iniciada com as suas credênciais

4. Selecione a funcionalidade **Controlo Parental**.
5. Na janela **OS MEUS FILHOS** que aparecer, pode controlar e configurar os perfis do Consultor Parental para cada dispositivo.

> **Nota**
> Certifique-se que tem a sessão iniciada com a conta de administrador. Apenas os utilizadores com direitos de administrador no sistema podem aceder e configurar o Consultor Parental.

4.14.2. Adicionar o perfil do seu filho

Para começar a monitorizar as atividades dos seus filhos, precisa de configurar um perfil e instalar o Agente Consultor Parental do Bitdefender em dispositivos que ele utiliza.

Para adicionar o perfil do seu filho ao Consultor Parental:

1. Aceda ao painel do Consultor Parental a partir da Bitdefender Central.
2. Clique em **ADICIONAR PERFIL** no lado direito da janela **OS MEUS FILHOS**.
3. Preencha os campos correspondentes com as informações específicas, tais como: nome e data de nascimento. Para adicionar uma foto de perfil, clique na ligação **Escolher um ficheiro**. Clique em **SEGUINTE** para continuar.

   Com base no desenvolvimento infantil, definir a idade da criança carrega automaticamente as definições para pesquisar na Web consideradas apropriadas para a sua faixa etária.
4. Caso o dispositivo do seu filho já possua o Bitdefender Total Security instalado, selecione o dispositivo da lista disponível e selecione a conta que pretende monitorizar. Clique em **GUARDAR**.

   Se o seu filho utilizar um dispositivo Android e a aplicação Controlo Parental do Bitdefender não estiver instalada, clique em **ADICIONAR DISPOSITIVO**. Se o seu filho utilizar um dispositivo Mac e a aplicação Bitdefender Antivirus for Mac não estiver instalada, clique no mesmo botão. Selecione o sistema operativo onde pretende instalar a aplicação e clique em **PRÓXIMO PASSO** para continuar.
5. Digite o endereço de e-mail para onde devemos enviar a hiperligação de transferência de instalação da aplicação Bitdefender e clique em **ENVIAR HIPERLIGAÇÃO DE INSTALAÇÃO**.

Importante
Em dispositivos com Windows, o Bitdefender Total Security que incluir na sua subscrição tem de ser transferido e instalado.
Em dispositivos macOS, o produto Bitdefender Antivirus for Mac tem de ser transferido e instalado.
Em dispositivos Android e iOS, a aplicação Controlo Parental do Bitdefender tem de ser transferida e instalada.

Atribuir vários dispositivos ao mesmo perfil

É possível atribuir vários dispositivos ao mesmo perfil, de modo que as mesmas restrições sejam aplicadas, da seguinte forma:

1. Aceda Bitdefender Central.
2. Selecione a funcionalidade Controlo Parental.
3. Clique no ícone ⋮ no cartão de dispositivo pretendido e, em seguida, selecione **Dispositivos**.
4. Selecione a lista em cada dispositivo disponível ao qual pretende atribuir o perfil.

   Se o seu filho utilizar um dispositivo Android e a aplicação Controlo Parental do Bitdefender não estiver instalada, clique em **ADICIONAR DISPOSITIVO**. Se o seu filho utilizar um dispositivo Mac e a aplicação Bitdefender Antivirus for Mac não estiver instalada, clique no mesmo botão. Selecione o sistema operativo onde pretende instalar a aplicação e clique em **PRÓXIMO PASSO** para continuar.

   Digite o endereço de e-mail para onde devemos enviar a hiperligação de transferência de instalação da aplicação Bitdefender e clique em **ENVIAR HIPERLIGAÇÃO DE INSTALAÇÃO**.
5. Após concluir o processo de instalação no novo dispositivo, selecione-o na lista para aplicar o perfil.
6. Selecione **GUARDAR**.

Vincular o Consultor Parental a Bitdefender Central

Para monitorizar a atividade online do seu filho no Android e iOS, deve associar o dispositivo dele à sua conta Bitdefender ao iniciar sessão na conta a partir da aplicação.

Para associar um dispositivo à sua conta Bitdefender:

- Em **Android**:

  1. Selecione o botão que aparece no e-mail enviado pelo nosso servidor. Está a ser redirecionado para a Google Play Store.

     Se não escolher na sua conta Bitdefender enviar uma hiperligação de transferência para o endereço de e-mail do seu filho, aceda a Google Play e pesquise pela aplicação do Controlo Parental do Bitdefender.

  2. Toque em **INSTALAR** na janela do Controlo Parental do Bitdefender e, em seguida, toque em **ACEITAR** se lhe forem solicitadas permissões. Bitdefender necessita de permissões para o manter informado sobre a atividade do seu filho e, se não forem aceites, a aplicação não será instalada.
  3. Abra a aplicação do Consultor Parental.
  4. Leia o **Contrato de Subscrição** e, em seguida, toque em **CONTINUAR**.
  5. Inicie sessão na sua conta Bitdefender ou aceda com uma conta do Google.

     Se não tiver uma conta Bitdefender, pode optar por criar uma nova conta utilizando a opção correspondente.

  6. Toque em **ACEDER A DEFINIÇÕES** para ser redirecionado para o ecrã onde pode ativar a opção de acessibilidade da aplicação. Siga as instruções no ecrã para configurar corretamente a aplicação.
  7. Toque em **ACEDER A DEFINIÇÕES** para ser redirecionado para o ecrã onde pode ativar a opção de acessibilidade da aplicação. Siga as instruções no ecrã para configurar corretamente a aplicação.
  8. Toque em **IR PARA DEFINIÇÕES** para ser redirecionado para o ecrã onde pode ativar a opção Ativar Direitos de Administrador de Dispositivos da aplicação. Siga as instruções no ecrã para configurar corretamente a aplicação.

     Isso irá prevenir que o seu filho desinstale o Agente Consultor Parental.

  9. Toque em **CONCLUIR** para terminar o processo de instalação.

     Nota
     Em versões Android 4.4 e mais recentes, para conseguir controlar as mensagens SMS do seu filho, Bitdefender necessita que as definições da aplicação Android Messages integrada sejam alteradas.

Recomendamos que escolha **Sim** na caixa de diálogo pop-up que aparece depois de tocar em **CONCLUIR** na aplicação.

- Em **iOS**:
  1. Selecione o botão que aparece no e-mail enviado pelo nosso servidor e instale a aplicação.
  2. Abra a aplicação do Consultor Parental.
  3. É apresentado um assistente de introdução com detalhes sobre as características do produto. Toque em **Seguinte** para continuar.
  4. Inicie sessão na sua conta Bitdefender utilizando o seu endereço de e-mail e palavra-passe.
  5. Permita o acesso à localização do dispositivo para que o Bitdefender o possa localizar.
  6. Permita que a aplicação envie notificações.
  7. Atribua o dispositivo ao perfil da criança.

Monitorizar a atividade da criança

O Bitdefender ajuda a controlar o que os seus filhos fazem online.

Desta forma, pode sempre descobrir exatamente que sites Web eles visitaram, que aplicações utilizaram ou que atividades foram bloqueadas pelo Consultor Parental.

Dependendo das definições que definir, os relatórios podem conter informações detalhadas sobre cada evento, tais como:

- O estado do evento.
- A gravidade da notificação.
- O nome do dispositivo.
- A data e a hora em que ocorreu o evento.

Para monitorizar o tráfego Internet, as aplicações acedidas ou a atividade no Facebook do seu filho:

1. Aceda ao painel do Consultor Parental a partir da Bitdefender Central.
2. Selecione o cartão do dispositivo pretendido.

Na janela **Atividade** pode visualizar as informações que lhe interessam. Alternativamente, selecione a ligação **Ver a atividade de hoje** no cartão do dispositivo monitorizado para ser redirecionado para a janela de **Atividade**.

Configurar as Definições Gerais

Por defeito, quando o Consultor Parental está ativado, as atividades dos seus filhos são registadas.

Para receber notificações por e-mail:

1. Aceda ao painel do Consultor Parental a partir da Bitdefender Central.
2. Selecione o separador **Definições**no canto superior direito.
3. Ative a opção correspondente para receber relatórios de atividade.
4. Digite o endereço eletrónico para onde serão enviadas das notificações por correio eletrónico.
5. Receber notificações por e-mail para o seguinte:
   - Sites Web bloqueados
   - App bloqueadas
   - Áreas restritas
   - Chamada ou SMS recebida de um número de telefone bloqueado
   - Remoção da aplicação Consultor Parental para Facebook
6. Clique em **GUARDAR**.

Editar um perfil

Para editar um perfil existente:

1. Aceda Bitdefender Central.
2. Selecione o painel **Consultor Parental**.
3. Clique no ícone ⋮ no cartão de dispositivo pretendido e, em seguida, selecione **Editar**.
4. Após personalizar as definições pretendidas, selecione **GUARDAR**.

Remover um perfil

Para remover um perfil existente:

1. Aceda Bitdefender Central.
2. Selecione o painel **Consultor Parental**.
3. Clique no ícone ⋮ no cartão de dispositivo pretendido e, em seguida, selecione **Remover**.
4. Confirme a sua escolha.

4.14.3. Configurar perfis do Consultor Parental

Para iniciar a monitorização dos seus filhos, deverá ser designado um perfil ao dispositivo que tem o Agente Consultor Parental do Bitdefender instalado.

Após criar um perfil para o seu filho, pode personalizar definições mais detalhadas para monitorizar e controlar o acesso à Internet e às aplicações específicas.

Para iniciar a configuração de um perfil, selecione o cartão de perfil pretendido na janela **OS MEUS FILHOS**.

Clique num separador para configurar as funcionalidades do Consultor Parental correspondentes ao dispositivo:

- Atividade - exibe as atividades, interesses, locais e interações com amigos, a partir do dia atual.
- Aplicações - permite-lhe bloquear o acesso a certas aplicações, tais como jogos, software de mensagens instantâneas, filmes, etc.
- Websites - permite filtrar a navegação na Internet.
- Contactos telefónicos - aqui pode especificar que contatos da lista do seu filho têm permissão para contatá-lo por telefone.
- Localização da criança - aqui pode definir que locais são seguros ou não para o seu filho.
- Social - permite-lhe bloquear o acesso a redes sociais.
- Programação -permite-lhe bloquear o acesso aos dispositivos que especificou no perfil do seu filho.

Actividade

A janela Atividade fornece informações detalhadas sobre as atividades dos seus filhos nas últimas 24 horas, dentro e fora de casa. Para ver as atividades do dia anterior clique no ícone do calendário no canto superior esquerdo da janela.

Dependendo da atividade, esta janela pode incluir informações sobre:

- **Locais** - aqui pode visualizar os locais onde o seu filho esteve durante o dia.
- **Interesses** - aqui pode visualizar informações sobre que categorias de páginas da Internet o seu filho visitou. Clique na hiperligação **Rever conteúdo inapropriado** para permitir ou negar acesso a interesses específicos.
- **Interações Sociais** - aqui é possível visualizar os contactos com os quais o seu filho comunicou. Clique na hiperligação **Gerir contactos** para selecionar os contactos com os quais o seu filho pode comunicar ou não.
- **Aplicações** — aqui pode ver as aplicações utilizadas pelos seus filhos. Clique na hiperligação **Rever as restrições de aplicações** para bloquear ou permitir o acesso a aplicações específicas.
- **Atividade diária** - aqui pode ver o tempo passado online em todos os dispositivos atribuídos ao seu filho e o local onde esteve ativo. As informações recolhidas são do dia atual.

Aplicações

A janela Aplicações ajuda-o a bloquear a execução de aplicações. Jogos, software de multimédia e de mensagens, assim como outras categorias de software podem ser bloqueadas desta forma.

A funcionalidade pode ser ativada ou desativada utilizando o botão correspondente.

Para configurar o Controlo de Aplicações para uma determinada conta de utilizador:

1. Uma lista com cartões será exibida. Os cartões representam as aplicações que o seu filho utiliza.
2. Selecione o cartão com a aplicação que pretende que o seu filho pare de utilizar.

O símbolo de marcação que aparecerá indica que o seu filho não poderá utilizar a aplicação.

Websites

A janela de Websites ajuda-o a bloquear sites com conteúdo inapropriado. Os sites que possuem vídeos, jogos, software multimédia e de mensagens instantâneas, assim como outras categorias de conteúdo negativo, podem ser bloqueados desta forma.

A funcionalidade pode ser ativada ou desativada utilizando o botão correspondente.

Dependendo da idade que definiu para o seu filho, a lista de Interesses já vem com uma variedade de categorias ativas. Para permitir ou negar o acesso a uma categoria específica, clique na mesma.

O símbolo de marcação que aparece indica que o seu filho não será capaz de aceder aos conteúdos relacionados com uma categoria específica.

Permitir ou bloquear um site Web

Para permitir ou negar o acesso a certas páginas Web, tem de adicioná-las à lista de Exclusões, conforme se segue:

1. Clique no botão **GERIR**.
2. Escreva o endereço da página que deseja permitir ou bloquear no campo correspondente.
3. Selecione **Permitir** ou **Bloquear**.
4. Clique em **TERMINAR** para guardar as alterações.

> **Nota**
> As restrições de acesso a sites Web só podem ser definidas para dispositivos Windows, Android e macOS adicionados ao perfil do seu filho.

Contactos telefónicos

A janela Contactos telefónicos permite-lhe especificar que amigos da lista de contatos do seu filho têm permissão para contatá-lo por telefone.

Para restringir o número telefónico de um contacto, primeiro deve adicionar ao perfil do seu filho um dispositivo Android que esteja a utiliza através dos seguintes passos:

1. Selecione o painel **Consultor Parental** na Bitdefender Central.
2. Clique na ligação **Instale Parental Advisor num dispositivo** no cartão pretendido.
3. Clique em **ADICIONAR O DISPOSITIVO** na janela que aparece.
4. A opção **Parental Advisor DO Bitdefender para Android** é seleciona por predefinição. Clique em **SEGUINTE** para continuar.
5. Selecione o perfil da criança que pretenda estabelecer restrições.
6. Selecione o separador **Contactos telefónicos**.

   Uma lista com cartões será exibida. Os cartões representam os contactos do smartphone Android do seu filho.
7. Selecione o cartão com o número de telefone que pretende bloquear.

   O símbolo de marcação que aparecerá indica que o seu filho não poderá ser contatado pelo número de telefone selecionado.

Para bloquear números desconhecidos, ative o botão **Bloquear interações com números desconhecidos**.

Nota
As restrições de chamadas telefónicas só podem ser definidas para dispositivos Android adicionados ao perfil do seu filho.

Localização do seu filho

Visualizar a localização atual do dispositivo no Google Maps. A localização é atualizada a cada 5 segundos para que possa controlá-lo se estiver em movimento.

A precisão da localização depende do quanto o Bitdefender é capaz de o determinar:

- Caso o GPS esteja ativado no dispositivo, a sua localização pode ser determinada no alcance de dois metros, desde que esteja ao alcance dos satélites GPS (ou seja, fora de um edifício).
- Se o dispositivo estiver dentro de um edifício, a sua localização pode ser determinada no alcance de 10 metros caso o Wi-Fi esteja ativado e existam rede sem fios disponíveis no seu alcance.

- Caso contrário, a localização será determinada utilizando apenas as informações da rede móvel, que pode oferecer uma precisão não melhor que várias centenas de metros.

Configurar localização e check-in seguro

Para certificar-se de que o seu filho vai a certos locais, pode criar uma lista de locais seguros e não seguros. Sempre que entrar sozinho numa área predefinida, será apresentada uma notificação na aplicação Controlo Parental a pedir para confirmar que está seguro. Ao tocar em **CHEGUEI BEM** é informado através de uma notificação na sua conta Bitdefender de que o destino final foi alcançado.

No caso de o seu filho não confirmar, continua a poder ver o histórico da sua localização ao longo do dia ao consultar o seu perfil na sua conta Bitdefender.

Para configurar um local:

1. Clique em **Dispositivos** dentro da janela **Localização da criança**.
2. Clique em **ESCOLHER DISPOSITIVOS** e, em seguida, selecione o dispositivo que pretende configurar.
3. Na janela **Áreas**, clique no botão **ADICIONAR ÁREA**.
4. Escolha o tipo de local, **SEGURO** ou **RESTRITO**.
5. Digite um nome válido para a área onde o seu filho tem autorização para entrar.
6. Defina a distância que deverá ser utilizada para monitorização na barra **Raio**.
7. Clique em **ADICIONAR ÁREA** para guardar as suas definições. É-lhe perguntado se o seu filho vai viajar sozinho ou acompanhado. Confirme com Sim ou Não.

Nota
O controlador de localização pode ser utilizado para monitorizar dispositivos Android e iOS que têm a aplicação Controlo Parental do Bitdefender instalada.

Social

O Consultor Parental monitoriza a conta de Facebook do seu filho e comunica as principais atividades que estão a decorrer.

Estas atividades online são verificadas e é avisado se elas demonstram ser uma ameaça para a privacidade do seu filho.

Os elementos monitorizados da conta online incluem:

- Informações da Conta
- Gostar de páginas
- fotos carregadas

Para configurar a proteção do Facebook para uma conta específica, escreva o e-mail da conta do seu filho e, em seguida, clique em **ENVIAR**.

Informe o seu filho das suas intenções e peça-lhe para clicar no botão **PROTEGER CONTA** que ele recebeu no e-mail.

Para aceder à conta do Facebook monitorizada, clique na hiperligação **Ver no Facebook**.

Para parar de monitorizar a conta, utilize o botão **DESASSOCIAR CONTA** na parte superior.

Para ser avisado por e-mail quando o seu filho remover a aplicação Consultor Parental do seu dispositivo, selecione a caixa de verificação correspondente.

Horário

A janela Programação permite-lhe restringir o acesso aos dispositivos que especificou no perfil do seu filho. As restrições podem ser definidas a qualquer hora durante o horário escolar ou aos fins de semana para dispositivos Android e Windows.

Para começar a configurar as restrições de tempo durante a noite:

1. Na área **HORA DE DORMIR**, selecione as caixas de verificação **Noites de escola** e **Noites de fim de semana**.
2. Clique no ícone ⊗ das caixas correspondentes e, de seguida, utilize as teclas com setas para cima e para baixo para definir os intervalos de tempo durante os quais o acesso deve ser bloqueado.

Para começar a configurar as restrições de tempo durante o dia:

1. Na área de **LIMITES DIÁRIOS** tem as seguintes opções:
   - **CUMULATIVO**

a. Selecione as caixas de verificação **Limites de tempo do dia de escola** e **Limites de tempo no fim de semana**.

b. Arraste o cursor ao longo da escala para definir durante quanto tempo o acesso aos dispositivos é permitido.

- **ESPECÍFICO**

a. Selecione as caixas de verificação **Limites de tempo do dia de escola** e **Limites de tempo no fim de semana**.

b. Selecione na grelha os intervalos de tempo durante os quais o acesso deve estar bloqueado.

Nota
As definições **CUMULATIVO** e **ESPECÍFICO** são concebidas para trabalhar de forma independente a partir de cada um.

4.15. Dispositivo Anti-Roubo

O roubo de portáteis é um assunto importante que afeta igualmente indivíduos e empresas. Mais do que perder o hardware em si, é a perda de informação que pode causar danos significativos, quer financeiramente quer emocionalmente.

No entanto são poucas as pessoas que tomam as devidas precauções para proteger a sua importante informação pessoal, financeira e de negócio em caso de perda ou roubo.

O Anti-roubo do Bitdefender ajuda-o a estar mais bem preparado para tal situação ao permitir-lhe localizar ou bloquear remotamente o seu computador portátil e até mesmo destruir toda a informação dele, se alguma vez se separar do seu computador portátil contra a sua vontade.

Para usar as funcionalidades do Anti-Roubo, os seguintes pré-requisitos devem ser preenchidos:

- Os comandos só podem ser enviados da conta Bitdefender.
- O computador portátil deve estar ligado à Internet para receber os comandos.

As funcionalidades Anti-roubo funcionam da seguinte forma:

Localizar
Mostra a localização do seu dispositivo no Google Maps.

A precisão da localização depende do quanto o Bitdefender é capaz de o determinar. A localização é determinada em dezenas de metros se a ligação Wi-fi está ativada no seu computador portátil e existam redes wireless ao seu alcance.

Se o computador portátil estiver ligado a uma rede LAn por cabo sem uma localização por Wi-fi disponível, a localização será determinada baseada no endereço IP, que é consideravelmente menos precisa.

Alerta

Envie um alerta remoto no dispositivo.

Esta funcionalidade só está disponível em dispositivos móveis.

Fechar

Bloqueie o seu computador portátil e defina um PIN de 4 dígitos para o desbloquear. Quando envia o comando de **Bloqueio**, o sistema reinicia e o login no Windows só é possível após inserir o PIN que definiu.

Se pretender que o Bitdefender tire fotos da pessoa que tentar aceder ao seu computador portátil, marque a caixa de verificação correspondente. As fotos são tiradas utilizando a câmara frontal e exibidas com a data e hora no painel da função Anti-furto. Apenas serão guardadas as duas fotos mais recentes.

Esta ação está disponível apenas para computadores portáteis que têm uma câmara frontal.

Limpar

Remover todos os dados do seu sistema. Quando envia o comando de **Limpeza**, o computador portátil reinicia e toda a informação nas partições do disco rígido é apagada.

Mostrar IP

Exibe o último endereço de IP para o dispositivo selecionado. Clique em **MOSTRAR IP** para torná-lo visível.

O Anti-roubo é ativado após a instalação e só pode ser acedido exclusivamente através da sua conta Bitdefender a partir de qualquer dispositivo ligado à Internet, em qualquer lado.

Utilizar funcionalidades Anti-Roubo

Para aceder às funcionalidades Anti-furto, utilize uma das seguintes possibilidades:

- A partir da interface principal do Bitdefender:
  1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
  2. Clique no botão de ação **Anti-furto**.
  3. Na janela da Bitdefender Central que abrir, clique no cartão do dispositivo pretendido e, em seguida, selecione **Anti-furto**.
- Em qualquer dispositivo com acesso à Internet:
  1. Abra um navegador Web e vá para: https://central.bitdefender.com.
  2. Inicie sessão na sua conta Bitdefender utilizando o seu endereço de e-mail e palavra-passe.
  3. Selecione o painel **Os Meus Dispositivos**.
  4. Clique no cartão do dispositivo pretendido e, em seguida, selecione **Anti-furto**.
  5. Selecione a funcionalidade que deseja usar:

     Mostrar IP - exibe o último endereço de IP do seu dispositivo.
     Localizar - exibe a localização do seu dispositivo no Google Maps.
     Alerta - emite um alerta no dispositivo.
     Bloquear - bloqueie o seu computador portátil e defina um PIN para desbloqueá-lo.
     Limpar - eliminar todos os dados do seu computador portátil.

     Importante
     Após apagar toda a informação de um dispositivo, todas as funcionalidades Anti-Roubo deixam de funcionar.

4.16. Bitdefender USB Immunizer

A funcionalidade Autorun inbuida no sistema operativo Windows é uma ferramenta bastante útil que permite aos computadores executarem automaticamente um ficheiro de um dispositivo de media ligado a ele. Por exemplo, as instalações de software podem iniciar automaticamente quando o CD é inserido na drive de CDs.

Infelizmente, esta funcionalidade também pode ser utilizada pelas ameaças para iniciar automaticamente e infiltrar no seu computador a partir de dispositivos multimédia graváveis, tais como unidades USB flash e cartões

de memória ligados através de leitores de cartões. Numerosos ataques Autorun foram criados nestes últimos anos.

Com o Imunizador USB pode evitar que qualquer unidade flash formatada em NTFS, FAT32 ou FAT jamais possa automaticamente executar ameaças. Uma vez que um dispositivo USB esteja imunizado, as ameaças já não o podem configurar para executar determinada aplicação quando o dispositivo esteja ligado ao computador em Windows.

Para imunizar um dispositivo USB:

1. Ligue a drive flash ao seu computador.
2. Explore o seu computador para localizar o dispositivo de armazenagem amovível e clique com o botão direito do rato sobre ele.
3. No menu contextual, aponte para o **Bitdefender** e selecione **Imunizar esta drive**.

> **Nota**
> Se a unidade já tiver sido imunizada, a mensagem **O dispositivo USB está protegido contra ameaças no autorun** aparecerá em vez da opção Imunizar.

Para evitar que o computador executar ameaças de dispositivos USB não imunizados, desative a função de autorun de suporte multimédia. Para mais informação, dirija-se a "*Usar monitorização de vulnerabilidade automática*" (p. 127).

5. OTIMIZAÇÃO DO SISTEMA

5.1. Ferramentas

O Bitdefender vem com uma secção de ferramentas que irá ajudá-lo a manter a integridade do seu sistema. As ferramentas de manutenção oferecidas são criticas para o melhoramento do desempenho do seu sistema e para uma gestão eficiente do espaço do seu disco duro.

O Bitdefender fornece as seguintes ferramentas de otimização do PC:

- O OneClick Optimizer analisa e melhora a velocidade do seu sistema ao executar diversas tarefas com um único clique de um botão.
- O Startup Optimizer reduz o tempo de arranque do seu sistema ao impedir que aplicações desnecessárias sejam carregadas quando o PC arranca.
- Limpeza de Disco identifica os ficheiros que podem ser os principais responsáveis pelo seu pouco espaço em disco e oferece a possibilidade de guardá-los ou não.

5.1.1. A otimizar a velocidade do seu sistema com apenas um clique

Problemas como falhas no disco rígido, restos de ficheiros de registo e o histórico do navegador, podem comprometer o desempenho do seu computador, e isso pode tornar-se irritante para si. Tudo isto pode ser corrigido com um único clique de um botão.

O Otimizador de Um Clique permite-lhe identificar e remover ficheiros inúteis ao executar uma série de tarefas de limpeza ao mesmo tempo.

Para iniciar o processo do OneClick Optimizer:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique no botão de ação **OneClick Optimizer**.
   a. **A analisar**

      Aguarde que o Bitdefender termine de procurar por problemas no sistema.

      - Limpeza de Disco — identifica os ficheiros e pastas desnecessários.

- Limpeza do Registo - identifica referências inválidas ou obsoletas no Registo do Windows.
- Limpeza de Privacidade - identifica ficheiros temporários da Internet, cookies, cache e histórico do navegador.

O número de problemas encontrados foi exibido. Clique na hiperligação **Ver detalhes** para revê-los antes de prosseguir com o processo de limpeza. Clique em **OPTIMIZE** para continuar.

b. **A otimizar**

Aguarde que o Bitdefender conclua a otimização do seu sistema.

c. **Questões**

Aqui pode ver o resultado da operação.

Se desejar informações completas sobre o processo de otimização, clique no botão **VISUALIZAR RELATÓRIO DETALHADO**.

5.1.2. A otimizar o tempo de arranque do seu PC.

O arranque prolongado do sistema é um problema real devido às aplicações que estão definidas para executar sem necessidade. Aguardar vários minutos para que um sistema arranque pode custar-lhe tempo precioso e produtividade.

A janela do Otimizador de Arranque apresenta quais aplicações estão a ser executadas durante o arranque do sistema e permite a gestão do seu comportamento nesta etapa.

Para iniciar o processo do Startup Optimizer:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique no botão de ação **Startup Optimizer**.

a. **Selecione as aplicações**

Pode ver uma lista de aplicações que estão a executar no arranque do sistema. Selecione aquelas que quer desativar ou adiar durante o arranque.

b. **Escolha da comunidade**

Veja o que os outros utilizadores da Bitdefender decidiram fazer com a aplicação que selecionou.

c. **Tempo de arranque do sistema**

Verifique a barra de deslocamento na parte superior da janela para ver o tempo necessário tanto para o sistema como para as aplicações selecionadas para serem executadas durante o arranque.

A reinicialização do sistema é necessária para ser capaz de obter as informações sobre o tempo de arranque do sistema e das aplicações.

d. **Estado do arranque**

- **Permitir.** Selecione esta opção quando quiser uma aplicação que execute no arranque do sistema. Esta opção é ativada por defeito.
- **Atraso.** Selecione esta opção para adiar a execução de um programa no arranque do sistema. Isto significa que as aplicações selecionadas irão arrancar com um atraso de cinco minutos após o utilizador iniciar sessão no sistema. A funcionalidade do **Atraso** é pré-definida e não pode ser configurada pelo utilizador.
- **Desativar.** Selecione esta opção para desativar a execução de um programa no arranque do sistema.

e. **Resultados**

As informações, como o tempo estimado para o arranque do sistema após adiar ou desativar programas, são apresentadas.

Pode ser necessária a reinicialização do sistema para ver todas as informações.

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

Nota
Caso a sua subscrição expire ou decida desinstalar o Bitdefender, os programas que configurou para não serem executados no arranque serão restaurados para as suas predefinições de arranque.

5.1.3. A otimizar o seu disco

Ficheiros e pastas desnecessários que ocupam espaço no seu disco podem tornar o seu sistema lento. Portanto, é recomendado que melhore a velocidade do seu sistema limpando-o regularmente.

A Limpeza de Disco do Bitdefender ajuda a otimizar o seu espaço em disco facilmente identificando os ficheiros que poderiam ser os principais

responsáveis pelo seu pouco espaço em disco. Ainda terá a possibilidade de decidir o que quer fazer com os ficheiros identificados.

Para começar a limpar o seu sistema:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique no botão de ação **Limpeza de Disco**.
3. A primeira vez que aceder à Limpeza de Disco, verá uma apresentação da função. Clique em **OK, ENTENDI** para continuar.
   a. **Unidades de disco e dispositivos**

      Pode consultar uma lista dos discos disponíveis. Além dos discos do Windows, discos rígidos externos e dispositivos USB são verificados e exibidos na lista. Clique em **ANALISAR DISCO** na área do disco que deseja limpar.

   b. **A analisar disco**

      O drive selecionado é analisado. Aguarde que o Bitdefender termine de procurar por ficheiros e pastas grandes.

   c. **Questões**

      Aqui pode ver os resultados da operação. Para selecionar em que ordem os resultados devem ser apresentados, utilize a seta para baixo **ORDENAR POR** que se encontra na parte esquerda da janela. Pode filtrar os resultados por tamanho (desde 10 MB até mais de 5 GB) ou por tipo (os ficheiros são ordenados em pastas separadas pelas suas extensões).

      Selecione os ficheiros que pretende apagar e clique em **CONFIRMAR SELEÇÃO** para iniciar o processo.

      Os ficheiros protegidos ou importantes responsáveis pela operação do seu sistema também são identificados, mas não podem ser selecionados ou eliminados.

      Clique no ícone para ter acesso às pastas pertencentes aos ficheiros selecionados.

   d. **Confirme a sua seleção**

      É apresentada a lista dos ficheiros selecionados. Dê uma olhada e verifique se realmente não precisa mais destes ficheiros, já que mais

adiante, não poderão ser recuperados do lixo. Confirme a sua escolha ao clicar em **ELIMINAR**.

e. **Resumo do Resultado**

O estado do processo é apresentado da seguinte forma:

Todos os ficheiros selecionados foram eliminados.
Não foi possível eliminar um ou mais dos ficheiros selecionados **ou** não foi possível eliminar nenhum dos ficheiros selecionados.

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

5.2. Perfis

Atividades de trabalho diárias, ver filmes ou jogar podem provocar lentidão no sistema, especialmente se estes estiverem a ser executados simultaneamente com os processos de atualização do Windows e as tarefas de manutenção. Com o Bitdefender, pode agora escolher e aplicar o seu perfil preferido; o que irá ajustar o sistema a melhorar o desempenho de aplicações específicas.

O Bitdefender fornece os seguintes perfis:

- Perfil Trabalho
- Perfil de Filme
- Perfil de Jogo
- Perfil Wi-Fi Público
- Perfil do Modo de Bateria

Caso decida não utilizar os **Perfis**, um perfil predefinido chamado **Padrão** será ativado e não fará qualquer otimização no seu sistema.

De acordo com a sua atividade, as seguintes definições do produto serão aplicadas quando os perfis Trabalho, Filme ou Jogo são ativados:

- Todos os alertas e pop-ups do Bitdefender são desativados.
- A Atualização Automática é adiada.
- As análises agendadas são adiadas.
- O módulo Antispam está ativado.
- O Consultor de Pesquisa é desativado.

- As notificações de ofertas especiais estão desativadas.

De acordo com sua atividade, as seguintes definições do sistema são aplicadas quando os perfis Trabalho, Filme ou Jogo são ativados:

- As Atualizações Automáticas do Windows são adiadas.
- Os alertas e pop-ups do Windows são desativados.
- Os programas desnecessários em segundo plano são suspensos.
- Os efeitos visuais são ajustados para o melhor desempenho.
- As tarefas de manutenção são adiadas.
- As definições do plano de energia são ajustadas.

Ao executar neste perfil Wi-Fi público, o Bitdefender Total Security é definido automaticamente de modo a obter as seguintes definições de programa:

- Advanced Threat Defense ativado
- A Firewall do Bitdefender é ativada e as definições seguintes são aplicadas ao seu adaptador sem fios:
  - Modo Stealth - : LIGADO
  - Tipo de rede- Pública
- As seguintes definições da Proteção na Web estão desativadas:
  - Analisar SSL
  - Proteção contra fraudes
  - Proteção contra phishing

5.2.1. Perfil Trabalho

A execução de várias tarefas no trabalho, tais como o envio de e-mails, ter uma videoconferência com os seus colegas distantes ou trabalhar com aplicações de design pode afetar o desempenho do sistema. O Perfil de Trabalho foi desenhado para ajudá-lo a melhorar a sua eficiência no trabalho, desativando alguns dos serviços e tarefas de manutenção em segundo plano.

A configurar o Perfil de Trabalho

Para configurar as ações a executar enquanto está no Perfil de Trabalho:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Selecione o separador **PERFIS**.
3. Clique no botão **CONFIGURAR** na área do Perfil de Trabalho.
4. Escolha os ajustes do sistema que quer que sejam aplicados selecionando as seguintes opções:
   - Aumente o desempenho das aplicações de trabalho
   - Otimize as definições do produto para o perfil Trabalho
   - Adie programas em segundo plano e tarefas de manutenção
   - Adiar as Atualizações Automáticas do Windows
5. Clique em **Guardar** para guardar as alterações e fechar a janela.

A adicionar aplicações manualmente à lista do Perfil de Trabalho

Se o Bitdefender não entrar automaticamente no Perfil de Trabalho quando abre uma determinada aplicação de trabalho, pode adicionar a aplicação manualmente à **Lista de Aplicações**.

Para adicionar aplicações manualmente à Lista de aplicações do Perfil de Trabalho:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Selecione o separador **PERFIS**.
3. Clique no botão **CONFIGURAR** na área do Perfil de Trabalho.
4. Na janela **PERFIL DE TRABALHO**, clique na ligação **Lista de aplicações**.
5. Clique em **Adicionar** para adicionar uma nova aplicação à **Lista de aplicações**.

   Aparece uma nova janela. Vá até ao ficheiro executável da aplicação, selecione-o e clique em **OK** para o adicionar à lista.

5.2.2. Perfil de Filme

A exibição de conteúdo de vídeo de alta qualidade, como filmes de alta definição, exige recursos significativos do sistema. O Perfil de Filme ajusta as definições do sistema e do produto para que possa desfrutar de uma experiência cinematográfica agradável e sem interrupções.

A configurar o Perfil de Filme

Para configurar as ações a serem tomadas no Perfil de Filme:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Selecione o separador **PERFIS**.
3. Clique no botão **CONFIGURAR** na área do Perfil de Filme.
4. Escolha os ajustes do sistema que quer que sejam aplicados selecionando as seguintes opções:
   - Aumente o desempenho dos leitores de vídeo
   - Otimize as definições do produto para o perfil Filme
   - Adie programas em segundo plano e tarefas de manutenção
   - Adiar as Atualizações Automáticas do Windows
   - Ajustar as definições do esquema de energia para filmes
5. Clique em **Guardar** para guardar as alterações e fechar a janela.

A adicionar manualmente leitores de vídeo à lista do Perfil de Filme

Se o Bitdefender não entrar automaticamente no Perfil de Filme ao iniciar uma determinada aplicação de reprodução de vídeo, pode adicionar manualmente a aplicação à **Lista de leitores**.

Para adicionar manualmente leitores de vídeo à Lista de leitores no Perfil de Filme:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Selecione o separador **PERFIS**.
3. Clique no botão **CONFIGURAR** na área do Perfil de Filme.
4. Na janela **PERFIL DE FILME**, clique na ligação **Lista de leitores**.
5. Clique em **Adicionar** para adicionar uma nova aplicação à **Lista de leitores**.

   Aparece uma nova janela. Vá até ao ficheiro executável da aplicação, selecione-o e clique em **OK** para o adicionar à lista.

5.2.3. Perfil de Jogo

Para desfrutar de uma experiência de jogo sem interrupções, é importante reduzir a carga do sistema e diminuir a lentidão. Ao utilizar heurísticas comportamentais, juntamente com uma lista de jogos conhecidos, o Bitdefender pode detectar automaticamente os jogos em execução e otimizar os recursos do sistema para que possa aproveitar a sua pausa de jogo.

A configurar o Perfil de Jogo

Para configurar as ações a serem tomadas no Perfil de Jogos:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Selecione o separador **PERFIS**.
3. Clique no botão **CONFIGURAR** na área do Perfil de Jogos.
4. Escolha os ajustes do sistema que quer que sejam aplicados selecionando as seguintes opções:
   - Aumente o desempenho dos jogos
   - Otimize as definições do produto para o perfil Jogo
   - Adie programas em segundo plano e tarefas de manutenção
   - Adiar as Atualizações Automáticas do Windows
   - Ajustar as definições do esquema de energia para jogos
5. Clique em **Guardar** para guardar as alterações e fechar a janela.

Adicionar os jogos manualmente à lista de Jogos

Se o Bitdefender não entrar automaticamente no Perfil de Jogo ao iniciar um determinado jogo ou aplicação, pode adicionar a aplicação manualmente à **Lista de jogos**.

Para adicionar jogos manualmente à Lista de jogos no Perfil de Jogo:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Selecione o separador **PERFIS**.
3. Clique no botão **CONFIGURAR** na área do Perfil de Jogos.
4. Na janela **PERFIL DE JOGOS**, clique na ligação **Lista de jogos**.

5. Clique em **Adicionar** para adicionar um novo jogo à **Lista de jogos**.

   Aparece uma nova janela. Navegue até o ficheiro executável do jogo, selecione-o e clique em **OK** para adicioná-lo à lista.

5.2.4. Perfil Wi-Fi Público

Enviar e-mails, digitar credenciais sensíveis ou fazer compras online enquanto ligado a uma rede sem fios insegura pode colocar os seus dados pessoais em risco. O perfil Wi-Fi Público ajusta as definições do produto para lhe dar a possibilidade de fazer pagamentos online e utilizar informações sensíveis num ambiente protegido.

A configurar o perfil Wi-Fi Público

Para configurar o Bitdefender para aplicar as definições do produto enquanto ligado a uma rede sem fios insegura:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Selecione o separador **PERFIS**.
3. Clique no botão **CONFIGURAR** na área do Perfil Wi-Fi Público.
4. Deixe a caixa de verificação **Ajusta as definições do produto para aumentar a proteção quando ligado a uma rede Wi-Fi pública insegura** marcada.
5. Clique em **Guardar**.

5.2.5. Perfil do Modo de Bateria

O perfil Modo de Bateria foi concebido especialmente para utilizadores de portáteis e tablets. O seu objetivo é minimizar o impacto do sistema e do Bitdefender no consumo de energia quando o nível de bateria estiver abaixo do nível predefinido que selecionou.

Configurando o perfil Modo de Bateria

Para configurar o perfil Modo de Bateria:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Selecione o separador **PERFIS**.
3. Clique no botão **CONFIGURAR** na área do Perfil Modo de bateria.

4. Escolha os ajustes do sistema que serão aplicados selecionando as seguintes opções:
   - Otimize as definições do produto para o modo Bateria.
   - Adie programas em segundo plano e tarefas de manutenção.
   - Adiar as Atualizações Automáticas do Windows.
   - Ajuste as definições do plano de energia para o modo Bateria.
   - Desative os dispositivos externos e as portas de rede.
5. Clique em **Guardar** para guardar as alterações e fechar a janela.

Digite um valor válido na caixa de rotação ou selecione um valor utilizando os botões de setas para cima e para baixo para especificar quando o sistema deve começar a operar no Modo de Bateria. Por defeito, o modo é ativado quando o nível da bateria cai abaixo dos 30%.

As definições do produto seguinte são aplicadas quando o Bitdefender opera em Modo de Bateria:

- A Atualização Automática do Bitdefender é adiada.
- As análises agendadas são adiadas.
- A Miniaplicação de Segurança é desligada.

O Bitdefender detecta quando o seu portátil está a funcionar na bateria e dependendo do nível de carga, entra automaticamente em Modo de Bateria. Da mesma forma, o Bitdefender sai automaticamente do Modo de Bateria ao detectar que o portátil já não está a funcionar pela bateria.

5.2.6. Otimização em tempo real

A Otimização em Tempo Real do Bitdefender é um plugin que melhora o desempenho do seu sistema de forma silenciosa, em segundo plano, garantindo que não seja interrompido enquanto está num modo de perfil. Dependendo da carga do CPU, o plug-in monitoriza todos os processos, focando naqueles que utilizam uma carga maior, para ajustá-los às suas necessidades.

Para ativar ou desativar a Otimização em Tempo Real:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Selecione o separador **PERFIS**.

3. Desloque-se para baixo até ver a opção de otimização em tempo real e utilize o botão correspondente para a ativar ou desativar.

6. SOLUÇÃO DE PROBLEMAS

6.1. Resolver incidências comuns

Este capítulo apresenta alguns dos problemas que poderá encontrar ao utilizar o Bitdefender e as possíveis soluções. A maioria destes problemas pode ser resolvida com a configuração correta das definições do produto.

- "*O meu sistema parece estar lento*" (p. 188)
- "*A análise não inicia*" (p. 190)
- "*Já não posso utilizar uma aplicação*" (p. 192)
- "*O que fazer quando o Bitdefender bloqueia um site Web ou uma aplicação online segura*" (p. 193)
- "*O que fazer se o Bitdefender detetar uma aplicação segura como ransomware*" (p. 194)
- "*Como atualizar o Bitdefender numa ligação à Internet lenta*" (p. 198)
- "*Os serviços Bitdefender não estão a responder*" (p. 199)
- "*O filtro Antispam não está a funcionar corretamente*" (p. 200)
- "*A funcionalidade Preenchimento automático na minha Carteira não funciona*" (p. 204)
- "*Remoção de Bitdefender falhou*" (p. 205)
- "*O meu sistema não reinicia após a instalação de Bitdefender*" (p. 207)

Se não conseguir encontrar o seu problema aqui, ou se as soluções apresentadas não resolvem o seu problema, pode contactar os representantes do apoio técnico da Bitdefender como mostrado no capítulo "*Pedir Ajuda*" (p. 325).

6.1.1. O meu sistema parece estar lento

Normalmente, após a instalação de um software de segurança, o sistema poderá abrandar ligeiramente, o que é, até um certo nível, normal.

Se notar um abrandamento significativo, este problema pode dever-se às seguintes razões:

- **O Bitdefender não é o único programa de segurança instalada no sistema.**

Apesar de o Bitdefender procurar e remover os programas de segurança encontrados durante a instalação, é recomendado que remova todas as outras soluções de segurança utilizadas antes de instalar o Bitdefender. Para mais informação, dirija-se a "*Como posso remover outras soluções de segurança?*" (p. 82).

- **Não estão cumpridos os Requisitos Mínimos do Sistema para executar o Bitdefender.**

  Se o seu computador não cumprir os Requisitos Mínimos do Sistema, ficará lento, especialmente se estiver a executar muitas aplicações ao mesmo tempo. Para mais informação, dirija-se a "Requisitos mínimos do sistema" (p. 3).

- **Instalou aplicações que não utiliza**.

  Qualquer computador tem programas ou aplicações que não utiliza. E quaisquer programas indesejados são executados em segundo plano, ocupando espaço no disco rígido e na memória. Caso não utilize um programa, desinstale-o. Também se aplica a qualquer outro software pré-instalado ou aplicação de teste que se esqueceu de remover.

  > **Importante**
  > Caso suspeite que um programa ou aplicação seja parte essencial de seu sistema operativo, não remova o mesmo e entre em contacto com a Assistência ao Cliente do Bitdefender para obter assistência.

- **O seu sistema pode estar infetado**.

  A velocidade do seu sistema e o seu comportamento geral também podem ser afetados pelas ameaças. Spyware, malware, Trojans e adware prejudicam o desempenho do seu computador. Certifique-se de que analisa o seu sistema periodicamente, pelo menos uma vez por semana. Recomendamos a utilização da Análise do Sistema do Bitdefender pois a mesma analisa todos os tipos de ameaças que prejudicam a segurança do seu sistema.

  Para iniciar a Verificação do Sistema:

  1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
  2. Clique na hiperligação **VER FUNCIONALIDADES**.
  3. No painel **ANTIVÍRUS**, clique em **Análise do sistema**.

4. Siga os passos do assistente.

6.1.2. A análise não inicia

Este tipo de problema pode ter duas causas principais:

- **Uma instalação anterior do Bitdefender que não foi totalmente removida ou uma instalação do Bitdefender mal sucedida**.

  Neste caso, reinstale o Bitdefender:

  - No **Windows 7**:
    1. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
    2. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
    3. Clique em **REINSTALAR** na janela que aparece.
    4. Aguarde pela conclusão do processo de reinstalação e reinicie o sistema.
  - No **Windows 8 e Windows 8.1**:
    1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
    2. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
    3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
    4. Clique em **REINSTALAR** na janela que aparece.
    5. Aguarde pela conclusão do processo de reinstalação e reinicie o sistema.
  - No **Windows 10**:
    1. Clique em **Iniciar**, em seguida, clique em Definições.
    2. Clique no ícone **Sistema** na área das Definições, em seguida, selecione **Aplicações instaladas**.
    3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
    4. Clique em **Desinstalar** novamente para confirmar a sua escolha.
    5. Clique em **REINSTALAR** na janela que aparece.

6. Aguarde pela conclusão do processo de reinstalação e reinicie o sistema.

> **Nota**
> Ao seguir este procedimento de reinstalação, as definições personalizadas são guardadas e estão disponíveis no novo produto instalado. As outras definições podem ser alteradas novamente para a configuração predefinida.

- **O Bitdefender não é a única solução de segurança instalada no seu sistema**.

  Neste caso:

  1. Remover a outra solução de segurança. Para mais informação, dirija-se a "*Como posso remover outras soluções de segurança?*" (p. 82).
  2. Reinstalar Bitdefender:
     - No **Windows 7**:
       a. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
       b. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
       c. Clique em **REINSTALAR** na janela que aparece.
       d. Aguarde pela conclusão do processo de reinstalação e reinicie o sistema.
     - No **Windows 8 e Windows 8.1**:
       a. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
       b. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
       c. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
       d. Clique em **REINSTALAR** na janela que aparece.
       e. Aguarde pela conclusão do processo de reinstalação e reinicie o sistema.
     - No **Windows 10**:
       a. Clique em **Iniciar**, em seguida, clique em Definições.

b. Clique no ícone **Sistema** na área das Definições, em seguida, selecione **Aplicações instaladas**.

c. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.

d. Clique em **Desinstalar** novamente para confirmar a sua escolha.

e. Clique em **REINSTALAR** na janela que aparece.

f. Aguarde pela conclusão do processo de reinstalação e reinicie o sistema.

Nota
Ao seguir este procedimento de reinstalação, as definições personalizadas são guardadas e estão disponíveis no novo produto instalado. As outras definições podem ser alteradas novamente para a configuração predefinida.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 325).

6.1.3. Já não posso utilizar uma aplicação

Este problema ocorre quando está a tentar utilizar um programa que estava a funcionar normalmente antes de instalar o Bitdefender.

Após instalar o Bitdefender pode deparar-se com uma das seguintes situações:

- Poderá receber uma mensagem do Bitdefender a informar que o programa está a tentar modificar o sistema.
- Pode receber uma mensagem de erro do programa que está a tentar utilizar.

Este tipo de situação ocorre quando o Advanced Threat Defense deteta erradamente algumas aplicações como maliciosas.

Advanced Threat Defense é uma funcionalidade do Bitdefender que monitoriza constantemente as aplicações executadas no seu sistema e comunica o comportamento potencialmente malicioso. Como esta funcionalidade se baseia num sistema heurístico, pode haver casos em que as aplicações legítimas são comunicadas pelo Advanced Threat Defense.

Quando esta situação ocorre, pode excluir a respetiva aplicação da monitorização do Advanced Threat Defense.

Para adicionar o programa à lista de exclusões:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone no canto inferior direito do painel **ADVANCED THREAT DEFENSE**.
4. Na janela **LISTA DE PERMISSÕES**, clique em **Adicionar aplicações à lista de permissões**.
5. Encontre e selecione a aplicação que pretende excluir e, em seguida, clique em **OK**.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 325).

6.1.4. O que fazer quando o Bitdefender bloqueia um site Web ou uma aplicação online segura

O Bitdefender oferece uma experiência de navegação Web segura filtrando todo o tráfego da rede e bloqueando os conteúdos maliciosos. No entanto, é possível que o Bitdefender considere um site Web ou uma aplicação online segura como insegura, o que fará com que a análise do tráfego de HTTP do Bitdefender bloqueie-os incorretamente.

Se a mesma página ou aplicação for bloqueada repetidamente, estes podem ser adicionados a uma lista branca para que não sejam analisados pelos mecanismos do Bitdefender, o qeu assegura uma experiência de navegação Web normal.

Para adicionar uma página web à **Lista branca**:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **PROTEÇÃO NA WEB**, clique em **Lista branca**.
4. Forneça o endereço do site Web ou da aplicação online bloqueada no campo correspondente e clique em **Adicionar**.
5. Clique em **Guardar** para guardar as alterações e fechar a janela.

Apenas os sites Web e as aplicações em que confia totalmente devem ser adicionados a esta lista. Estes irão ser excluídos da análise pelos seguintes mecanismos: ameaças, phishing e fraude.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 325).

6.1.5. O que fazer se o Bitdefender detetar uma aplicação segura como ransomware

Ransomware é um programa malicioso que tenta lucrar com os utilizadores através do bloqueio dos seus sistemas vulneráveis. Para manter o sistema protegido de situações desagradáveis, o Bitdefender fornece a possibilidade de recuperar ficheiros pessoais.

Quando uma aplicação tenta alterar ou eliminar um dos seus ficheiros protegidos, será considerado como desprotegido e o Bitdefender irá bloquear esta funcionalidade.

Caso uma aplicação seja adicionada à lista de aplicações não fidedignas e se tiver certeza de que é seguro utilizá-la, siga estes passos:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **SAFE FILES**, clique em **Acesso a aplicações**.
4. As aplicações que pediram para alterar ficheiros nas suas pastas protegidas são listadas. Clique no botão Permitir junto da aplicação que tem a certeza que é segura.

6.1.6. Não consigo ligar-me à Internet

Poderá verificar que um programa ou navegador da web já não consegue ligar à Internet ou aceder aos serviços em rede após a instalação do Bitdefender.

Neste caso, a melhor solução é configurar o Bitdefender para permitir automaticamente as ligações de e para a respetiva aplicação de software:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.

3. Clique no ícone ⚙ no canto inferior direito do painel **FIREWALL**.
4. Selecione o separador **REGRAS**.
5. Para adicionar uma regra de aplicação, clique na hiperligação **Adicionar regra**.
6. Uma nova janela aparece onde possa adicionar os detalhes. Certifique-se de que seleciona todos os tipos de rede disponíveis e na seção **Permissão** seleciona **Permitir**.

Feche o Bitdefender, abra a aplicação de software e tente de novo ligar-se à Internet.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 325).

6.1.7. Não consigo aceder a um dispositivo na minha rede

Dependendo da rede a que está ligado, a firewall do Bitdefender poderá bloquear a ligação entre o seu sistema e outro dispositivo (como outro computador ou uma impressora). Como resultado, já não poderá partilhar ou imprimir ficheiros.

Neste caso, a melhor solução é configurar o Bitdefender para permitir automaticamente as ligações de e para o respetivo dispositivo como se segue:

1. Clique no ícone Ⓑ na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. Clique no ícone ⚙ no canto inferior direito do painel **FIREWALL**.
4. Clique na hiperligação **Adicionar regra** na parte superior da janela **REGRAS**.
5. Na janela **DEFINIÇÕES**, ative a opção **Aplicar esta regra a todas as aplicações**.
6. Clique no separador **AVANÇADO**.
7. Na caixa **Personalizar endereço remoto**, digite o endereço IP do computador ou impressora ao qual pretende ter acesso ilimitado.

Se ainda não conegue ligar-se ao dispositivo, a incidência poderá não ser causada pelo Bitdefender.

Procure por outras potenciais causas, tais como as seguintes:

- A firewall no outro computador poderá bloquear a partilha de ficheiros e impressoras com o seu computador.
  - Se a Firewall do Windows estiver a utilizada, pode ser configurada para permitir a partilha de ficheiros e impressora da seguinte forma:
    - No **Windows 7**:
      1. Clique em **Iniciar**, aceda ao **Painel de Controlo** e selecione **Sistema e Segurança**.
      2. Aceda a **Firewall do Windows** e, em seguida, clique em **Permitir um programa através da Firewall do Windows**.
      3. Selecione a caixa de verificação **Partilha de ficheiros e impressoras**.
    - No **Windows 8 e Windows 8.1**:
      1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
      2. Clique em **Sistema e Segurança**, aceda a **Firewall do Windows** e selecione **Deixar uma aplicação passar pela Firewall do Windows**.
      3. Selecione a caixa de verificação **Partilha de ficheiros e impressoras** e, em seguida, clique em **OK**.
    - No **Windows 10**:
      1. Introduza "Permitir uma aplicação através do Firewall do Windows" na caixa de pesquisa da barra de tarefas e clique no ícone correspondente.
      2. Clique em **Alterar definições**.
      3. Na lista **Aplicações e recursos permitidos**, selecione a caixa de verificação **Partilha de Ficheiros e Impressoras** e, em seguida, clique em **OK**.
  - Se outro programa de firewall estiver a ser utilizado, por favor consulte a documentação e ficheiro de ajuda.
- Condições gerais que podem impedir a utilização ou conexão com a impressora compartilhada:
  - Poderá precisar de se ligar com uma conta de administrador do Windows para aceder à impressora compartilhada.

- As permissões são definidas para a impressora compartilhada para permitir acesso a um computador específico e apenas utilizadores. Se está a compartilhar a sua impressora, verifique as permissões definidas para a impressora para saber se o utilizador do outro computador está autorizado a aceder à impressora. Se está a tentar ligar-se a uma impressora compartilhada, verifique com o utilizador do outro computador se tem permissão para se conectar com a impressora.
- A impressora ligada ao seu computador ou ao outro computador não está a ser compartilhada.
- A impressora compartilhada não está adicionada ao computador.

> **Nota**
> Para aprender como gerir o compartilhamento de impressoras (compartilhar uma impressora, definir ou remover permissões para a impressora, conecta-se a uma rede de impressora ou a uma impressora partilhada), vá à Ajuda e Suporte do Windows (no menu Iniciar, clique em **Ajuda e Suporte**).

- O acesso a uma impressora em rede pode ser restringido a computadores ou apenas a utilizadores. Deverá verificar com o administrador da rede se tem ou não permissão para aceder à impressora.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 325).

6.1.8. A minha Internet está lenta

Esta situação poderá surgir depois de instalar o Bitdefender. Este problema poderá ser causado por erros na configuração da firewall do Bitdefender.

Para resolver esta situação:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **FIREWALL**, clique no botão ON/OFF para desativar a funcionalidade.
4. Verifique se a sua ligação à Internet melhorou com a firewall do Bitdefender desativada.

- Se ainda tem uma ligação à Internet lenta, a incidência poderá não ser causada pelo Bitdefender. Deve contactar o seu Fornecedor de Serviço de Internet para confirmar se a ligação está operacional.

  Se receber a confirmação do seu Fornecedor de Serviços de Internet que a ligação está operacional e o problema persistir, contacte a Bitdefender como indicado na secção "*Pedir Ajuda*" (p. 325).

- Se a ligação à Internet melhorou depois de desativar a firewall do Bitdefender:

  a. Clique no ícone na barra lateral esquerda da interface do Bitdefender.

  b. Clique na hiperligação **VER FUNCIONALIDADES**.

  c. Clique no ícone no canto inferior direito do painel **FIREWALL**.

  d. Aceda ao separador **ADAPTADORES DE REDE** e defina a sua ligação Internet como **Doméstica/escritório**.

  e. No separador **DEFINIÇÕES AVANÇADAS**, clique no botão para desativar **Bloquear verificações da porta na rede**.

  Na área **Modo furtivo**, clique em **Editar ligações furtivas**. Ative o modo furtivo para o adaptador de rede ao qual está ligado.

  f. Feche o Bitdefender, reinicie o sistema e verifique a velocidade de ligação à Internet.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 325).

6.1.9. Como atualizar o Bitdefender numa ligação à Internet lenta

Se tiver uma ligação à Internet lenta (por exemplo, ligação telefónica), poderão ocorrer erros durante o processo de atualização.

Para manter o seu sistema atualizado com a base de dados de informações de ameaças mais recente do Bitdefender:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Selecione o separador **ATUALIZAR**.

3. Ao lado do **Atualizar as regras de processamento**, selecione **Exibir antes de transferir** do menu suspenso.
4. Volte à janela principal e clique em **ATUALIZAR AGORA**.
5. Selecione apenas **Atualizações de assinaturas** e depois clique em **OK**.
6. O Bitdefender transfere e instala apenas a base de dados de informações de ameaças.

6.1.10. Os serviços Bitdefender não estão a responder

Este artigo ajuda-o a troubleshoot os erros de**Os Serviços Bitdefender não estão a responder**. Pode encontrar esse erro da seguinte forma:

- O ícone Bitdefender na Barra de Notificação está a cinzento e é informado que os serviços do Bitdefender não estão a responder.
- A janela do Bitdefender indica que os serviços do Bitdefender não estão a responder.

O erro pode ter ocorrido devido a um dos seguintes fatores:

- problemas temporários de comunicação entre os serviços da Bitdefender.
- alguns dos serviços da Bitdefender estão parados.
- Outras soluções de segurança em execução no seu computador, ao mesmo tempo que o Bitdefender.

Para solucionar este erro, tente estas soluções:

1. Espere uns momentos e verifique se existe alguma alteração. Este erro pode ser temporário.
2. Reinicie o computador e aguarde alguns momentos até o Bitdefender iniciar. Abra o Bitdefender e veja se o erro se mantém. Reiniciar o computador normalmente resolve o problema.
3. Verifique se tem qualquer outra solução de segurança instalada na medida em que possam interferir no funcionamento normal do Bitdefender. Se for este o caso, recomendamos que remova todas as outras soluções de segurança e reinstale Bitdefender.

   Para mais informação, dirija-se a "*Como posso remover outras soluções de segurança?*" (p. 82).

Se o erro persistir, por favor contacte os nossos representantes do suporte conforme descrito na secção "*Pedir Ajuda*" (p. 325).

6.1.11. O filtro Antispam não está a funcionar corretamente

Este artigo ajuda a solucionar os seguintes problemas relacionados com a operação de filtragem do Antispam do Bitdefender:

- Um número de mensagens de e-mail legítimas são marcadas como [spam].
- Muitas mensagens spam não estão marcadas de acordo com o filtro antispam.
- O filtro antispam não deteta qualquer mensagem de spam.

Mensagens legítimas são marcadas como [spam]

Mensagens legítimas são marcadas como [spam] simplesmente porque elas parecem spam para o filtro antispam do Bitdefender. Pode normalmente resolver este problema ao configurar adequadamente o filtro Antispam.

O Bitdefender adiciona automaticamente os remetentes das suas mensagens de e-mail à Lista de Amigos. As mensagens de e-mail recebidas dos contactos na lista de Amigos são consideradas legítimas. Elas não são verificadas pelo filtro antispam e, deste modo, elas nunca são marcadas como [spam].

A configuração automática da lista de Amigos não impede a deteção de erros que podem ocorrer nestas situações:

- Recebeu muitos e-mails publicitários solicitados como resultado de se inscrever em vários sites. Neste caso, a solução é adicionar à Lista de Amigos o endereço de e-mail do qual recebeu esses e-mails.
- Uma parte significativa dos seus mails legítimos são de pessoas com quem nunca trocou e-mails antes, tais como clientes, potenciais parceiros empresariais e outros. Outras soluções são requeridas neste caso.

  Se estiver a utilizar um cliente de email com o qual o Bitdefender é compatível, indique erros de deteção.

> **Nota**
> O BiDefender integra uma barra antispam de facil utilização, nos clientes de email mais comuns. Para ver a lista completa de clientes de e-mail suportados, por favor consulte o "*Clientes de email e protocolos suportados*" (p. 113).

Adicionar contactos à Lista de Amigos

Se está a utilizar um cliente de mail suportado, pode facilmente adicionar os remetentes das mensagens legítimas à lista de Amigos. Siga os seguintes passos:

1. No seu cliente de mail, selecione a mensagem de e-mail do remetente que quer adicionar à lista de Amigos.
2. Clique no botão **Adicionar Amigos** da barra de tarefas antispam do Bitdefender.
3. Poderá ser convidado a reconhecer os endereços adicionados à lista de Amigos. Selecione **Não mostrar esta mensagem outra vez** e clique **OK**.

Irá sempre receber mensagens de e-mail destes endereços, independentemente do conteúdo da mensagem.

Se está a utilizar um cliente de mail diferente, poderá adicionar os contactos à lista Amigos a partir do interface do Bitdefender. Siga os seguintes passos:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **ANTISPAM**, clique em **Gerir amigos**.

   Aparece uma janela de configuração.
4. Digite o endereço de email onde quer sempre receber as mensagens de email e depois clique em **Adicionar**. Pode adicionar quantos endereços de email desejar.
5. Clique em **OK** para guardar as alterações e fechar a janela.

Indique os erros de deteção

Se estiver a usar um cliente de e-mail suportado, pode facilmente corrigir o filtro antispam (indicando mensagens de correio eletrónico que não deveriam ter sido marcadas como[spam]). Se o fizer, ajuda a melhorar a eficiência do filtro antispam. Siga os seguintes passos:

1. Abra o mail de cliente.
2. Vá à pasta de lixo eletrónico, para onde são movidas as mensagens.
3. Selecione a mensagem legítima incorretamente marcada como [spam] pelo Bitdefender.

4. Clique no botão **Adicionar Amigos** da barra de tarefas antispam do Bitdefender para adicionar o remetente à lista de Amigos. Pode necessitar de clicar em **OK** para confirmar. Irá sempre receber mensagens de e-mail destes endereços, independentemente do conteúdo da mensagem.
5. Clique no botão **Não Spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de mail do cliente). A mensagem de email será movida para a pasta de Entrada.

Muitas mensagens de spam não são detetadas

Se está a receber muitas mensagens spam que não estão marcadas como [spam], tem de configurar o filtro antispam Bitdefender de modo a melhorar a sua eficiência.

Tente as seguintes soluções:

1. Se estiver a utilizar um cliente de email com o qual o Bitdefender é compatível, indique mensagens de spam não detetadas.

   Nota

   O BiDefender integra uma barra antispam de facil utilização, nos clientes de email mais comuns. Para ver a lista completa de clientes de e-mail suportados, por favor consulte o *"Clientes de email e protocolos suportados"* (p. 113).

2. Adicione spammers à lista de Spammers. As mensagens de e-mail recebidas dos endereços na lista de Spammers são automaticamente marcadas como [spam].

Indica mensagens de spam não detetadas

Se estiver a utilizar um cliente de e-mail suportado, pode facilmente indicar quais as mensagens de e-mail que devem ser detectadas como spam. Se o fizer, ajuda a melhorar a eficiência do filtro antispam. Siga os seguintes passos:

1. Abra o mail de cliente.
2. Vá à pasta Caixa de Entrada.
3. Selecione as mensagens spam não detetadas
4. Clique no botão **É Spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de email

do cliente). São imediatamente marcadas como [spam] e movidas para a pasta de lixo electrónico.

Adicionar spammers à lista de Spammers

Se está a utilizar um cliente de mail suportado, pode facilmente adicionar os remetentes das mensagens spam à lista Spammers. Siga os seguintes passos:

1. Abra o mail de cliente.
2. Vá à pasta de lixo eletrónico, para onde são movidas as mensagens.
3. Selecione a mensagem marcada como [spam] pelo Bitdefender.
4. Clique no botão **Adicionar Spammer** da barra de tarefas antispam do Bitdefender.
5. Poderá ser convidado a reconhecer os endereços como Spammers. Selecione **Não mostrar esta mensagem outra vez** e clique **OK**.

Se está a utilizar um cliente de mail diferente, poderá adicionar manualmente os spammers à lista de Spammers a partir do interface do Bitdefender. É conveniente que o faça apenas quando receber várias mensagens spam do mesmo endereço e-mail. Siga os seguintes passos:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **ANTISPAM**, clique em **Gerir spammers**.

   Aparece uma janela de configuração.
4. Digite o endereço de email do spammer e depois clique em **Adicionar**. Pode adicionar quantos endereços de email desejar.
5. Clique em **OK** para guardar as alterações e fechar a janela.

O Filtro Antispam não deteta nenhuma mensagem spam

Se nenhuma mensagem spam for marcada como [spam], poderá haver algum problema como o filtro Antispam do Bitdefender. Antes de resolver este problema, certifique-se de que não é causado por nenhuma das seguintes condições:

- A proteção antispam poderá estar desligada. Para verificar o estado de proteção antispam, clique no ícone na barra lateral esquerda da

interface do Bitdefender e, em seguida, selecione a hiperligação **VER FUNCIONALIDADES**. Clique na roda dentada do painel **ANTISPAM**, em seguida, consulte o lado superior da janela para verificar se a funcionalidade está ativada.

Se o Antispam estava desligado, era isso que estava a causar o problema. Clique no botão correspondente para ativar a sua proteção antispam.

- A proteção de Antispam do Bitdefender está disponível apenas para clientes de correio eletrónico configurado para receber mensagens de e-mail via protocolo POP3. Isto significa o seguinte:
  - As mensagens de Email obtidas através de Webmail (Yahoo, Gmail, Hotmail ou outros) não são filtradas como spam pelo Bitdefender.
  - Se o seu cliente de e-mail está configurado para receber mensagens de e-mail usando outro protocolo que não o POP3 (por exemplo, IMAP4), o filtro Antispam do Bitdefender não as analisará à procura de spam.

  Nota

  POP3 é um dos protocolos mais utilizados para fazer o download de mensagens de e-mail a partir de um servidor de correio. Se você não sabe o protocolo que o seu cliente de e-mail utiliza para importar mensagens de e-mail, solicite à pessoa que o configurou.

- O Bitdefender Total Security não analisa o tráfego POP3 do Lotus Notes.

Uma solução possivel é reparar ou reinstalar o produto. Contudo, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 325).

6.1.12. A funcionalidade Preenchimento automático na minha Carteira não funciona

Guardou as suas credenciais online no seu Gestor de Palavras-passe do Bitdefender e constatou que o preenchimento automático não está a funcionar. Normalmente, este problema surge quando a extensão da Carteira do Bitdefender não está instalada no seu browser.

Para resolver esta situação, siga estes passos:

- No **Internet Explorer:**

  1. Abra o Internet Explorer.

2. Clique em Ferramentas.
3. Clique em Gerir suplementos.
4. Clique em Ferramentas e Extensões.
5. Consulte **Portfólio do Bitdefender** e clique em **Ativar**.

- No **Mozilla Firefox:**
  1. Abra o Mozilla Firefox.
  2. Clique em Ferramentas.
  3. Clique em Suplementos.
  4. Clique em Extensões.
  5. Consulte **Portfólio do Bitdefender** e clique em **Ativar**.
- No **Google Chrome:**
  1. Abra o Google Chrome.
  2. Aceda ao ícone Menu.
  3. Clique em Mais Ferramentas.
  4. Clique em Extensões.
  5. Consulte **Portfólio do Bitdefender** e clique em **Ativar**.

Nota
O suplemento será ativado após reiniciar o browser.

Agora verifique se a funcionalidade de preenchimento automático na Carteira está a funcionar para as suas contas online.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 325).

6.1.13. Remoção de Bitdefender falhou

Caso pretenda remover o seu produto Bitdefender e constate que o processo demora ou o sistema bloqueia, clique em **Cancelar** para interromper a ação. Se isso não funcionar, reinicie o sistema.

Se a remoção falhar, algumas chaves de registo e ficheiros do Bitdefender poderão permanecer no seu sistema. Esses resquícios podem impedir uma

nova instalação do Bitdefender. Podem também afectar o desempenho e a estabilidade do sistema.

Para remover o Bitdefender completamente do seu sistema:

- No **Windows 7**:
  1. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
  2. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
  3. Clique em **REMOVER** na janela que aparece.
  4. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.
- No **Windows 8 e Windows 8.1**:
  1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
  2. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
  3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
  4. Clique em **REMOVER** na janela que aparece.
  5. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.
- No **Windows 10**:
  1. Clique em **Iniciar**, em seguida, clique em Definições.
  2. Clique no ícone **Sistema** na área das Definições, em seguida, selecione **Aplicações instaladas**.
  3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
  4. Clique em **Desinstalar** novamente para confirmar a sua escolha.
  5. Clique em **REMOVER** na janela que aparece.
  6. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

6.1.14. O meu sistema não reinicia após a instalação de Bitdefender

Se instalou o Bitdefender e não consegue reiniciar o seu sistema no modo normal, podem existir vários motivos para este problema.

Isto é muito provavelmente causado por uma instalação anterior de Bitdefender que não foi removida adequadamente ou por outra solução de segurança que ainda se encontra no sistema.

Eis como pode resolver cada situação:

- **Você tinha o Bitdefender anteriormente e não o removeu corretamente.**

  Para resolver isto:

  1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como o fazer, consulte "*Como posso reiniciar no Modo de Segurança?*" (p. 83).
  2. Remove Bitdefender do seu sistema:
     - No **Windows 7**:
       a. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
       b. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
       c. Clique em **REMOVER** na janela que aparece.
       d. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.
       e. Reinicie o sistema no modo normal.
     - No **Windows 8 e Windows 8.1**:
       a. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
       b. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
       c. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
       d. Clique em **REMOVER** na janela que aparece.

e. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

f. Reinicie o sistema no modo normal.

- No **Windows 10**:

a. Clique em **Iniciar**, em seguida, clique em Definições.

b. Clique no ícone **Sistema** na área das Definições, em seguida, selecione **Aplicações instaladas**.

c. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.

d. Clique em **Desinstalar** novamente para confirmar a sua escolha.

e. Clique em **REMOVER** na janela que aparece.

f. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

g. Reinicie o sistema no modo normal.

3. Reinstale o seu produto Bitdefender

- **Você tinha uma solução de segurança diferente anteriormente e não a eliminou corretamente.**

Para resolver isto:

1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como o fazer, consulte "*Como posso reiniciar no Modo de Segurança?*" (p. 83).

2. Remova as outras soluções de segurança do seu sistema:

- No **Windows 7**:

a. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.

b. Encontre o nome do programa que pretende remover e selecione **Remover**.

c. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

- No **Windows 8 e Windows 8.1**:

a. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.

b. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.

c. Encontre o nome do programa que pretende remover e selecione **Remover**.

d. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

- No **Windows 10**:

a. Clique em **Iniciar**, em seguida, clique em Definições.

b. Clique no ícone **Sistema** na área das Definições, em seguida, selecione **Aplicações instaladas**.

c. Encontre o nome do programa que pretende remover e selecione **Desinstalar**.

d. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

Para desinstalar corretamente outro software, aceda ao site Web do fornecedor e execute a ferramenta de desinstalação ou contacte-o para diretamente, para que lhe indiquem os procedimentos de desinstalação.

3. Reinicie o seu sistema no modo normal e reinstale o Bitdefender.

Já seguiu os passos acima e o problema não está resolvido.

Para resolver isto:

1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como o fazer, consulte "*Como posso reiniciar no Modo de Segurança?*" (p. 83).
2. Usar a opção de Restauro do Sistema do Windows para restaurar o computador para uma data anterior antes de instalar o produto Bitdefender.
3. Reinicie o sistema no modo normal e contacte os nossos representantes do suporte conforme descrito na secção "*Pedir Ajuda*" (p. 325).

6.2. Remover ameaças do seu sistema

As ameaças podem afetar o seu sistema de várias formas e a atuação do Bitdefender depende do tipo de ataque da ameaça. Como as ameaças alteram frequentemente o modo de ação, é difícil estabelecer um padrão com base no comportamento e nas ações.

Há situações em que o Bitdefender não consegue remover automaticamente a infecção de ameaças do seu sistema. Nestes casos, a sua intervenção é necessária.

- "*Modo de Recuperação Bitdefender (ambiente de recuperação no Windows 10)*" (p. 210)
- "*O que fazer se o Bitdefender encontrar ameaças no seu computador?*" (p. 214)
- "*Como posso limpar uma ameaça num ficheiro?*" (p. 216)
- "*Como posso limpar uma ameaça num ficheiro de e-mail?*" (p. 217)
- "*O que fazer se suspeitar que um ficheiro é perigoso?*" (p. 218)
- "*O que são os ficheiros protegidos por palavra-passe no relatório de análise?*" (p. 218)
- "*O que são os itens ignorados no relatório de análise?*" (p. 219)
- "*O que são os ficheiros muito comprimidos no relatório de análise?*" (p. 219)
- "*Por que é que Bitdefender eliminou automaticamente um ficheiro infectado?*" (p. 219)

Se não conseguir encontrar o seu problema aqui, ou se as soluções apresentadas não resolvem o seu problema, pode contactar os representantes do apoio técnico da Bitdefender como mostrado no capítulo "*Pedir Ajuda*" (p. 325).

6.2.1. Modo de Recuperação Bitdefender (ambiente de recuperação no Windows 10)

O **Modo de Recuperação** é uma funcionalidade do Bitdefender que permite analisar e desinfetar todas as partições existentes do disco rígido dentro e fora do sistema operativo.

Quando o Bitdefender Total Security for instalado no **Windows 7, Windows 8 e Windows 8.1** e o ficheiro da imagem do modo de recuperação do

Bitdefender for transferido, o Modo de Recuperação pode ser utilizado mesmo se já não conseguir arrancar no Windows.

No Windows 10, o Ambiente de Recuperação do Bitdefender é integrado com Windows RE, ou seja, não é necessário transferir qualquer Imagem do Modo de Recuperação neste sistema operativo e não é possível utilizar a funcionalidade se houver problemas de arranque. Para limpar o sistema antes de os serviços do Windows serem carregados, recomendamos utilizar o CD de Recuperação do Bitdefender.

O CD de Recuperação do Bitdefender é uma ferramenta gratuita que analisa e limpa o seu computador sempre que suspeitar que uma ameaça está a afetar o seu funcionamento. Os artigos úteis com detalhes sobre a respetiva criação e utilização estão disponíveis na plataforma do Centro de Suporte do Bitdefender em https://www.bitdefender.com/support/consumer.html.

A transferir a imagem do Modo de Recuperação do Bitdefender

Para utilizar o Modo de Recuperação no **Windows 7, Windows 8 e Windows 8.1**, primeiro tem de transferir o respetivo ficheiro de imagem como se segue:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **ANTIVÍRUS**, clique em **Modo de Recuperação**.
4. Clique em **SIM** na janela de confirmação que surge para reiniciar o seu computador.

   Aguarde pela transferência do ficheiro de imagem do Modo de Recuperação do Bitdefender dos servidores do Bitdefender. Assim que o processo de transferência estiver concluído, o computador reinicia.

   Surge um menu a solicitar que selecione um sistema operativo. Neste passo pode escolher iniciar com o seu sistema no Modo de Recuperação ou no modo normal.

Nota

Devido à integração com o Ambiente de Recuperação do Windows no **Windows 10**, não é necessário transferir qualquer Imagem do Modo de Recuperação neste sistema operativo.

Arranque o sistema no Modo de Recuperação no Windows 7, Windows 8 e Windows 8.1

Pode entrar no Modo de Recuperação de duas formas:

A partir da interface do Bitdefender

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **ANTIVÍRUS**, clique em **Modo de Recuperação**.
4. Clique em **SIM** na janela de confirmação que surge para reiniciar o seu computador.
5. Depois de o computador reiniciar, irá aparecer um menu para selecionar um sistema operativo. Escolha **Modo de Recuperação do Bitdefender** para iniciar no ambiente do Bitdefender, de onde pode limpar a sua partição do Windows.
6. Se notificado, prima **Enter** e selecione a resolução do ecrã mais aproximada daquela que normalmente usa. Depois prima de novo **Enter**.

   O Modo de Recuperação do Bitdefender carrega dentro de momentos.

Arranque o seu computador diretamente no Modo de Recuperação

Se o Windows já não iniciar, pode arrancar o seu computador diretamente no Modo de Recuperação do Bitdefender, seguindo os passos abaixo:

- No **Windows 7**:
  1. Prima a tecla **F8** até o ecrã **Opções de Arranque Avançadas** ser apresentado.
  2. Utilize as teclas de seta para selecionar o Modo de Recuperação do Bitdefender e prima **Enter**.

     O Modo de Recuperação do Bitdefender irá carregar dentro de momentos.
- No **Windows 8 e Windows 8.1**:
  1. Prima a tecla **Shift** até o ecrã **Opções de Arranque Avançadas** ser apresentado.

2. Selecione a opção **Utilizar outro sistema operativo** e, em seguida, Modo de Recuperação do Bitdefender.

   O Modo de Recuperação do Bitdefender irá carregar dentro de momentos.

> **Nota**
> É possível carregar o computador no Modo de Recuperação apenas se o ficheiro da Imagem do Modo de Recuperação tiver sido transferido previamente como descrito em "A transferir a imagem do Modo de Recuperação do Bitdefender" (p. 211).

Arranque do sistema no Ambiente de Recuperação no Windows 10

Só pode aceder ao Ambiente de Recuperação a partir do produto Bitdefender como se segue:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Clique na hiperligação **VER FUNCIONALIDADES**.
3. No painel **ANTIVÍRUS**, clique em **Ambiente de Recuperação**.
4. Clique em **Reiniciar** na janela que é apresentada.

   O Ambiente de Recuperação do Bitdefender é carregado dentro de momentos.

Analisar o sistema no Modo de Recuperação (Ambiente de Recuperação no Windows 10)

Para analisar o sistema no Modo de Recuperação (Ambiente de Recuperação):

- No **Windows 7, Windows 8 e Windows 8.1**:
  1. Entre no Modo de Recuperação, conforme descrito em "Arranque o sistema no Modo de Recuperação no Windows 7, Windows 8 e Windows 8.1" (p. 212).
  2. O logótipo do Bitdefender surgirá e os motores da solução de segurança começarão a ser copiados.
  3. Uma janela de boas-vindas aparece. Clique em **Continuar**.

4. Foi iniciada uma atualização da base de dados de informações de ameaças.
5. Quando a atualização estiver concluída, a janela da Análise-a-pedido do Bitdefender irá aparecer.
6. Clique em **Analisar Agora**, selecione o alvo da análise na janela que surge e, em seguida, clique em **Abrir** para iniciar a análise.

   Recomenda-se que analise toda a partição do Windows.

   > **Nota**
   > Ao trabalhar no Modo de Recuperação, lida com nomes de partições do tipo do Linux. As partições do disco surgirão como sda1 provavelmente correspondendo à (C:) partição do Windows, sda2 correspondendo a (D:) e assim sucessivamente.

7. Aguarde que a análise termine. Se for detetada qualquer ameaça, siga as instruções para a remover.
8. Para sair do Modo de Recuperação, clique com o botão direito do rato numa área vazia do ambiente de trabalho, selecione **Sair** no menu que aparece e depois escolha entre reiniciar ou encerrar o computador.

- No **Windows 10**:

1. Aceda ao Ambiente de Recuperação como descrito em "Arranque do sistema no Ambiente de Recuperação no Windows 10" (p. 213).
2. O processo de análise do Bitdefender começa automaticamente assim que o sistema é carregado no Ambiente de Recuperação.
3. Aguarde que a análise termine. Se for detetada qualquer ameaça, siga as instruções para a remover.
4. Para sair do Ambiente de Recuperação, clique no botão **FECHAR** na janela com os resultados da análise.

6.2.2. O que fazer se o Bitdefender encontrar ameaças no seu computador?

Pode descobrir que tem uma ameaça no seu computador de uma das seguintes formas:

- O Bitdefender analisou o seu computador e encontrou itens infectados.

- Um alerta de ameaças avisa que o Bitdefender bloqueou uma ou várias ameaças no seu computador.

Nessas situações, atualize o Bitdefender para se certificar de que possui a base de dados mais recente de informações sobre a ameaça e realize uma Análise de Sistema.

Assim que a análise do sistema terminar, selecione a ação pretendida para os itens infetados (Desinfetar, Eliminar, Mover para a Quarentena).

Atenção
Se suspeitar que o ficheiro faz parte do sistema operativo do Windows ou que não é um ficheiro infectado, não siga estes passos e contacte e Apoio ao Cliente do Bitdefender assim que possível.

Se não for possível efetuar a ação selecionada e o relatório da análise indicar uma infecção que não foi possível eliminar, tem de remover o(s) ficheiro(s) manualmente:

O primeiro método pode ser utilizado no modo normal:

1. Desative a proteção antivírus em tempo real do Bitdefender:
   a. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
   b. Clique na hiperligação **VER FUNCIONALIDADES**.
   c. Clique no ícone no canto inferior direito do painel **ANTIVÍRUS**.
   d. Na janela **PROTEÇÃO**, clique no botão LIGAR/DESLIGAR.
2. Mostrar objetos ocultos no Windows. Para saber como o fazer, consulte "*Como posso mostrar objetos ocultos no Windows?*" (p. 81).
3. Procure a localização do ficheiro infectado (veja no relatório da análise) e elimine-o.
4. Ligue a proteção antivírus em tempo real do Bitdefender.

Caso o primeiro método para remover a infeção falhe:

1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como o fazer, consulte "*Como posso reiniciar no Modo de Segurança?*" (p. 83).
2. Mostrar objetos ocultos no Windows. Para saber como o fazer, consulte "*Como posso mostrar objetos ocultos no Windows?*" (p. 81).

3. Procure a localização do ficheiro infectado (veja no relatório da análise) e elimine-o.
4. Reinicie o seu sistema e inicie sessão no modo normal.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 325).

6.2.3. Como posso limpar uma ameaça num ficheiro?

Um arquivo é um ficheiro ou um conjunto de ficheiros comprimidos num formato especial para reduzir o espaço no disco necessário para armazenar os ficheiros.

Alguns destes formatos são formatos livres, possibilitando ao Bitdefender a opção de analisar o conteúdo e aplicar as ações adequadas para os remover.

Outros formatos de arquivo estão parcial ou totalmente fechados, mas o Bitdefender só pode detetar a presença de ameaças no interior, mas não pode aplicar outras ações.

Se o Bitdefender avisar que foi detetada uma ameaça dentro de um arquivo e não estiver disponível uma ação, significa que não é possível remover a ameaça devido a restrições nas definições de permissão do arquivo.

Eis como pode limpar uma ameaça armazenada num arquivo:

1. Identifique o arquivo que inclui a ameaça ao executar uma Análise do Sistema.
2. Desative a proteção antivírus em tempo real do Bitdefender:
   a. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
   b. Clique na hiperligação **VER FUNCIONALIDADES**.
   c. Clique no ícone no canto inferior direito do painel **ANTIVÍRUS**.
   d. Na janela **PROTEÇÃO**, clique no botão LIGAR/DESLIGAR.
3. Vá à localização do arquivo e descomprima-o com uma aplicação de arquivo, como o WinZip.
4. Identifique e elimine o ficheiro infectado.

5. Elimine o arquivo original de modo a garantir que a infecção é totalmente removida.
6. Comprima novamente os ficheiros num novo arquivo com uma aplicação de arquivo, como o WinZip.
7. Ative a proteção antivírus em tempo real do Bitdefender e execute uma análise ao sistema para se certificar que não há outras infeções no sistema.

Nota
É importante observar que uma ameaça armazenada num arquivo não é uma ameaça imediata para o seu sistema pois a ameaça tem de ser descomprimida e executada para infetar o seu sistema.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 325).

6.2.4. Como posso limpar uma ameaça num ficheiro de e-mail?

O Bitdefender também pode identificar ameaças em bases de dados de correio eletrónico e arquivos de correio eletrónico armazenados no disco.

Por vezes, é necessário identificar a mensagem infectada com a informação fornecida no relatório da análise, e elimine-o manualmente.

Eis como pode limpar uma ameaça armazenada num arquivo de e-mail:

1. Analisar a base de dados do correio eletrónico com o Bitdefender.
2. Desative a proteção antivírus em tempo real do Bitdefender:
   a. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
   b. Clique na hiperligação **VER FUNCIONALIDADES**.
   c. Clique no ícone no canto inferior direito do painel **ANTIVÍRUS**.
   d. Na janela **PROTEÇÃO**, clique no botão LIGAR/DESLIGAR.
3. Abra o relatório da análise e utilize a informação de identificação (Assunto, De, Para) das mensagens infectadas para localizá-las no cliente de correio eletrónico.

4. Elimine as mensagens infectadas. A maioria dos clientes de correio eletrónico move a mensagem eliminada para uma pasta de recuperação, a partir da qual pode ser recuperada. Deve certificar-se que a mensagem também é eliminada desta pasta de recuperação.
5. Compactar a pasta com a mensagem infectada.
   - No Microsoft Outlook 2007: No menu Ficheiro, clique em Gestão de Ficheiros de Dados. Selecione os ficheiros das pastas (.pst) que pretende compactar e clique em Definições. Clique em Compactar Agora.
   - No Microsoft Outlook 2010/2013/2016: No menu Ficheiro, clique em Informações e, em seguida, em definições de Conta (Adicionar e remover contas ou alterar as definições de ligação existentes). Clique em Ficheiro de Dados, selecione os ficheiros das pastas (.pst) que pretende compactar e clique em Definições. Clique em Compactar Agora.
6. Ligue a proteção antivírus em tempo real do Bitdefender.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 325).

6.2.5. O que fazer se suspeitar que um ficheiro é perigoso?

Pode suspeitar que um ficheiro do seu sistema é perigoso, embora o seu produto Bitdefender não o tenha detetado.

Para garantir que o seu sistema está protegido:

1. Execute uma **Análise de Sistema** com o Bitdefender. Para saber como o fazer, consulte "*Como posso analisar o seu sistema?*" (p. 59).
2. Se no resultado da análise parece estar limpo, mas você ainda tem dúvidas e quer verificar o ficheiro, contacte os representantes do suporte para que o possamos ajudar.

   Para saber como o fazer, consulte "*Pedir Ajuda*" (p. 325).

6.2.6. O que são os ficheiros protegidos por palavra-passe no relatório de análise?

Isto é apenas uma notificação que indica que o Bitdefender detetou que estes ficheiros estão protegidos por palavra-passe ou por outra forma de encriptação.

Normalmente, os itens protegidos por palavra-passe são:

- Ficheiros que pertencem a outras solução de segurança.
- Ficheiros que pertencem ao sistema operativo.

Para analisar verdadeiramente os conteúdos, estes ficheiros têm de ser extraídos ou descodificados.

Se estes conteúdos pudessem ser extraídos, o verificador em tempo real do Bitdefender analisaria-os automaticamente para manter o seu computador protegido. Se pretende analisar esses ficheiros com o Bitdefender, terá de contactar o fabricante do produto para receber mais informações sobre esses ficheiros.

Recomendamos que ignore estes ficheiros pois não constituem uma ameaça ao seu sistema.

6.2.7. O que são os itens ignorados no relatório de análise?

Todos os ficheiros que aparecem como Ignorados no relatório de análise estão limpos.

Para um melhor desempenho, o Bitdefender não analisa ficheiros que não tenham sido alterados desde a última análise.

6.2.8. O que são os ficheiros muito comprimidos no relatório de análise?

Os itens sobre-comprimidos são elementos que não puderam ser extraídos pelo motor de análise ou elementos para os quais a desencriptação levaria demasiado tempo, tornando o sistema instável.

Sobre-comprimido significa que o Bitdefender não realizou a análise a esse arquivo pois a descompactação iria consumir demasiados recursos do sistema. O conteúdo será analisado aquando o acesso em tempo real, se necessário.

6.2.9. Por que é que Bitdefender eliminou automaticamente um ficheiro infectado?

Se for detetado um ficheiro infectado, o Bitdefender tentará automaticamente desinfectá-lo. Se a desinfecção falhar, o ficheiro é movido para a quarentena de modo a restringir a infecção.

Para determinados tipos de ameaças, a desinfeção não é possível por o ficheiro detetado ser totalmente malicioso. Nestes casos, o ficheiro infectado é eliminado do disco.

Este é, normalmente, o caso de ficheiros de instalação que são transferidos de sites Internet suspeitos. Se se deparar numa situação assim, transfira o ficheiro de instalação do site Internet do fabricante ou de outro site fidedigno.

ANTIVIRUS PARA MAC

7. INSTALAÇÃO E REMOÇÃO

Este capítulo inclui os seguintes tópicos:

- "*Requisitos de Sistema*" (p. 222)
- "*A instalar Bitdefender Antivirus for Mac*" (p. 222)
- "*Remover o Bitdefender Antivirus for Mac*" (p. 228)

7.1. Requisitos de Sistema

Pode instalar o Bitdefender Antivirus for Mac em computadores Macintosh com Intel e com OS X Mavericks (10.9.5), OS X Yosemite (10.10.5), OS X El Capitan (10.11.6), macOS Sierra (10.12.5 ou posterior), macOS High Sierra 10.13 instalados.

Seu Mac também deve atender a todos esses requisitos adicionais:

- Mínimo de 1 GB de Memória RAM
- Mínimo 600 MB de espaço disponível em disco

É necessária uma ligação à Internet para registar e atualizar Bitdefender Antivirus for Mac.

Como obter a versão do seu macOS e informações de hardware do seu Mac

Clique no ícone Apple no canto superior esquerdo do ecrã e escolha **Sobre este Mac**. Na janela apresentada, pode ver a versão do seu sistema operativo e outras informações úteis. Clique em **Mais informações** para obter informações detalhadas sobre o hardware.

7.2. A instalar Bitdefender Antivirus for Mac

A aplicação Bitdefender Antivirus for Mac pode ser instalada a partir da sua conta Bitdefender, conforme se segue:

1. Inicie sessão como administrador.
2. Vá para: https://central.bitdefender.com.
3. Inicie sessão na sua conta Bitdefender utilizando o seu endereço de e-mail e palavra-passe.

4. Selecione o painel **Os meus dispositivos**, e clique em **INSTALAR PROTEÇÃO LOCAL**.
5. Escolha uma das duas opções disponíveis:
   - **DOWNLOAD**

     Clique no botão e guarde o ficheiro de instalação.
   - **Noutro dispositivo**

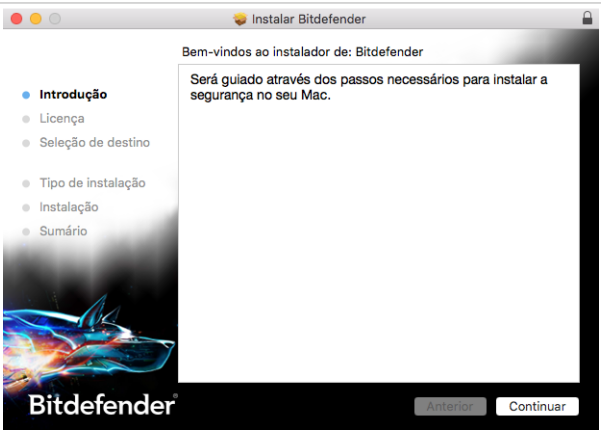
     Selecione **macOS X** para transferir o seu produto Bitdefender e clique em **CONTINUAR**. Introduza um endereço de e-mail no campo correspondente e clique em **ENVIAR**.
6. Execute o Bitdefender que transferiu.
7. Conclua os passos de instalação.

7.2.1. Processo de instalação

Para instalar o Bitdefender Antivirus for Mac:

1. Clique no ficheiro transferido. O instalador será iniciado e você será guiado pelo processo de instalação.
2. Siga o assistente de instalação.

Passo 1 - Janela de Boas-vindas



Janela de boas-vindas

Clique em **Continuar**.

Passo 2 - Ler o Acordo da Subscrição

Ler o Acordo da Subscrição

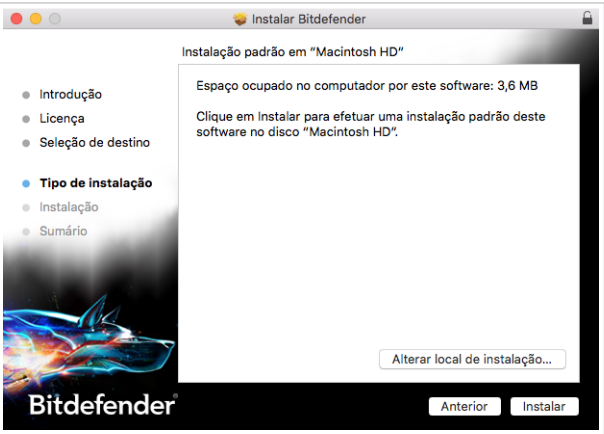
Antes de continuar com a instalação, tem de concordar com o Contrato de Subscrição. Leia o Contrato de Subscrição com calma pois contém os termos e condições que regem a utilização do Bitdefender Antivirus for Mac.

Clique em **Continuar** e em **Concordar**.

Importante

Caso não concorde com esses termos, clique em **Continuar** e em **Discordar** para cancelar a instalação e sair do instalador.

Passo 3 - Iniciar instalação

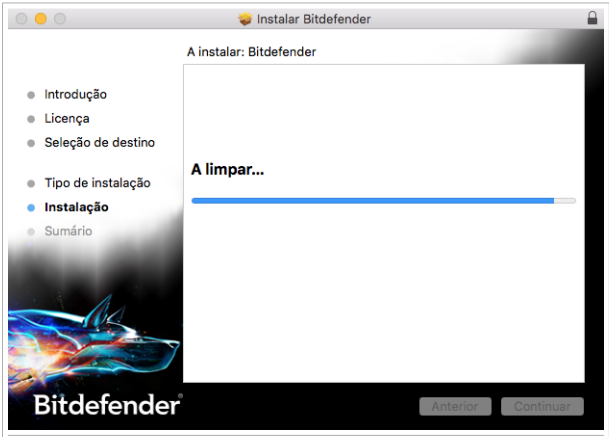


Iniciar instalação

O Bitdefender Antivirus for Mac será instalado em Macintosh HD/Biblioteca/Bitdefender. O caminho da instalação não pode ser modificado.

Clique em **Instalar** para iniciar a instalação.

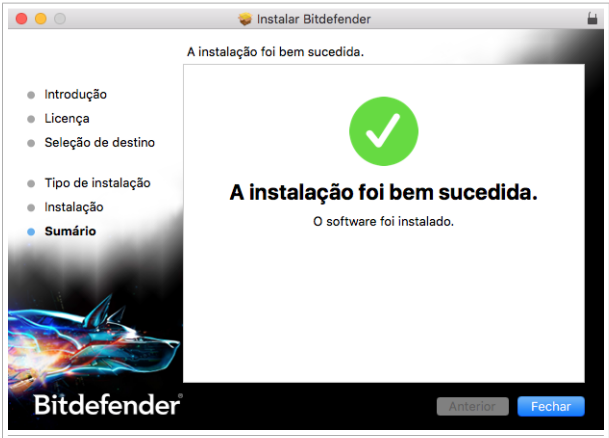
Passo 4 - Instalar o Bitdefender Antivirus for Mac



A instalar Bitdefender Antivirus for Mac

Aguarde a instalação concluir e clique em **Continuar**.

Passo 5 - Terminar



Terminar

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

O processo de instalação agora está concluído.

Importante
Se você está instalando o Bitdefender Antivirus for Mac no macOS versão High Sierra 10.13 ou superior, a notificação **System Extension Blocked** é exibida. A notificação informa que as extensões assinadas por Bitdefender foram bloqueadas e devem ser habilitadas manualmente. Clique em **OK** para continuar. Na janela Bitdefender Antivirus for Mac que é exibida, clique no link **Security & Privacy**. Selecione a caixa de verificação Bitdefender check na lista e, de seguida, clique em **OK**.

Na primeira instalação do Bitdefender Antivirus for Mac, o assistente da Proteção da Máquina do Tempo aparecerá e o Safe Files são exibidos. Para mais informações, aceda a "*Safe Files*" (p. 246) e a "*Proteção da Máquina do Tempo*" (p. 235).

Será direcionado à ferramenta de VPN. Clique em **Seguinte** para continuar. Para mais informação, dirija-se a "*VPN*" (p. 271).

7.3. Remover o Bitdefender Antivirus for Mac

Por ser uma aplicação complexa, o Bitdefender Antivirus for Mac não pode ser removido da forma convencional, ou seja, ao arrastar o ícone da aplicação da pasta Aplicações para a Reciclagem.

Para remover o Bitdefender Antivirus for Mac, siga os seguintes passos:

1. Abra uma janela **Finder** e aceda à pasta Aplicações.
2. Abra a empresa Bitdefender e clique duas vezes em DesinstalarBitdefender.
3. Clique em **Desinstalar** e aguarde pela conclusão do processo.
4. Clique em **Fechar** para terminar.

Importante
Se ocorrer um erro, pode entrar em contacto com o Atendimento ao Consumidor da Bitdefender, como descrito em "*Pedir Ajuda*" (p. 325).

8. INTRODUÇÃO

Este capítulo inclui os seguintes tópicos:

- "*Sobre o Bitdefender Antivirus for Mac*" (p. 229)
- "*A abrir o Bitdefender Antivirus for Mac*" (p. 229)
- "*Janela principal da aplicação*" (p. 230)
- "*Ícone de doca da aplicação*" (p. 231)

8.1. Sobre o Bitdefender Antivirus for Mac

O Bitdefender Antivirus for Mac é um detetor antivírus poderoso, que pode detetar e remover todos os tipos de software malicioso ("ameaças"), incluindo:

- ransomware
- Adware
- vírus
- spyware
- Trojans
- keyloggers
- worms

Esta aplicação deteta e remove não só ameaças no Mac, mas também ameaças no Windows, prevenindo, assim, que envie ficheiros infetados para a sua família, amigos e colegas utilizando PC.

8.2. A abrir o Bitdefender Antivirus for Mac

Pode abrir o Bitdefender Antivirus for Mac de várias formas.

- Clique no ícone do Bitdefender Antivirus for Mac no Launchpad.
- Clique no ícone na barra de menus e escolha **Abrir Janela Principal**.
- Abra uma janela do Finder, aceda a Aplicações e clique duas vezes no ícone Bitdefender Antivirus for Mac.

8.3. Janela principal da aplicação

Na janela principal da aplicação, pode verificar o estado de segurança do computador, efetuar análises do sistema, tornar a sua navegação na Web mais segura ou iniciar sessão na sua conta Bitdefender.

Janela principal da aplicação

A opção **Autopilot**, localizada na parte direita superior da janela principal, monitoriza continuamente as aplicações executadas no computador, à procura de ações típicas de ameaças e previne que novas entrem no seu sistema.

Por motivos de segurança, é recomendável deixar o Autopilot ligado. Se o Autopilot estiver desligado, não estará protegido automaticamente contra ameaças.

A barra de estado na parte superior da janela informa-o sobre o estado de segurança do sistema utilizando mensagens explícitas e cores sugestivas. Se o Bitdefender Antivirus for Mac não tiver alertas, a barra de estado é verde. Quando um problema de segurança for detetado, a barra de estado muda para amarelo. Clique no botão **Ver problemas** para ver os problemas que afetam a segurança do seu sistema. Para informações detalhadas sobre problemas e como os reparar, consulte "*Reparar Incidência*" (p. 238).

Sob a barra de estado, estão disponíveis três botões de análise para o ajudar a analisar o seu Mac:

- **Análise Rápida** - procura por ameaças nos locais mais vulneráveis no seu sistema (por exemplo, as pastas que contêm os documentos, transferências, transferências de e-mail e ficheiros temporários de cada utilizador).
- **Análise Completa** - realiza uma verificação completa por ameaças em todo o sistema. Todas as montagens ligadas também serão analisadas.
- **Análise Personalizada** - ajuda a verificar ameaças em ficheiros, pastas ou volumes específicos.

Para mais informação, dirija-se a "*Analisar o seu Mac*" (p. 234).

Além dos botões de análise, estão disponíveis opções adicionais:

- **Proteção na Web** - filtra todo o tráfego na Web e bloqueia qualquer conteúdo malicioso para tornar a sua experiência na Web mais segura. Para mais informação, dirija-se a "*Proteção da Internet*" (p. 239).
- **Aceder a conta Bitdefender** - clique na hiperligação **Aceder à sua conta** na parte inferior direita da interface principal para aceder à sua conta Bitdefender. Para mais informação, dirija-se a "*Bitdefender Central*" (p. 255).
- **Número de dias restantes** - apresenta o tempo restante antes de a sua subscrição expirar. Quando a data de expiração chegar, clique na hiperligação para aceder à página da Web onde pode renovar a sua subscrição.
- **Comprar** - redireciona-o para a página da Bitdefender, onde é possível conferir as ofertas disponíveis ou comprar uma subscrição.
- **Feedback** - abre uma nova janela no seu email de cliente predefinido para entrar em contacto connosco.

8.4. Ícone de doca da aplicação

O ícone do Bitdefender Antivirus for Mac pode ser visto na Dock assim que abrir a aplicação. O ícone na Dock proporciona uma forma fácil de procurar ameaças em ficheiros e pastas. Basta arrastar e largar o ficheiro ou pasta no ícone da Dock e a análise iniciará imediatamente.

Ícone na Dock

9. PROTEGER CONTRA SOFTWARE MALICIOSO

Este capítulo inclui os seguintes tópicos:

- "*Dicas de Utilização*" (p. 233)
- "*Analisar o seu Mac*" (p. 234)
- "*Ativar ou desativar o Autopilot*" (p. 235)
- "*Proteção da Máquina do Tempo*" (p. 235)
- "*Assistente de Análise*" (p. 237)
- "*Reparar Incidência*" (p. 238)
- "*Proteção da Internet*" (p. 239)
- "*Atualizações*" (p. 240)

9.1. Dicas de Utilização

Para manter o seu sistema protegido contra ameaças e evitar infeções acidentais de outros sistemas, siga estas práticas:

- Mantenha o **Autopilot** ligado para permitir que os ficheiros do sistema sejam verificados pelo Bitdefender Antivirus for Mac.
- Mantenha o seu Bitdefender Antivirus for Mac atualizado com as informações sobre ameaças e as atualizações de produto mais recentes, enquanto o **Autopilot** está ativado.
- Verifique e repare os problemas relatados pelo Bitdefender Antivirus for Mac regularmente. Para informação detalhada dirija-se a "*Reparar Incidência*" (p. 238).
- Verifique o registo detalhado de eventos referentes à atividade do Bitdefender Antivirus for Mac no seu computador. empre que algo relevante para a segurança do seu sistema ou dados acontecer, é adicionada uma nova mensagem ao histórico de Bitdefender. Para mais detalhes, aceda a "*Histórico*" (p. 248).
- É recomendável que também siga estas práticas:
  - Crie o hábito de verificar ficheiros que baixa de uma memória de armazenamento externa (como uma unidade USB ou CD), especialmente quando desconhecer a fonte.

- Se tiver um ficheiro DMG, monte-o e analise o seu conteúdo (os ficheiros no volume/imagem montada).

A forma mais fácil de analisar um ficheiro, pasta ou volume é arrastar&largar na janela ou ícone do Bitdefender Antivirus for Mac na Dock.

Nenhuma outra configuração ou ação é necessária. No entanto, se pretender, é possível ajustar as definições e preferências da aplicação para melhor satisfazer as suas necessidades. Para mais informação, dirija-se a "*Configurar preferências*" (p. 243).

9.2. Analisar o seu Mac

Além da funcionalidade **Autopilot**, que monitoriza continuamente as aplicações em execução no computador à procura de ações típicas de ameaças e previne que novas ameaças de malware entrem no seu sistema, pode analisar o seu Mac ou ficheiros específicos sempre que quiser.

A forma mais fácil de analisar um ficheiro, pasta ou volume é arrastar&largar na janela ou ícone do Bitdefender Antivirus for Mac na Dock. O assistente de análise aparece e orienta-o pelo processo de análise.

Também pode iniciar uma análise como se segue:

1. Abrir o Bitdefender Antivirus for Mac.
2. Clique num dos três botões para iniciar a análise desejada.
   - **Análise Rápida** - procura por ameaças nos locais mais vulneráveis no seu sistema (por exemplo, as pastas que contêm os documentos, transferências, transferências de e-mail e ficheiros temporários de cada utilizador).
   - **Análise Completa** - realiza uma verificação completa por ameaças em todo o sistema. Todas as montagens ligadas também serão analisadas.

> **Nota**
>
> Dependendo do tamanho do seu disco rígido, analisar todo o sistema pode demorar (até uma hora ou mais). Para um desempenho melhor, é recomendável não executar esta tarefa ao executar outras tarefas intensivas (como edição de vídeo).
> Se preferir, pode optar por não analisar volumes montados específicos adicionando-os à lista Exclusões na janela de Preferências.

- **Análise Personalizada** - ajuda a verificar ameaças em ficheiros, pastas ou volumes específicos.

9.3. Ativar ou desativar o Autopilot

Para ativar ou desativar o Autopilot, siga qualquer um dos seguintes passos:

- Abra o Bitdefender Antivirus for Mac e clique no botão para ativar ou desativar o Autopilot.
- Clique no ícone na barra de menus e escolha **DESATIVAR Autopilot**.

Atenção
Recomendamos que desative o Autopilot pelo tempo mais curto possível. Se o Autopilot estiver desligado, não estará protegido automaticamente contra ameaças.

9.4. Proteção da Máquina do Tempo

A Proteção da Máquina do Tempo da Bitdefender funciona como uma camada de segurança adicional para a sua unidade de backup, incluindo todos os ficheiros armazenados, através do bloqueio do acesso de qualquer fonte externa. Caso os ficheiros da sua unidade da Máquina do Tempo sejam encriptados por ransomware, será capaz de recuperá-los sem pagar pelo resgate.

Assistente da Proteção da Máquina do Tempo

O assistente da Proteção da Máquina do Tempo da Bitdefender aparecerá assim que o Bitdefender Antivirus for Mac for instalado pela primeira vez no seu Macintosh.

Assistente da Proteção da Máquina do Tempo

Necessita de configurar a aplicação do sistema de backup da Máquina do Tempo antes de ativar a proteção do Bitdefender.

Se a funcionalidade Máquina do Tempo não estiver ativada na sua máquina:

1. Clique na opção **Ir para Máquina do Tempo**.

   A janela **Máquina do Tempo** em Preferências do Sistema aparecerá.

2. Ative a funcionalidade e, em seguida, selecione o local para armazenar os ficheiros de backup.

Se necessitar de informações adicionais sobre como ativar a aplicação Máquina do Tempo no seu sistema, clique no link **Descobrir como configurar o Máquina do Tempo** no assistente.

Para ativar a Proteção da Máquina do Tempo da Bitdefender para os seus backups:

1. Clique na opção **Ativar proteção**.

   Aparece uma janela de confirmação.

2. Clique em **Fechar**.

Ativar ou desativar a Proteção da Máquina do Tempo

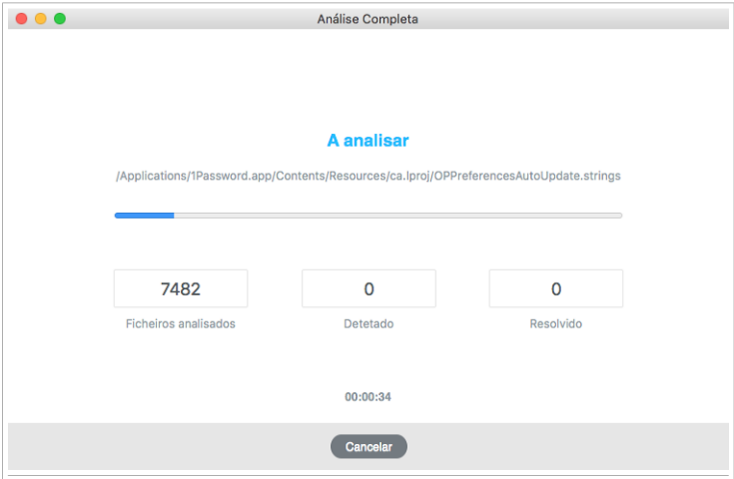
Para ativar ou desativar a Proteção da Máquina do Tempo:

1. Abrir o Bitdefender Antivirus for Mac.

2. Clique em Bitdefender Antivirus for Mac na barra de menus e escolha **Preferências**.
3. Selecione o separador **Proteção**.
4. Selecione ou desmarque a caixa de seleção **Proteção da Máquina do Tempo**.

9.5. Assistente de Análise

Sempre que iniciar uma verificação, o assistente de análise do Bitdefender Antivirus for Mac aparece.



Análise em progresso

Informações em tempo real sobre as ameaças detetadas e resolvidas são apresentadas durante cada análise.

Espere que o Bitdefender Antivirus for Mac termine a análise.

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

9.6. Reparar Incidência

O Bitdefender Antivirus for Mac deteta automaticamente e informa-o sobre uma série de problemas que podem afetar a segurança do seu sistema e dados. Desta forma, pode reparar riscos de segurança facilmente e a tempo.

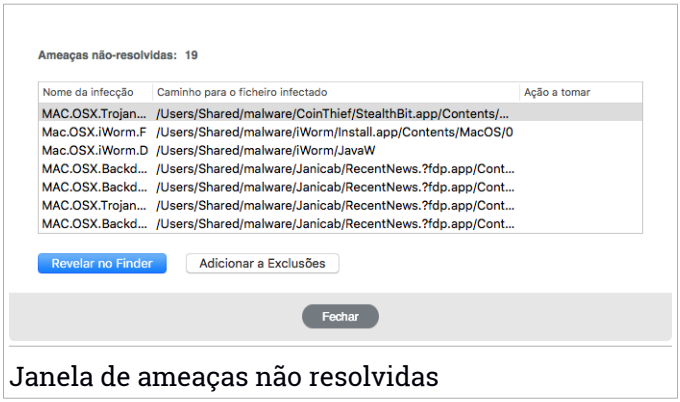
Reparar os problemas indicados pelo Bitdefender Antivirus for Mac é uma forma rápida e fácil de garantir a melhor proteção do seu sistema e dados.

Os problemas detetados incluem:

- As novas informações sobre ameaças e atualizações do produto não foram transferidas dos nossos servidores porque o **Autopilot** está desativado.
- Foram detetadas ameaças não resolvidas no seu sistema.
- O **Autopilot** está desativado.

Para verificar e reparar os problemas detetados:

1. Abrir o Bitdefender Antivirus for Mac.
2. Se o Bitdefender não tiver alertas, a barra de estado é verde. Quando um problema de segurança for detetado, a barra de estado muda para amarelo.
3. Verifique a descrição para obter mais informações.
4. Quando um problema for detetado, clique no botão **Ver problemas** para ver informações sobre o que está a afetar a segurança do seu sistema. Pode escolher ações na janela que aparece.



Janela de ameaças não resolvidas

A lista de ameaças não resolvidas é atualizada após cada análise de sistema.

Pode escolher as seguintes ações para ameaças não resolvidas:

- Revelar no Finder. Escolha essa ação para remover as infeções manualmente.
- Adicionar a Exclusões. Essa ação não está disponível para ameaças encontradas dentro de ficheiros.

9.7. Proteção da Internet

O Bitdefender Antivirus for Mac utiliza as extensões do TrafficLight para tornar a sua experiência de navegação na Web completamente segura. As extensões do TrafficLight intercetam, processam e filtram todo o tráfego na Web, bloqueando qualquer conteúdo malicioso.

As extensões funcionam e integram-se com os seguintes browsers: Mozilla Firefox, Google Chrome e Safari.

Ativar extensões do TrafficLight

Para ativar as extensões do TrafficLight, siga estes passos:

1. Abrir o Bitdefender Antivirus for Mac.
2. Clique em **Reparar Agora** para ativar a proteção na Web.
3. O Bitdefender Antivirus for Mac detetará que browser tem instalado no seu sistema. Para instalar a extensão do TrafficLight no seu browser, clique em **Obter Extensão**.
4. Será redirecionado para esta localização online:

   https://bitdefender.com/solutions/trafficlight.html
5. Selecione **Transferência gratuita**.
6. Siga os passos para instalar a extensão do TrafficLight correspondente ao seu browser.

Gerir definições da extensões

Está disponível uma variedade de funcionalidades para o proteger de todas as formas de ameaças que pode encontrar enquanto navega na Internet. Para acedê-los, clique no ícone do TrafficLight próximo das definições do navegador e, em seguida, clique em **Definições**:

- **Definições do Bitdefender TrafficLight**

- Filtro de Ameaças Avançado - previne que aceda a sites Web utilizados para ataques de malware, phishing e fraudulentos.
- Detetor do Controlador - deteta os controladores nas páginas Web visitadas e fornece-lhe informações acerca da sua presença.
- Analisador de Resultados de Pesquisa - proporciona alertas antecipados de sites Web de risco nos seus resultados de pesquisa.

  Caso todas as definições estejam desativadas, nenhuma página será verificada.

- **Lista Segura**

  As páginas podem ser excluídas da verificação pelos mecanismos do Bitdefender. No campo correspondente, introduza o nome do website que deseja adicionar à lista e, em seguida, clique em **ADICIONAR**.

  Nenhum aviso será exibido caso ameaças estejam presentes nas páginas excluídas. É por isso que apenas as páginas que confia totalmente devem ser adicionadas a esta lista.

Classificação de página e alertas

Dependendo de como o TrafficLight classifica a página que está a ver, é apresentado um dos seguintes ícones nessa área:

Esta página é segura. Pode continuar com o seu trabalho.
Esta página web pode conter conteúdo perigoso. Tenha cuidado se decidir visitá-la.
Deve sair da página imediatamente, pois contém malware ou outras ameaças.

No Safari, o fundo dos ícones do TrafficLight é preto.

9.8. Atualizações

Todos os dias são encontradas e identificadas novas ameaças. É por isto que é muito importante manter Bitdefender Antivirus for Mac atualizado com as atualizações de informação mais recentes.

Mantenha o **Autopilot** ligado para permitir que as informações sobre as ameaças e as atualizações do produto sejam transferidas automaticamente para o seu sistema. Se forem detectadas actualizações, serão automaticamente descarregadas e instaladas no seu computador.

As atualizações de informações sobre as ameaças são executadas na hora, ou seja, os ficheiros que precisam de ser atualizados são substituídos progressivamente. Dessa forma, a atualização não afetará a operação do produto e, ao mesmo tempo, qualquer vulnerabilidade será eliminada.

- Se o Bitdefender Antivirus for Mac estiver atualizado, pode detetar as ameaças mais recentes descobertas e limpar os ficheiros infetados.
- Se o Bitdefender Antivirus for Mac não estiver atualizado, não poderá detetar e remover as ameaças mais recententemente descobertas pelos laboratórios da Bitdefender.

9.8.1. Solicitar uma Actualização

Pode solicitar uma atualização manualmente sempre que quiser.

É necessária uma ligação à Internet ativa para verificar atualizações disponíveis e transferi-las.

Para solicitar uma atualização manualmente:

1. Abrir o Bitdefender Antivirus for Mac.
2. Clique no botão **Ações** na barra de menu.
3. Escolha **Atualizar base de dados de vírus**.

Em alternativa, pode solicitar uma atualização manualmente ao premir CMD + U.

Pode ver o progresso de atualização e ficheiros transferidos.

9.8.2. A obter atualizações através de um servidor proxy

O Bitdefender Antivirus for Mac só pode ser atualizado através de servidores proxy que não requerem autenticação. Não precisa de modificar quaisquer definições do programa.

Caso se ligue à Internet através de um servidor proxy que requer autenticação, é necessário mudar para uma ligação direta regularmente para obter atualizações de informações sobre as ameaças.

9.8.3. Atualizar para uma nova versão

Ocasionalmente, lançamos atualizações do produto para adicionar novas funcionalidades e melhorias ou reparar problemas. Estas atualizações podem exigem um reinício do sistema para iniciar a instalação de ficheiros novos.

Por predefinição, se uma atualização requer a reinicialização do sistema, o Bitdefender Antivirus for Mac continuará a trabalhar com os ficheiros anteriores até reiniciar o sistema. Neste caso, o processo de atualização não interferirá com o trabalho do utilizador.

Quando uma atualização do produto é concluída, uma janela pop-up irá informar para reiniciar o sistema. Se perder a notificação, pode clicar em **Reiniciar para atualizar** na barra de menus ou reiniciar o sistema manualmente.

9.8.4. Encontrar informações sobre o Bitdefender Antivirus for Mac

Para mais informações sobre a versão do Bitdefender Antivirus for Mac que tem instalada, aceda à janela **Informações**. Na mesma janela, pode obter acesso e visualizar as licenças de código aberto do Contrato de Subscrição e a Política de Privacidade.

Para aceder à janela Sobre:

1. Abrir o Bitdefender Antivirus for Mac.
2. Clique em Bitdefender Antivirus for Mac na barra de menus e escolha **Sobre o antivírus para Mac**.

10. CONFIGURAR PREFERÊNCIAS

Este capítulo inclui os seguintes tópicos:

- "*Aceder às preferências*" (p. 243)
- "*Info da conta*" (p. 243)
- "*Preferências de proteção*" (p. 244)
- "*Exclusões de Análise*" (p. 245)
- "*Safe Files*" (p. 246)
- "*Histórico*" (p. 248)
- "*Quarentena*" (p. 249)

10.1. Aceder às preferências

Para abrir a janela de preferências do Bitdefender Antivirus for Mac:

1. Abrir o Bitdefender Antivirus for Mac.
2. Faça uma das coisas seguintes:
   - Clique em Bitdefender Antivirus for Mac na barra de menus e escolha **Preferências**.
   - Clique no ícone na barra de menus e escolha **Preferências**.
   - Prima Command-Vírgula(,).

10.2. Info da conta

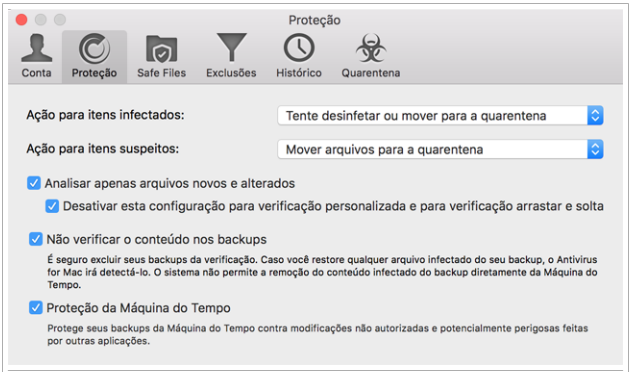
A janela de informações da conta contém detalhes sobre a sua subscrição e a sua conta Bitdefender.

Sempre que pretender iniciar sessão com outra conta Bitdefender, clique no botão **Trocar de conta**, insira o seu novo endereço de email e palavra-passe na janela da conta Bitdefender e clique em **ENTRAR**.

A partir desta janela, é possível desmarcar ou selecionar a opção **As minhas ofertas**. Ao permitir esta opção, as notificações serão exibidas sempre que Bitdefender tiver uma oferta especial para si.

10.3. Preferências de proteção

As preferências de proteção permitem que configure a abordagem geral de análise. Pode configurar as ações para ficheiros infectados e suspeitos detetados e outras definições gerais.

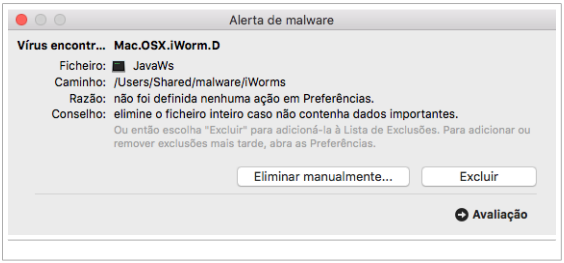


Preferências de proteção

- **Ação para os itens infectados.** Quando deteta uma ameaça, o Bitdefender Antivirus for Mac irá tentar remover automaticamente o código malicioso do ficheiro e reconstruir o ficheiro original. Esta operação é designada por desinfecção. Os ficheiros que não podem ser desinfetados são movidos para a quarentena para conter a infeção.

  Embora não seja recomendado, pode configurar a aplicação para não tomar qualquer ação com ficheiros infetados. Os ficheiros detetados são apenas registados.

  O Autopilot garante uma boa proteção contra ameaças com um impacto mínimo no desempenho do sistema. Se houver ameaças não resolvidas, pode vê-las e decidir o que fazer com elas.



- **Ação para itens suspeitos.** Os ficheiros são detectados como suspeitos pela análise heurística. Não foi possível desinfectar os ficheiros suspeitos por não estar disponível uma rotina de desinfecção.

  Por predefinição, os ficheiros suspeitos são movidos para a quarentena. Quando uma ameaça se encontra na quarentena não pode provocar nenhum mal, porque não pode ser nem lida nem executada.

  Se preferir, pode optar por ignorar ficheiros suspeitos. Os ficheiros detetados são apenas registados.

- **Analisar só ficheiros alterados.** Selecione esta caixa para configurar o Bitdefender Antivirus for Mac para analisar apenas ficheiros que não foram analisados anteriormente ou que foram modificados desde a última análise.

  Pode optar por não aplicar esta definição para a análise ao arrastar&largar ao selecionar a caixa correspondente.

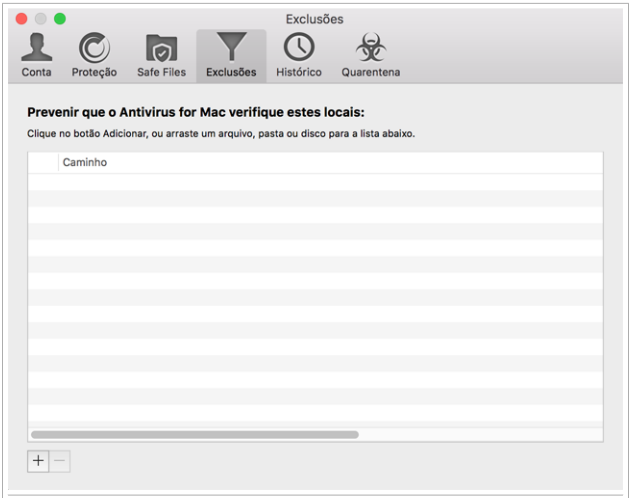
- **Não verificar o conteúdo nas cópias.** Selecione esta caixa para eliminar os ficheiros de cópia de segurança da análise. Se os ficheiros infetados forem restaurados posteriormente, o Bitdefender Antivirus for Mac os detetará automaticamente e tomará a ação necessária.

- **Proteção da Máquina do Tempo.** Selecione esta caixa de verificação para proteger os ficheiros armazenados na Máquina do Tempo. Caso os ficheiros da sua unidade da Máquina do Tempo sejam encriptados por ransomware, será capaz de recuperá-los sem pagar pelo resgate.

10.3.1. Exclusões de Análise

Se quiser, pode configurar o Bitdefender Antivirus for Mac para não analisar ficheiros, pastas ou até mesmo um volume inteiro específicos. Por exemplo, pode pretender eliminar da análise:

- Ficheiros que são erroneamente identificados como infetados (conhecidos como falsos positivos)
- Ficheiros que causam erros de análise
- Volumes de cópia de segurança



Exclusões de Análise

A lista de exclusões contém os caminhos que foram excluídos da análise.

Há duas formas de configurar uma exclusão de análise:

- Arraste&largue um ficheiro, pasta ou volume na lista de exclusões.
- Clique no botão com o sinal mais (+), localizado sob a lista de exclusões. Em seguida, escolha o ficheiro, pasta ou volume a ser excluído da análise.

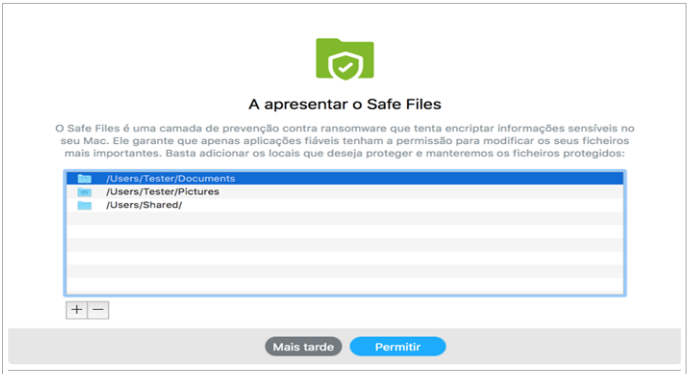
Para remover uma exclusão de análise, selecione-a na lista e clique no botão com o sinal menos (-), localizado na lista de exclusões.

10.4. Safe Files

Ransomwares são softwares maliciosos que atacam sistemas vulneráveis bloqueando-os e exigindo dinheiro para permitir que o utilizador volte a ter controlo do seu sistema. Este software malicioso finge ser inteligente ao exibir mensagens falsas para assustar o utilizador, persuadindo-o a realizar o pagamento solicitado.

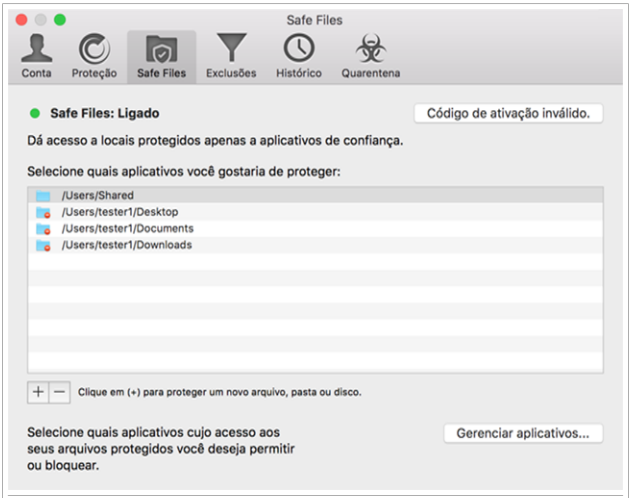
Utilizando a tecnologia mais recente, a Bitdefender assegura a integridade do sistema ao proteger as áreas críticas do sistema contra ataques de ransomware sem ter impacto no sistema. Contudo, também pode querer proteger os seus ficheiros pessoais, tais como documentos, fotografias ou filmes, contra o acesso de aplicações não fiáveis. Com o Safe Files

Bitdefender, pode colocar os ficheiros pessoais num local seguro e definir as aplicações que têm ou não permissão para realizar alterações nos ficheiros protegidos.



Assistente de Safe Files

O assistente de Safe Files Bitdefender é exibido assim que instala o Bitdefender Antivirus for Mac no seu Macintosh. Selecione ou adicione novas localizações que pretende proteger e, em seguida, clique em **Ativar Safe Files**.



Safe Files

Existem duas formas de adicionar ficheiros posteriormente ao ambiente protegido:

- Arraste&largue um ficheiro, pasta ou volume na janela Safe Files.
- Clique no botão com o sinal mais (+), localizado sob a lista de ficheiros protegidos. Em seguida, escolha o ficheiro, pasta ou volume a proteger no caso de ataques de ransomware que tentam aceder aos mesmos.

Para evitar o abrandamento do sistema, recomendamos que adicione no máximo 30 pastas ou guarde vários ficheiros numa única pasta.

Por predefinição, as pastas Imagens, Documentos, Ambiente de Trabalho e Transferências estão protegidas contra ataques de ameaças.

Nota
Pastas personalizadas apenas podem ser protegidas para os utilizadores atuais. Unidades externas, ficheiros do sistema e de aplicações não podem ser adicionados ao ambiente de proteção.

Será informador sempre que uma aplicação desconhecida com um comportamento incomum tente modificar os ficheiros adicionados. Clique em **Permitir** ou **Bloquear** para adicioná-la à lista Gerir aplicações.

10.4.1. Gerir aplicações

As aplicações que tentam mudar ou apagar ficheiros protegidos podem ser sinalizadas como potencialmente inseguras e adicionadas à lista de aplicações bloqueadas. Se a aplicação for bloqueada e se tiver a certeza que o seu comportamento é normal, pode autorizá-la ao clicar no botão **Gerir aplicações**, em seguida, alterar o seu estado para Permitida.

As aplicações definidas como Permitidas também podem ser definidas como Bloqueadas.

Utilize o método arraste&largar ou clique no sinal positivo (+) para adicionar mais aplicações à lista.

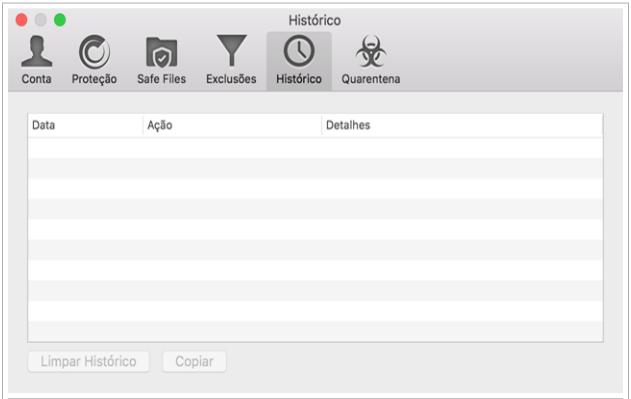
10.5. Histórico

O Bitdefender mantém um registo detalhado dos eventos relacionados com a sua atividade no seu computador. Sempre que acontece algo relevante para a segurança do seu sistema ou dados, é adicionada uma nova

mensagem ao Histórico do Bitdefender Antivirus for Mac, de forma semelhante a um novo e-mail a aparecer na sua caixa de entrada.

Os eventos são uma ferramenta importante na monitorização e gestão da proteção do seu Bitdefender. Por exemplo, pode verificar facilmente se a atualização foi levada a cabo com sucesso, se foi encontrada uma ameaça no seu computador, se uma aplicação não autorizada tentar aceder à sua unidade da Máquina do tempo, etc.

São apresentados detalhes sobre a atividade do produto.



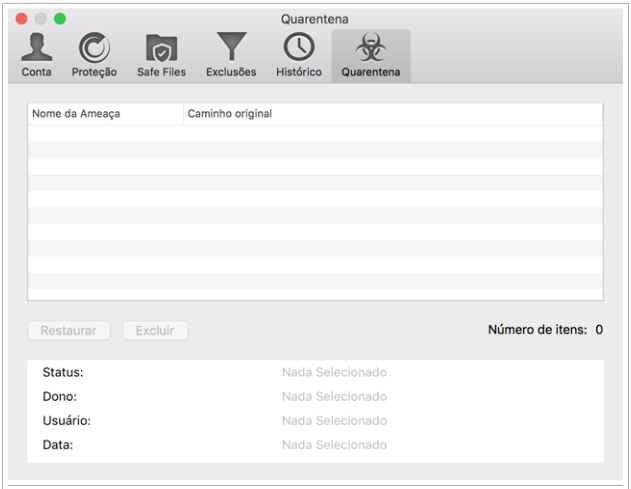
Histórico

Quando pretender eliminar o histórico, clique no botão **Limpar Histórico**.

O botão **Copiar** possibilita a cópia destas informações para a área de transferência.

10.6. Quarentena

O Bitdefender Antivirus for Mac permite o isolamento de ficheiros infectados ou suspeitos numa área segura, chamada de quarentena. Quando uma ameaça se encontra na quarentena não pode provocar nenhum mal, porque não pode ser nem lida nem executada.



Ficheiros em quarentena

A secção de Quarentena mostra todos os ficheiros actualmente isolados na pasta da Quarentena.

Para eliminar um ficheiro da quarentena, selecione-o e clique em **Eliminar**. Se pretende restaurar um ficheiro da quarentena para a respetiva localização original, selecione-o e clique em **Restaurar**.

11. VPN

Este capítulo inclui os seguintes tópicos:

- "*Sobre a VPN*" (p. 251)
- "*A instalar a VPN*" (p. 251)
- "*A abrir a VPN*" (p. 252)
- "Interface da VPN" (p. 252)
- "*Assinaturas*" (p. 272)

11.1. Sobre a VPN

Com o Bitdefender VPN , pode manter os seus dados privados sempre que se ligar a redes sem fios não seguras em aeroportos, shoppings, cafés ou hotéis. Assim, poderá evitar situações inoportunas, como roubo de dados pessoais ou tentativas de tornar o endereço de IP do seu dispositivo acessível a hackers.

A VPN funciona como um túnel entre o seu dispositivo e a rede à qual se liga, protegendo a sua ligação, encriptando os seus dados utilizando uma encriptação de nível bancário e escondendo o seu endereço IP onde quer que esteja. O seu tráfego é redirecionado por meio de um servidor separado, tornando o seu dispositivo quase impossível de ser identificado entre os incontáveis dispositivos que usam os nossos serviços. Além disso, enquanto estiver ligado à Internet com o Bitdefender VPN, pode aceder a conteúdos que normalmente são restritos em áreas específicas.

Nota

Alguns países censuram a Internet e, portanto, a utilização de VPN nos seus territórios foi banida por lei. Para evitar consequências legais, pode ser apresentada uma mensagem de aviso ao tentar utilizar a aplicação Bitdefender VPN pela primeira vez. Ao continuar a utilizar a funcionalidade, confirma que está ciente dos regulamentos aplicáveis e dos riscos aos quais pode estar exposto.

11.2. A instalar a VPN

A aplicação VPN pode ser instalada a partir da janela principal de Bitdefender como se segue:

1. Abrir o Bitdefender Antivirus for Mac.
2. Clique em **Obter agora** no canto inferior direito.
3. Na janela com a descrição da aplicação VPN, leia o **Contrato de subscrição** e clique em **Instalar VPN**. Se não concordar com estes termos, clique em **Mais tarde** para cancelar a instalação.
4. Clique em **Compreendi** para concluir o processo de instalação.

11.3. A abrir a VPN

Para abrir a aplicação VPN da Bitdefender, clique no ícone na barra de menu. Adicionalmente, pode aceder à pasta Aplicações, abrir a pasta Bitdefender e clicar duas vezes no ícone Bitdefender VPN.

11.4. Interface

A interface do VPN exibe o estado da aplicação, conectado ou desconectado. O local do servidor para utilizadores com a versão gratuita é determinado automaticamente pelo Bitdefender para o servidor mais adequado, enquanto os utilizadores Premium têm a possibilidade de alterar o local do servidor ao qual desejam se ligar selecionando-o na lista **SELECIONAR LOCAL**. Para detalhes sobre as subscrições de VPN, aceda a "*Assinaturas*" (p. 272).

Para ligar ou desligar, basta clicar no estado exibido no topo do ecrã. A barra de menu fica preta quando a VPN está conectada e branca quando a VPN está desconectada.

Interface do VPN

Enquanto estiver ligado, o tempo decorrido é mostrado na parte inferior da interface. Para aceder a mais opções, clique no ícone ⚙ no canto superior direito:

- **A minha conta** - detalhes sobre a sua conta Bitdefender e a subscrição do VPN são exibidos. Clique em **Trocar conta** se deseja entrar com outra conta.
- **Definições** - dependendo das suas necessidades, pode personalizar o comportamento do seu produto:
  - configure a VPN para que seja executada na inicialização do sistema
  - receba notificações quando a VPN se conectar ou desconectar automaticamente

- • **Atualizar para o Premium**: Se estiver a utilizar a versão gratuita, pode atualizar para o plano Premium aqui. Clique em **ATUALIZAR AGORA** para ser redirecionado para uma página da web de onde pode comprar uma subscrição.
- **Suporte** - é redirecionado para a nossa plataforma do Centro de Apoio onde poderá ler um artigo útil sobre como utilizar o Bitdefender VPN.
- **Sobre** - são apresentadas informações sobre a versão instalada.
- **Sair** - sai da aplicação.

11.5. Assinaturas

O Bitdefender VPN oferece gratuitamente 200 MB de franquia por dispositivo para proteger a sua ligação sempre que precisar, além de ligá-lo automaticamente ao melhor local de servidor.

Para obter tráfego ilimitado e acesso irrestrito a conteúdos no mundo inteiro escolhendo um local da sua preferência, atualize para a versão Premium.

Pode atualizar para a versão Bitdefender Premium VPN a qualquer momento ao clicar no botão **OBTER TRÁFEGO ILIMITADO** disponível na interface do produto.

A subscrição Bitdefender Premium da VPN é independente da subscrição do Bitdefender Antivirus for Mac, ou seja, poderá usá-la durante todo o seu período de disponibilidade, não importando o estado da subscrição da sua segurança. Caso a subscrição do Bitdefender Premium VPN expire, mas Bitdefender Antivirus for Mac continua ativa, voltará para o plano gratuito.

O Bitdefender VPN é um produto multiplataforma, disponível nos produtos Bitdefender compatíveis com Windows, macOS, Android e iOS. Quando atualizar para o plano Premium, poderá usar a sua subscrição em todos os seus produtos, desde que faça login com a mesma conta Bitdefender.

12. BITDEFENDER CENTRAL

Este capítulo inclui os seguintes tópicos:

- "*Sobre Bitdefender Central*" (p. 255)
- "*As minhas subscrições*" (p. 256)
- "*Meus dispositivos*" (p. 257)

12.1. Sobre Bitdefender Central

Bitdefender Central é a plataforma Web onde tem acesso às funcionalidades e serviços online do produto, e pode realizar remotamente tarefas importantes nos dispositivos em que o Bitdefender estiver instalado. Pode iniciar sessão na sua conta Bitdefender a partir de qualquer computador ou dispositivo móvel ligado à internet através https://central.bitdefender.com. Assim que tiver obtido acesso, pode realizar o seguinte:

- Transfira e instale o Bitdefender nos sistemas operativos Windows, macOS, iOS e Android. Os produtos disponíveis para download são:
  - Bitdefender Antivirus for Mac
  - A linha de produtos Windows da Bitdefender
  - Bitdefender Mobile Security para Android
  - Bitdefender Mobile Security for iOS
  - Consultor Parental Bitdefender
- Gerir e renovar as suas subscrições do Bitdefender.
- Adicionar novos dispositivos à sua rede e gerir as suas funcionalidades onde quer que esteja.

12.2. A aceder Bitdefender Central

Existem diversas formas de aceder à Bitdefender Central. Dependendo da tarefa que quiser realizar, pode utilizar qualquer uma das seguintes opções:

- A partir da interface principal do Bitdefender Antivirus for Mac:
  1. Clique na hiperligação **Ir para a sua conta** na parte inferior direita do ecrã.
- Do seu navegador Web:

1. Abrir um navegador em qualquer dispositivo com acesso à internet.
2. Vá para: https://central.bitdefender.com.
3. Inicie sessão na sua conta com o seu endereço de e-mail e palavra-passe.

12.3. As minhas subscrições

A plataforma da Bitdefender Central possibilita-lhe controlar facilmente as subscrições que possui para todos os seus dispositivos.

12.3.1. Ativar subscrição

Uma subscrição pode ser ativada durante o processo de instalação utilizando a sua conta Bitdefender. Juntamente com o processo de ativação, a validade da subscrição inicia a sua contagem decrescente.

Se tver comprado um código de ativação de um dos nossos revendedores ou o tiver recebido como presente, pode adicionar a sua disponibilidade à sua subscrição do Bitdefender.

Para ativar uma subscrição com um código de ativação, siga os passos abaixo:

1. Aceda Bitdefender Central.
2. Clique no ícone ☰ localizado no canto superior esquerdo da janela e selecione o painel **As minhas subscrições**.
3. Clique no botão **CÓDIGO DE ATIVAÇÃO** e, em seguida, escreva o código no campo correspondente.
4. Clique em **ATIVAR** para continuar.

A subscrição está ativada agora.

Para começar a instalar o produto nos seus dispositivos, consulte "*A instalar Bitdefender Antivirus for Mac*" (p. 222).

12.3.2. Comprar assinatura

Pode comprar uma subscrição diretamente a partir da sua conta Bitdefender seguindo os seguintes passos:

1. Aceda Bitdefender Central.

2. Clique no ícone ☰ localizado no canto superior esquerdo da janela e selecione o painel **As minhas subscrições**.
3. Clique na hiperligação **Comprar Agora**. Será redirecionado para uma página da Web de onde poderá fazer a compra.

Assim que finalizar o processo, a disponibilidade da subscrição fica visível no canto inferior direito da interface principal do produto.

12.4. Meus dispositivos

A seção **Meus dispositivos** na sua conta Bitdefender permite-lhe instalar, gerir e realizar ações remotas no seu Bitdefender em qualquer dispositivo, desde que esteja ativado e ligado à Internet. Os cartões de dispositivos exibem o nome do dispositivo, o estado da proteção e se há algum risco de segurança afetando a proteção dos seus dispositivos.

12.4.1. Personalize o seu dispositivo

Para identificar facilmente os seus dispositivos, pode personalizar o nome de cada um:

1. Aceda Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.
3. Clique no cartão de dispositivo pretendido e, em seguida, o ícone ⋮ no canto superior direito do ecrã.
4. Selecione **Definições**.
5. Digite um novo nome no campo **Nome do dispositivo** e clique **GUARDAR**.

Pode criar e atribuir um proprietário a cada um dos seus dispositivos para uma melhor gestão:

1. Aceda Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.
3. Clique no cartão de dispositivo pretendido e, em seguida, o ícone ⋮ no canto superior direito do ecrã.
4. Selecione **Perfil**.

5. Clique em **Add owner** e, em seguida, preencha os respetivos campos. Personalize o perfil adicionando uma fotografia e selecionando a data de nascimento, além de um e-mail e número de telefone.
6. Clique em **ADICIONAR** para guardar o perfil.
7. Selecione o proprietário pretendido na lista **Proprietário do dispositivo** e, em seguida, clique em **ATRIBUIR**.

12.4.2. Ações remotas

Para atualizar o Bitdefender remotamente no dispositivo:

1. Aceda Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.
3. Clique no cartão de dispositivo pretendido e, em seguida, o ícone ⋮ no canto superior direito do ecrã.
4. Selecione **Atualizar**.

Para ativar remotamente o recurso de Autopilot:

1. Aceda Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.
3. Clique no cartão de dispositivo pretendido e, em seguida, o ícone ⋮ no canto superior direito do ecrã.
4. Selecione **Definições**. Clique no botão correspondente para ativar o Autopilot.

Quando clicar no cartão de dispositivo, ficam disponíveis os seguintes separadores:

- **Painel**. Nesta janela, pode visualizar os detalhes sobre o dispositivo selecionado, verificar o seu estado de proteção e quantas ameaças foram bloqueadas nos últimos sete dias. O estado de proteção pode estar verde, quando não houver problemas a afetar o seu dispositivo, amarelo, quando o dispositivo exigir a sua atenção, ou vermelho, quando o dispositivo estiver em risco. Quando houver problemas a afetar o seu dispositivo, clique no seta pendente na área de estado acima para saber mais detalhes. A partir daqui poderá resolver manualmente os problemas que afetam a segurança dos seus dispositivos.

- **Proteção**. A partir desta janela, pode realizar remotamente uma Análise Rápida ou Completa nos seus dispositivos. Clique no botão **VERIFICAR** para iniciar o processo. Também pode conferir quando é que a última verificação foi realizada no dispositivo e aceder a um relatório da última verificação, contendo as informações mais importantes. Para mais informações sobre esses dois processos de análise, consulte "*Analisar o seu Mac*" (p. 234).

13. PERGUNTAS FREQUENTES

Como posso experimentar o Bitdefender Antivirus for Mac antes de fazer a subscrição?

É um novo cliente Bitdefender e gostaria de experimentar o nosso produto antes de o comprar. O período de avaliação é de 30 dias e pode continuar a utilizar o produto instalado apenas se comprar uma subscrição Bitdefender. Para avaliar o Bitdefender Antivirus for Mac, precisa de:

1. Criar uma conta Bitdefender seguindo os seguintes passos:
   - Vá para: https://central.bitdefender.com.
   - Escreva as informações necessárias nos campos correspondentes e, em seguida, clique no botão **CRIAR CONTA**.

     Os dados que nos fornecer serão mantidos confidenciais.
2. Transfira o Bitdefender Antivirus for Mac como se segue:
   - Selecione o painel **Os meus dispositivos**, e clique em **INSTALAR PROTEÇÃO LOCAL**.
   - Escolha uma das duas opções disponíveis:
     - **DOWNLOAD**

       Clique no botão e guarde o ficheiro de instalação.
     - **Noutro dispositivo**

       Selecione **macOS X** para transferir o seu produto Bitdefender e clique em **CONTINUAR**. Escreva um endereço de e-mail no campo correspondente e clique em **ENVIAR**.
   - Execute o Bitdefender que transferiu.

Tenho um código de ativação. Como adiciono a sua validade à minha subscrição?

Se tver comprado um código de ativação de um dos nossos revendedores ou o tiver recebido como presente, pode adicionar a sua disponibilidade à sua subscrição do Bitdefender.

Para ativar uma subscrição com um código de ativação, siga os passos abaixo:

1. Aceda Bitdefender Central.

2. Clique no ícone ☰ localizado no canto superior esquerdo da janela e selecione o painel **As minhas subscrições**.
3. Clique no botão **CÓDIGO DE ATIVAÇÃO** e, em seguida, escreva o código no campo correspondente.
4. Clique em **ATIVAR** para continuar.

A extensão está agora visível na sua conta Bitdefender e no seu produto Bitdefender Antivirus for Mac instalado, na parte inferior direita do ecrã.

O registo de análise indica que ainda há itens não resolvidos. Como os removo?

Os itens não resolvidos no registo de análise podem ser:

- ficheiros de acesso restrito (xar, rar, etc.)

  Solução: utilize a opção **Revelar no Finder** para encontrar o ficheiro e eliminá-lo manualmente. Não se esqueça de esvaziar a Reciclagem.

- caixas de correio de acesso restrito (Thunderbird, etc.)

  Solução: utilize a aplicação para remover a entrada que contém o ficheiro infetado.

- O conteúdo nas cópias

  Solução: ative a opção **Não verificar o conteúdo nas cópias** nas Preferências de proteção ou selecione **Adicionar às Exclusões** para ficheiros detetados.

  Se os ficheiros infetados forem restaurados posteriormente, o Bitdefender Antivirus for Mac os detetará automaticamente e tomará a ação necessária.

> **Nota**
> Ficheiros de acesso restrito significam que o Bitdefender Antivirus for Mac só os pode abrir, mas não pode modificá-los.

Onde posso ver detalhes sobre a atividade do produto?

O Bitdefender mantém um registo de todas as ações importantes, mudanças de estado e outras mensagens críticas relacionadas com a sua atividade. Para aceder a estas informações, abra a janela de preferências do Bitdefender Antivirus for Mac:

1. Abrir o Bitdefender Antivirus for Mac.

2. Faça uma das coisas seguintes:
   - Clique em Bitdefender Antivirus for Mac na barra de menus e escolha **Preferências**.
   - Clique no ícone na barra de menus e escolha **Preferências**.
   - Prima Command-Vírgula(,).
3. Escolha o separador **Histórico**.

   São apresentados detalhes sobre a atividade do produto.

Posso atualizar o Bitdefender Antivirus for Mac através de um servidor proxy?

O Bitdefender Antivirus for Mac só pode ser atualizado através de servidores proxy que não requerem autenticação. Não precisa de modificar quaisquer definições do programa.

Caso se ligue à Internet através de um servidor proxy que requer autenticação, é necessário mudar para uma ligação direta regularmente para obter atualizações de informações sobre as ameaças.

Como posso remover o Bitdefender Antivirus for Mac?

Para remover o Bitdefender Antivirus for Mac, siga os seguintes passos:

1. Abra uma janela **Finder** e aceda à pasta Aplicações.
2. Abra a empresa Bitdefender e clique duas vezes em DesinstalarBitdefender.
3. Clique em **Desinstalar** e aguarde pela conclusão do processo.
4. Clique em **Fechar** para terminar.

> **!** **Importante**
> Se ocorrer um erro, pode entrar em contacto com o Atendimento ao Consumidor da Bitdefender, como descrito em "*Pedir Ajuda*" (p. 325).

Como removo as extensões do TrafficLight do meu browser?

- Para remover as extensões do TrafficLight do Mozilla Firefox, siga estes passos:
  1. Abra o seu browser Mozilla Firefox.
  2. Aceda a **Ferramentas** e selecione **Suplementos**.
  3. Selecione **Extensões** na coluna da esquerda.
  4. Selecione a extensão e clique em **Remover**.

5. Reinicie o browser para concluir o processo de remoção.

- Para remover as extensões do TrafficLight do Google Chrome, siga estes passos:

  1. Abra o seu browser Google Chrome.
  2. Na parte superior direita, clique em **Mais** .
  3. Aceda a **Mais Ferramentas** e selecione **Extensões**.
  4. Clique no ícone **Remover do Chrome...** ao lado da extensão que deseja remover.
  5. Clique em **Desinstalar** para confirmar o processo de remoção.

- Para remover o Bitdefender TrafficLight do Safari, siga estes passos:

  1. Abra o seu browser Safari.
  2. Clique em na barra de ferramentas do browser e clique em **Preferências**.
  3. Selecione o separador **Extensões** e localize a extensão **Bitdefender TrafficLight no Safari** na lista.
  4. Selecione a extensão e clique em **Desinstalar**.
  5. Clique em **Desinstalar** para confirmar o processo de remoção.

Quando devo usar o Bitdefender VPN?

Tem de ter cuidado quando aceder, transferir ou enviar conteúdos na internet. Para garantir que fica em segurança enquanto navega na Web, recomendamos que utilize o Bitdefender VPN quando:

- quiser ligar-se a redes sem fios públicas
- quiser aceder a conteúdos que normalmente são restritos em áreas específicas, não importa se estiver em casa ou fora
- quiser manter os seus dados pessoais privados (nomes de utilizador, palavras-passe, informações de cartão de crédito, etc.)
- desejar esconder o seu endereço IP

O Bitdefender VPN vai ter um impacto negativo na bateria do meu dispositivo?

O Bitdefender VPN foi concebido para proteger os seus dados pessoais, esconder o seu endereço IP enquanto estiver ligado a redes sem fios

não seguras e aceder a conteúdo restrito em certos países. Para evitar um consumo desnecessário de bateria do seu dispositivo, recomendamos que use o VPN apenas quando precisar, e que o desconecte quando estiver offline.

Por que estou a deparar-me com lentidão na Internet enquanto uso o Bitdefender VPN?

O Bitdefender VPN foi concebido para suavizar a sua experiência enquanto navega na Internet. No entanto, a lentidão pode ser causada pela sua conectividade com a internet ou pela distância do servidor ao qual está ligado. Nesse caso, se não for uma necessidade ligar a um servidor distante com respeito à sua localização (por exemplo, dos EUA ou China), recomendamos que permita ao Bitdefender VPN ligá-lo automaticamente ao servidor mais próximo, ou encontrar um servidor próximo da sua localização atual.

MOBILE SECURITY PARA IOS

14. EM QUE CONSISTE O BITDEFENDER MOBILE SECURITY FOR IOS

Atividades online, como pagar contas, fazer reservas para as férias ou comprar bens e serviços são convenientes e práticas. Mas, como muitas atividades realizadas na Internet, fazem-se acompanhar de elevados riscos e, se os detalhes de segurança forem ignorados, os dados pessoais podem ser hackeados. E o que é mais importante do que proteger os dados armazenados em contas online e no seu smartphone?

O Bitdefender Mobile Security for iOS permite:

- Proteja os seus dados ao ligar-se a redes sem fios não seguras.
- Verificar se houve fugas nas contas online que utiliza diariamente.
- Localizar, bloquear e limpar os dados do dispositivo em caso de roubo ou perda.

O Bitdefender Mobile Security for iOS é entregue gratuitamente e requer a ativação com uma conta Bitdefender.

15. INTRODUÇÃO

Requisitos do Aparelho

O Bitdefender Mobile Security for iOS funciona em iPhone com iOS 10 ou superior e necessita de uma ligação à Internet para ser ativado e detetar quaisquer fugas de dados nas suas contas online.

A instalar Bitdefender Mobile Security for iOS

- **Da Bitdefender Central**
  - Em iOS
    1. Vá para: https://central.bitdefender.com.
    2. Iniciar sessão na sua conta Bitdefender.
    3. Pressione o ícone ☰ no canto superior esquerdo do ecrã e, em seguida, selecione **Os meus dispositivos**.
    4. Toque **INSTALAR PROTEÇÃO LOCAL**.
    5. Selecione Bitdefender Mobile Security da lista, em seguida, toque em **ACEDER A APP STORE**.
    6. Toque **INSTALAR** no ecrã da App Store.
  - No Windows, macOS e Android
    1. Vá para: https://central.bitdefender.com.
    2. Iniciar sessão na sua conta Bitdefender.
    3. Pressione o ícone ☰ no canto superior esquerdo do ecrã e, em seguida, selecione **Os meus dispositivos**.
    4. Pressione **INSTALAR PROTEÇÃO LOCAL** .
    5. No Windows e macOS, clique no link **Em outro dispositivo**.

       No Android, pressione **Deseja proteger outros dispositivos?**.
    6. Escolha **iOS**.
    7. Selecione **Segurança Móvel Bitdefender** da lista, em seguida, toque em **CONTINUAR**.

8. Escreva um endereço de e-mail no campo correspondente e toque em **ENVIAR**.
9. Aceda à sua conta de e-mail a partir do seu dispositivo iOS e toque em **OBTER NA AppStore** no e-mail recebido dos nossos servidores.

   Vai ser redirecionado para a aplicação da **App Store**.
10. Toque **INSTALAR** no ecrã da App Store.

- **Na App Store**

  Pesquise por Bitdefender Mobile Security for iOS para localizar e instalar a aplicação.

Para concluir o processo de instalação, tem de concordar com o Contrato de Subscrição. Leia o Contrato de Subscrição com calma pois contém os termos e condições que regem a utilização do Bitdefender Mobile Security for iOS.

Toque em **Continuar** para avançar para a janela seguinte.

Iniciar sessão na sua conta Bitdefender

Para utilizar o Bitdefender Mobile Security for iOS, deve associar o seu dispositivo a uma conta Bitdefender do Facebook, Google ou Microsoft iniciando sessão na conta a partir da aplicação. A primeira vez que abrir a aplicação, será pedido que inicie sessão numa conta.

Para associar o seu dispositivo a uma conta Bitdefender:

1. Introduza o endereço de e-mail e palavra-passe da sua conta Bitdefender nos campos correspondentes. Caso não tenha uma conta Bitdefender e deseje criar uma, pressione o link correspondente para criar uma.
2. Pressione **ENTRAR**.

Para entrar usando uma conta do Facebook, Google ou Microsoft, pressione o serviço que deseja usar na área **OU ENTRAR COM**. Será redirecionado para a página de login do serviço selecionado. Siga as instruções para vincular a sua conta ao Bitdefender Mobile Security for iOS.

> **Nota**
> O Bitdefender não obtém acesso a qualquer informação confidencial como a palavra-passe da conta que usa para iniciar sessão ou a informação particular dos seus amigos ou contactos.

Assistente

Um assistente introdutório com detalhes sobre as funções do produto é apresentado na primeira vez que abre a aplicação. Selecione **SEGUINTE** para continuar a ser guiado ou **Ignorar** para fechar o assistente.

Painel

Toque no ícone do Bitdefender Mobile Security for iOS na secção de aplicações do seu dispositivo para abrir a interface da aplicação.

Na primeira vez que abrir a aplicação, será solicitado a permitir ao Bitdefender o envio de notificações. Prima **Permitir** para permanecer informado sempre que o Bitdefender tiver de comunicar algo relevante para a sua aplicação. Para gerir as notificações do Bitdefender, aceda a Definições > Notificações > Segurança móvel.

Para aceder às informações necessárias, toque no ícone correspondente na parte inferior do ecrã.

VPN

Encripta a comunicação na Internet, ajudando-o a manter a sua privacidade, não importando a rede à qual está ligado. Para mais informação, dirija-se a "*VPN*" (p. 271).

Privacidade de conta

Saiba se as suas contas de e-mail foram invadidas ou não. Para mais informação, dirija-se a "*Privacidade de conta*" (p. 274).

Anti-Theft

Localize e bloqueie o seu dispositivo para evitar que os seus dados pessoais caiam nas mãos erradas. Para mais informação, dirija-se a "*Funcionalidades Anti Furto*" (p. 276).

Para ver mais opções, toque no ícone no dispositivo enquanto estiver no ecrã inicial da aplicação. São apresentadas as seguintes opções:

- Restaurar compras - aqui pode restaurar para a subscrição Premium VPN que comprou através da conta iTunes.
- Introdução — aqui pode aceder à apresentação rápida do produto.
- Comentários — aqui pode iniciar o cliente de e-mail predefinido para nos enviar comentários sobre a aplicação.

- Informações sobre a aplicação — aqui tem acesso a informações sobre a versão instalada e o Contrato de Subscrição, Política de Privacidade e conformidade com licenças de código aberto.

16. VPN

Com o Bitdefender VPN , pode manter os seus dados privados sempre que se ligar a redes sem fios não seguras em aeroportos, shoppings, cafés ou hotéis. Assim, poderá evitar situações inoportunas, como roubo de dados pessoais ou tentativas de tornar o endereço de IP do seu dispositivo acessível a hackers.

A VPN funciona como um túnel entre o seu dispositivo e a rede à qual se liga, protegendo a sua ligação, encriptando os seus dados utilizando uma encriptação de nível bancário e escondendo o seu endereço IP onde quer que esteja. O seu tráfego é redirecionado por meio de um servidor separado, tornando o seu dispositivo quase impossível de ser identificado entre os incontáveis dispositivos que usam os nossos serviços. Além disso, enquanto estiver ligado à Internet com o Bitdefender VPN, pode aceder a conteúdos que normalmente são restritos em áreas específicas.

Nota
Alguns países censuram a Internet e, portanto, a utilização de VPN nos seus territórios foi banida por lei. Para evitar consequências legais, pode ser apresentada uma mensagem de aviso ao tentar utilizar a funcionalidade Bitdefender VPN pela primeira vez. Ao continuar a utilizar a funcionalidade, confirma que está ciente dos regulamentos aplicáveis e dos riscos aos quais pode estar exposto.

Para ativar o Bitdefender VPN:

1. Toque no ícone na parte inferior do ecrã.
2. Pressione **Ligarr** sempre que quiser permanecer protegido enquanto estiver ligado às redes sem fios não seguras.

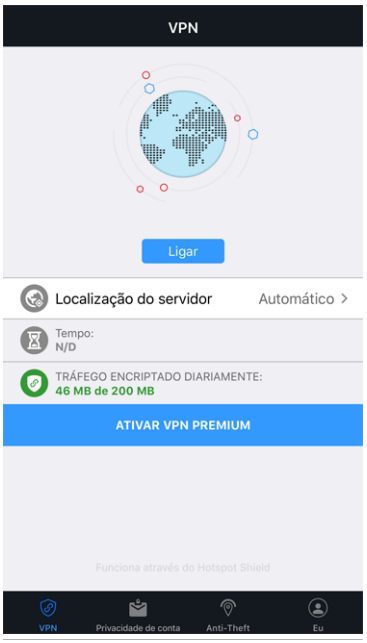
   Pressione **Desconectar** quando desejar desativar a ligação.

Nota
Na primeira vez que ligar o VPN, será solicitado a permitir que o Bitdefender faça configurações de VPN que monitorizarão o tráfego de rede. Prima **Permitir** para continuar. Se tiver sido configurado um método de autenticação (leitura de digital ou código PIN) para proteger o seu smartphone, será solicitado que o utilize.

O ícone VPN aparece na barra de estado quando a VPN está ativa.

Para economizar bateria, recomendamos que desligue a VPN quando não precisar de usá-la.

Se tiver uma subscrição Premium e quiser ligar-se a um servidor da sua escolha, pressione **Localização do Servidor** na interface da VPN e depois selecione o local desejado. Para detalhes sobre as subscrições de VPN, aceda a "*Assinaturas*" (p. 272).



VPN

16.1. Assinaturas

O Bitdefender VPN oferece gratuitamente 200 MB de franquia por dispositivo para proteger a sua ligação sempre que precisar, além de ligá-lo automaticamente ao melhor local de servidor.

Para obter tráfego ilimitado e acesso irrestrito a conteúdos no mundo inteiro escolhendo um local da sua preferência, atualize para a versão Premium.

Pode atualizar para a versão Bitdefender Premium VPN a qualquer momento, pressionando o botão **ATIVAR VPN PREMIUM** disponível na janela da VPN.

A subscrição Bitdefender Premium VPN é independente da subscrição grátis do Bitdefender Mobile Security for iOS, ou seja, poderá usá-lo por todo o seu período de disponibilidade. Caso a subscrição Bitdefender Premium VPN expire, voltará automaticamente para o plano gratuito.

O Bitdefender VPN é um produto multiplataforma, disponível nos produtos Bitdefender compatíveis com Windows, macOS, Android e iOS. Quando atualizar para o plano Premium, poderá usar a sua subscrição em todos os seus produtos, desde que faça login com a mesma conta Bitdefender.

17. PRIVACIDADE DE CONTA

A Privacidade de Conta Bitdefender deteta se houve fuga de dados nas contas que utiliza para fazer pagamentos online, compras ou iniciar sessão em diferentes aplicações ou sites Web. Os dados armazenados numa conta podem ser palavras-passe, informações de cartão de crédito ou informações de conta bancária e, se não forem devidamente protegidos, pode sofrer roubo de identidade ou invasão de privacidade.

O estado de privacidade de uma conta é apresentado depois da validação.

Para verificar se qualquer conta foi invadida, toque em **Procurar fugas**.

Para começar a proteger informações pessoais:

1. Toque no ícone na parte inferior do ecrã.
2. Toque em **Adicionar** no canto superior direito do ecrã.
3. Digite o seu endereço de e-mail no campo correspondente e toque em **Seguinte**.

   Bitdefender necessita de validar esta conta antes de apresentar informações privadas. Portanto, é enviado um e-mail com um código de validação para o endereço de e-mail fornecido.
4. Verifique a caixa de entrada e digite o código recebido na área **Privacidade de Conta** da aplicação. Se não conseguir encontrar o e-mail de validação na pasta Caixa de Entrada, verifique a pasta Spam.

   O estado de privacidade da conta validada é apresentado.

Se forem detetadas fugas nas suas contas, recomendamos que altere as palavras-passe assim que possível. Para criar uma palavra-passe forte e segura, tenha em mente estas dicas:

- Oito carateres no mínimo.
- Carateres maiúsculos e minúsculos.
- Pelo menos um número ou símbolo, como #, @, % ou !.

Privacidade de conta

18. FUNCIONALIDADES ANTI FURTO

Bitdefender pode ajudá-lo a localizar o seu dispositivo e impedir que os seus dados pessoais caiam nas mãos erradas.

Tudo o que necessita de fazer é ativar o Anti-roubo a partir do dispositivo e, quando necessário, aceder à **Bitdefender Central** a partir de qualquer Web browser, em qualquer lugar.

Bitdefender Mobile Security for iOS oferece as seguintes funcionalidades Anti Furto:

Localização Remota
Veja a localização atual do seu dispositivo no Maps.

A precisão da localização depende do quanto o Bitdefender é capaz de o determinar:

- Caso o GPS esteja ativado no dispositivo, a sua localização pode ser determinada no alcance de dois metros, desde que esteja ao alcance dos satélites GPS (ou seja, fora de um edifício).
- Se o dispositivo estiver dentro de um edifício, a sua localização pode ser determinada no alcance de 10 metros caso o Wi-Fi esteja ativado e existam rede sem fios disponíveis no seu alcance.
- Caso contrário, a localização será determinada utilizando apenas as informações da rede móvel, que pode oferecer uma precisão não melhor que várias centenas de metros.

Bloqueio Remoto
Bloqueie o ecrã do seu dispositivo remotamente.

Limpeza Remota
Remova todos os dados pessoais do seu dispositivo roubado.

A ativar o Anti Furto

Ativar as funcionalidades Antirroubo:

1. Toque no ícone na parte inferior do ecrã.
2. Ative o botão.
3. Conceda acesso à localização do dispositivo para que o Bitdefender possa localizá-lo em caso de perda ou roubo. Esta notificação só é apresentada

quando ativa o Antirroubo do Bitdefender pela primeira vez. Para gerir o acesso do Bitdefender, aceda a Definições > Serviços de localização > Segurança móvel.

4. Na primeira vez que ativar o Antirroubo no seu dispositivo, também deve instalar um perfil MDM (gestão de dispositivos móveis). Portanto, continue com estes passos:

   a. Toque em **Permitir** para ser redirecionado para a área Definições.

   b. Toque em **Instalar** para instalar o perfil MDM (gestão de dispositivos móveis) necessário ao Bitdefender para continuar com o processo de ativação.

      Se tiver sido configurado um código PIN para proteger o seu smartphone, deve utilizá-lo.

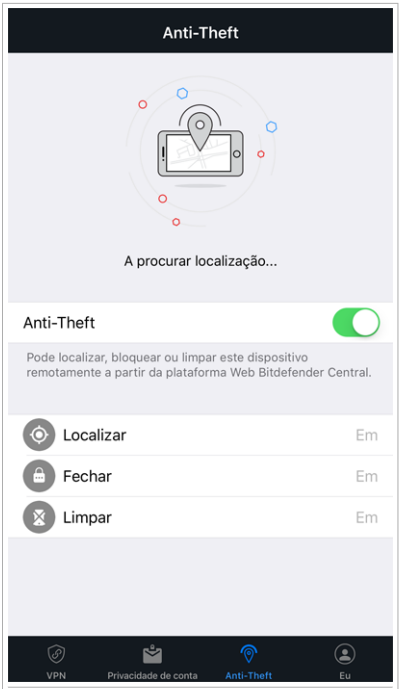
   c. Leia as informações associadas ao certificado raiz da AC e gestão de dispositivos móveis.

   d. Se concordar com os termos estabelecidos, toque em **Instalar**.

   e. Toque em **Confiar** no alerta de Gestão Remota e em **Concluído** para fechar a janela.

Nota

Se a instalação do perfil MDM do Bitdefender falhar, pode estar instalado um perfil MDM mais antigo e deve ser removido. Portanto, aceda a Definições > Geral > Gestão de dispositivos > Bitdefender. Selecione o perfil detetado e prima **Remover gestão**. Se tiver sido configurado um código PIN para proteger o seu smartphone, deve utilizá-lo. Prima **Remover gestão** novamente para confirmar a sua escolha. Tente novamente para ativar o Antirroubo. Se o problema persistir, envie um e-mail para a nossa equipa em bdios@bitdefender.com.



Anti-Theft

A utilizar as funcionalidades Anti Furto de Bitdefender Central (Controlo via Web)

Para aceder às funções anti-furto da sua conta Bitdefender:

1. Vá para: https://central.bitdefender.com.
2. Iniciar sessão na sua conta Bitdefender.
3. Pressione o ícone ☰ no canto superior esquerdo do ecrã e, em seguida, selecione **Os meus dispositivos**.
4. Toque no cartão de dispositivo desejado e no separador **Antirroubo**.
5. No último campo da janela, prima o ícone da função que pretende utilizar:

   Mostrar IP - exibe o último endereço de IP para o dispositivo selecionado.
   Localizar - apresenta a localização do seu dispositivo no Maps.

Bloquear - bloqueie o seu dispositivo e defina um PIN para desbloqueá-lo.
Limpar - eliminar todos os dados do seu dispositivo.

Importante
Após apagar toda a informação de um dispositivo, todas as funcionalidades Anti-Roubo deixam de funcionar.

19. CONTA BITDEFENDER

Uma conta Bitdefender é obrigatória para ativar o Bitdefender Mobile Security for iOS. Sempre que desejar aceder às ferramentas e serviços online do produto ou realizar remotamente tarefas importantes nos dispositivos nos quais o Bitdefender está instalado, pode entrar na sua conta a partir de qualquer computador ou dispositivo móvel ligado à Internet acedendo a https://central.bitdefender.com.

Meus dispositivos

A seção **OS MEUS DISPOSITIVOS** na sua conta Bitdefender permite-lhe instalar, gerir e realizar ações remotas no seu Bitdefender em qualquer dispositivo, desde que esteja ativado e ligado à Internet. Os cartões de dispositivos exibem o nome do dispositivo, o estado da proteção e se há algum risco de segurança afetando a proteção dos seus dispositivos.

Para identificar e gerir facilmente os seus dispositivos, pode personalizar o nome do dispositivo e criar ou atribuir um proprietário para cada um deles:

1. Pressione o ícone no canto superior esquerdo do ecrã e, em seguida, selecione **Os meus dispositivos**.
2. Toque no cartão de dispositivo pretendido e, em seguida, o ícone no canto superior direito do ecrã. Estão disponíveis as seguintes opções:
   - **Definições** - aqui pode alterar o nome do dispositivo selecionado.
   - **Perfil** - aqui pode ser atribuído um perfil ao dispositivo selecionado. Toque em **Adicionar proprietário** e preencha os campos correspondentes. Defina o nome, e-mail, número de telefone, data de nascimento e até pode selecionar uma fotografia de perfil.
   - **Remover** - a partir daqui, é possível remover um perfil juntamente com o dispositivo atribuído da sua conta Bitdefender.

Iniciar sessão com outra conta Bitdefender

Para iniciar sessão com outra conta Bitdefender:

1. Toque no ícone na parte inferior do ecrã.
2. Toque no ícone no canto superior direito do ecrã.

3. Toque em **Terminar sessão**.
4. Introduza o endereço de e-mail e palavra-passe da sua conta Bitdefender nos campos correspondentes.
5. Pressione **ENTRAR**.

MOBILE SECURITY PARA ANDROID

20. FUNCIONALIDADES DA PROTECÇÃO

O Bitdefender Mobile Security protege o seu dispositivo Android com os seguintes recursos:

- Analisador de Malware
- Privacidade de conta
- Proteção da Internet
- VPN
- AntiFurto, incluindo:
  - Localização Remota
  - Bloqueio remoto do aparelho
  - Limpeza remota do aparelho
  - Alertas do aparelho remoto
- Bloqueio de Aplicativo
- Relatórios
- WearON

Pode utilizar os recursos do produto por 14 dias, sem nenhum custo. Quando o período expirar, é necessário comprar a versão completa para proteger o seu dispositivo móvel.

21. INTRODUÇÃO

Requisitos do Aparelho

O Bitdefender Mobile Security funciona em qualquer dispositivo com Android 4.0.3 ou superior. É necessária uma ligação ativa à internet para a análise de ameaça na nuvem.

A instalar Bitdefender Mobile Security

- **Da Bitdefender Central**
  - Android
    1. Vá para: https://central.bitdefender.com.
    2. Iniciar sessão na sua conta Bitdefender.
    3. Pressione o ícone ☰ no canto superior esquerdo do ecrã e, em seguida, selecione **Os meus dispositivos**.
    4. Toque **INSTALAR PROTEÇÃO LOCAL**.
    5. Selecione **Segurança Móvel Bitdefender** da lista, em seguida, toque em **ACEDER A GOOGLE PLAY**.
    6. Toque **INSTALAR** no ecrã do Google Play.
  - No Windows, macOS, iOS
    1. Vá para: https://central.bitdefender.com.
    2. Iniciar sessão na sua conta Bitdefender.
    3. Pressione o ícone ☰ no canto superior esquerdo do ecrã e, em seguida, selecione **Os meus dispositivos**.
    4. Pressione **INSTALAR PROTEÇÃO LOCAL** .
    5. No Windows e macOS, clique no link **Em outro dispositivo**.

       No iOS, pressione **Deseja proteger outros dispositivos?**.
    6. Escolha **Android**.
    7. Selecione **Segurança Móvel Bitdefender** da lista, em seguida, pressione **CONTINUAR**.

8. Escreva um endereço de e-mail no campo correspondente e pressione **ENVIAR**.
9. Aceda à sua conta de e-mail no seu dispositivo Android, depois pressione o botão **OBTER NO Google Play**.

   Será redirecionado para a aplicação do **Google Play**.
10. Toque **INSTALAR** no ecrã do Google Play.

- **Do Google Play**

  Pesquise por Bitdefender Mobile Security para localizar e instalar a aplicação.

  Alternativamente, analise o código QR:

Código QR

Para concluir o processo de instalação, tem de concordar com o Contrato de Subscrição. Leia o Contrato de Subscrição com calma pois contém os termos e condições que regem a utilização do Bitdefender Mobile Security.

Toque em **CONTINUAR** para avançar para a janela seguinte.

Iniciar sessão na sua conta Bitdefender

Para utilizar o Bitdefender Mobile Security, deve associar o seu dispositivo a uma conta Bitdefender do Facebook, Google ou Microsoft iniciando sessão na conta a partir da aplicação. A primeira vez que abrir a aplicação, será pedido que inicie sessão numa conta.

Se instalou o Bitdefender Mobile Security a partir da sua conta Bitdefender, a aplicação tentará iniciar sessão automaticamente com essa conta.

Para associar o seu dispositivo a uma conta Bitdefender:

1. Abrir o Bitdefender Mobile Security.
2. Introduza o endereço de e-mail e palavra-passe da sua conta Bitdefender nos campos correspondentes. Caso não tenha uma conta Bitdefender e deseje criar uma, pressione o link correspondente para criar uma.
3. Pressione **ENTRAR**.

Para entrar usando uma conta do Facebook, Google ou Microsoft, pressione o serviço que deseja usar na área **OU ENTRAR COM**. Será redirecionado para a página de login do serviço selecionado. Siga as instruções para vincular a sua conta ao Bitdefender Mobile Security.

Nota
O Bitdefender não obtém acesso a qualquer informação confidencial como a palavra-passe da conta que usa para iniciar sessão ou a informação particular dos seus amigos ou contactos.

A activar o Bitdefender Mobile Security

Para obter a proteção do Bitdefender Mobile Security, deve ativar O seu produto com uma assinatura, que irá especificar por quanto tempo irá poder utilizar o produto. Assim que esse período acabar, a aplicação para de realizar as suas funções e proteger o seu dispositivo.

Para ativar o Bitdefender Mobile Security:

1. Abrir o Bitdefender Mobile Security.
2. A aplicação exibe informações sobre o estado atual da subscrição.

   Pressione **EU TENHO UM CÓDIGO**.
3. Digite um código de ativação no campo correspondente, depois pressione **ATIVAR**.

Para prolongar uma subscrição disponível:

1. Abrir o Bitdefender Mobile Security.
2. Pressione o botão **Menu** e selecione **Minha Conta** da lista de opções.
3. Na seção **Prolongar subscrição**, insira um código de ativação e toque em **ATIVAR**.

   Também pode prolongar a sua assinatura atual acedendo às ofertas listadas.

Painel

Toque no ícone do Bitdefender Mobile Security na secção de aplicações do seu dispositivo para abrir a interface da aplicação.

O Painel de Controlo apresenta informações sobre o estado de segurança do seu dispositivo e permite o fácil controlo de todas as funções de segurança.

Quando houver um processo em curso ou uma função solicitar uma ação sua, é exibido um cartão com mais informações e ações possíveis no Painel de Controlo.

Pode aceder às funções do Bitdefender Mobile Security e navegar facilmente de uma secção para a outra com a utilização do botão **Menu** localizado no canto superior esquerdo do ecrã:

Analisador de Malware
Permite que inicie uma análise sob demanda e que ative ou desative o Armazenamento da Análise. Para mais informação, dirija-se a "*Analisador de Malware*" (p. 289).

Privacidade de conta
Verifique se houve fuga de dados nas suas contas online. Para mais informação, dirija-se a "*Privacidade de conta*" (p. 292).

Proteção da Internet
Permite que ative ou desative o recurso de proteção na Web. Para mais informação, dirija-se a "*Proteção da Internet*" (p. 294).

VPN
Encripta a comunicação na Internet, ajudando-o a manter a sua privacidade, não importando a rede à qual está ligado. Para mais informação, dirija-se a "*VPN*" (p. 296).

Anti-Theft
Permite que ative ou desative as características Anti Furto e configure as definições Anti Furto. Para mais informação, dirija-se a "*Funcionalidades Anti Furto*" (p. 299).

Bloqueio de Aplicativo
Permite que proteja as suas aplicações instaladas, através da configuração de um código PIN de acesso. Para mais informação, dirija-se a "*Bloqueio de Aplicativo*" (p. 305).

Relatórios

Mantém um registo de todas as ações importantes, mudanças de estado e outras mensagens críticas relacionadas com a atividade do seu dispositivo. Para mais informação, dirija-se a "*Relatórios*" (p. 310).

WearON

Comunica com o seu smartwatch para ajudá-lo a encontrar o seu telefone, caso o tenha perdido ou caso se tenha esquecido onde o deixou. Para mais informação, dirija-se a "*WearON*" (p. 311).

22. ANALISADOR DE MALWARE

Bitdefender protege o seu aparelho e dados de aplicações maliciosas utilizando a análise na instalação e análise sob pedido.

Nota
Certifique-se de que o seu dispositivo móvel está ligado à internet. Se o seu dispositivo não estiver ligado à internet, o processo de análise não será iniciado.

- **Análise Na-Instalação**

  Sempre que instalar uma aplicação, o Bitdefender Mobile Security analisa automaticamente se o mesmo utiliza tecnologia na nuvem. O mesmo processo de verificação é iniciado toda vez que as aplicações instaladas são atualizadas.

  Este tipo de análise é realizada através da funcionalidade Autopiloto. O Autopiloto é um analisador inteligente que analisa todas as aplicações que instala ou atualiza, impedindo a penetração de ameaças.

  Se a aplicação for considerada maliciosa, irá aparecer um alerta solicitando que a desinstale. Toque em **Desinstalar** para aceder ao ecrã de desinstalação da aplicação.

- **Verificação por ordem**

  Sempre que quiser saber se as aplicações instaladas no seu dispositivo são seguras para utilização, pode executar uma análise.

  Para iniciar uma análise, simplesmente pressione o botão **INICIAR ANÁLISE** do cartão Analisador de Malware disponível no Painel de Controlo.

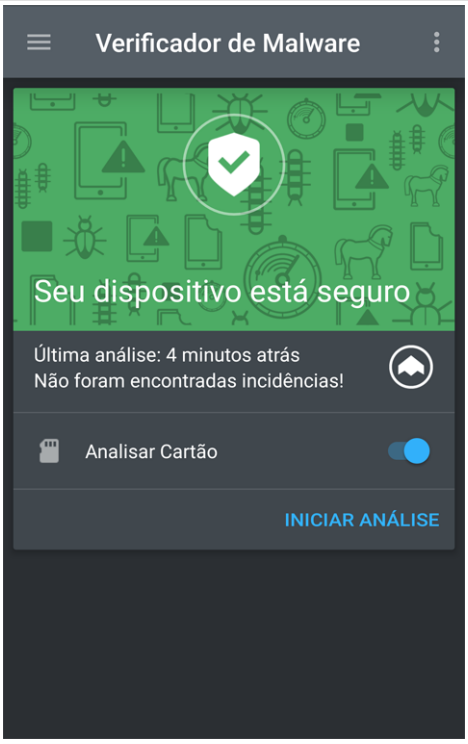
  Também pode executar uma análise seguindo estes passos:

  1. Abrir o Bitdefender Mobile Security.
  2. Pressione o botão **Menu** e selecione **Analisador de Malware** da lista de opções.
  3. Pressione **INICIAR ANÁLISE**.

     Nota
     São necessárias permissões adicionais no Android 6 para a função Analisador de Malware. Após pressionar o botão **INICIAR ANÁLISE**, selecione **Permitir** para as seguintes opções:

- Permitir que o **Antivírus** faça e administre chamadas?
- Permitir que o **Antivírus** aceda a fotos, multimédia e ficheiros no seu dispositivo?

O processo da análise será exibido e poderá interrompê-lo a qualquer momento.



Análise de Malware

O Bitdefender Mobile Security já vem configurado para analisar o armazenamento interno do seu dispositivo, incluindo qualquer cartão SD ligado. Desta forma, quaisquer aplicações perigosas que estejam no cartão podem ser detetadas antes de causar danos.

Para ativar ou desativar a Análise do Armazenamento:

1. Abrir o Bitdefender Mobile Security.

2. Pressione o botão **Menu** e selecione **Analisador de Malware** da lista de opções.
3. Toque no botão correspondente.

Também pode ativar ou desativar a análise do armazenamento na área de **Configurações** pressionando o botão , depois o botão correspondente.

Caso sejam detetadas quaisquer aplicações maliciosas, serão exibidas informações sobre elas e poderá removê-las tocando no botão **DESINSTALAR**.

O cartão do analisador de Malware exibe o estado do seu dispositivo. Quando está seguro, o cartão fica verde. Quando o dispositivo necessitar de análise ou de alguma ação sua, o cartão ficará vermelho.

23. PRIVACIDADE DE CONTA

A Privacidade de Conta Bitdefender deteta se houve fuga de dados nas contas que utiliza para fazer pagamentos online, compras ou iniciar sessão em diferentes aplicações ou sites Web. Os dados armazenados numa conta podem ser palavras-passe, informações de cartão de crédito ou informações de conta bancária e, se não forem devidamente protegidos, pode sofrer roubo de identidade ou invasão de privacidade.

O estado de privacidade de uma conta é apresentado depois da validação.

A novas verificações automáticas são definidas para serem executadas em segundo plano, mas é possível executar análises manuais diariamente.

As notificações serão apresentadas sempre que são detetadas novas fugas que incluam qualquer uma das contas de e-mail validadas.

Para começar a proteger informações pessoais:

1. Abrir o Bitdefender Mobile Security.
2. Toque no botão **Menu** e selecione **Privacidade de Conta** na lista.
3. Toque no círculo azul no canto inferior direito do ecrã.
4. Digite o seu endereço de e-mail no campo correspondente e toque em **SEGUINTE**.

   Bitdefender necessita de validar esta conta antes de apresentar informações privadas. Portanto, é enviado um e-mail com um código de validação para o endereço de e-mail fornecido.
5. Verifique a caixa de entrada e digite o código recebido na área **Privacidade de Conta** da aplicação. Se não conseguir encontrar o e-mail de validação na pasta Caixa de Entrada, verifique a pasta Spam.

   O estado de privacidade da conta validada é apresentado.

Se forem detetadas fugas nas suas contas, recomendamos que altere as palavras-passe assim que possível. Para criar uma palavra-passe forte e segura, tenha em mente estas dicas:

- Oito carateres no mínimo.
- Carateres maiúsculos e minúsculos.
- Pelo menos um número ou símbolo, como #, @, % ou !.

Ao proteger uma conta que constava de uma violação de privacidade, pode confirmar as alterações ao marcar a(s) fuga(s) identificada(s) como **Resolvido**. Para tal:

1. Abrir o Bitdefender Mobile Security.
2. Toque no botão **Menu** e selecione **Privacidade de Conta** na lista.
3. Toque na conta que acabou de proteger.
4. Na área **Fugas**, passe o dedo para a esquerda sobre a fuga contra a qual protegeu a sua conta.
5. Toque no ícone .
6. É apresentada a opção **Marcar como resolvido**.

   Toque em **CONFIRMAR** para confirmar que a conta está protegida.

Quando todas as fugas detetadas estiverem marcadas como **Resolvido**, a conta já não aparece como fuga, pelo menos até à deteção de uma nova fuga.

24. PROTEÇÃO DA INTERNET

A Segurança na Web usa os serviços em nuvem do Bitdefender para verificar as páginas da web que acede com o navegador padrão do Android, Google Chrome, Firefox, Opera, Opera Mini e Dolphin. Uma lista completa com os navegadores suportados está disponível na secção Segurança na Web.

Caso um URL aponte para um site web conhecido por phishing ou fraude, ou para conteúdo malicioso como spyware ou vírus, a página web fica temporariamente bloqueada e é exibido um alerta.

Pode então optar por ignorar o alerta e prosseguir para página web ou voltar a uma página segura.

Nota

São necessárias permissões adicionais no Android 6 para a função Web Protection.
Ative a permissão para registar como serviço de Acessibilidade e pressione **LIGAR** quando solicitado. Toque em **Antivírus** e ative o botão, depois confirme que concorda com o acesso às permissões do seu dispositivo.

Proteção da Internet

25. VPN

Com o Bitdefender VPN , pode manter os seus dados privados sempre que se ligar a redes sem fios não seguras em aeroportos, shoppings, cafés ou hotéis. Assim, poderá evitar situações inoportunas, como roubo de dados pessoais ou tentativas de tornar o endereço de IP do seu dispositivo acessível a hackers.

A VPN funciona como um túnel entre o seu dispositivo e a rede à qual se liga, protegendo a sua ligação, encriptando os seus dados utilizando uma encriptação de nível bancário e escondendo o seu endereço IP onde quer que esteja. O seu tráfego é redirecionado por meio de um servidor separado, tornando o seu dispositivo quase impossível de ser identificado entre os incontáveis dispositivos que usam os nossos serviços. Além disso, enquanto estiver ligado à Internet com o Bitdefender VPN, pode aceder a conteúdos que normalmente são restritos em áreas específicas.

Nota
Alguns países censuram a Internet e, portanto, a utilização de VPN nos seus territórios foi banida por lei. Para evitar consequências legais, pode ser apresentada uma mensagem de aviso ao tentar utilizar a funcionalidade Bitdefender VPN pela primeira vez. Ao continuar a utilizar a funcionalidade, confirma que está ciente dos regulamentos aplicáveis e dos riscos aos quais pode estar exposto.

Há duas formas de ativar ou desativar o Bitdefender VPN:

- Pressione o botão de ligar no cartão de VPN no Painel de Controlo.

  O estado do Bitdefender VPN é exibido.

- Pressione o botão **Menu** e selecione **VPN** na lista.

  Pressione **CONECTAR** sempre que quiser permanecer protegido enquanto estiver conectado a redes sem fios não seguras.

  Pressione **DESCONECTAR** quando desejar desativar a ligação.

Nota
Na primeira vez que ligar o VPN, deve permitir a solicitação do Bitdefender para configurar uma ligação VPN que monitorizará o tráfego de rede. Toque em **OK** para continuar.

O ícone aparece na barra de estado quando o Bitdefender VPN está ativo.

Para economizar bateria, recomendamos que desligue a VPN quando não precisar de usá-la.

Se tiver uma subscrição Premium e quiser ligar-se a um servidor da sua escolha, pressione **ESCOLHER LOCALIZAÇÃO** na funcionalidade de VPN e depois selecione o local desejado. Para detalhes sobre as subscrições de VPN, aceda a “Assinaturas” (p. 298).

VPN

Pressione **MAIS DETALHES** no cartão de VPN no painel para aceder à ferramenta que lhe permite:

- Visualizar o tráfego restante que tem na sua franquia diária ou obter a versão Premium - informações disponíveis na versão gratuita da VPN.

- Escolher o servidor ao qual gostaria de se conectar e ver quanto tempo resta na sua subscrição - informações disponíveis na versão Premium do VPN.

Definições da VPN

Toque no botão no menu de funções da VPN e selecione **Definições** para uma configuração avançada da VPN.

Nas **Definições** da VPN pode configurar as seguintes opções:

- Notificação da VPN de acesso rápido - é apresentada uma notificação na barra de estado para permitir que ligue rapidamente a VPN.
- Notificação ao ligar a uma rede Wi-Fi aberta - sempre que se ligar a uma rede Wi-Fi aberta, será notificado na barra de estado para utilizar a VPN.
- Notificação ao ligar um site de operações bancárias - sempre que aceder a um site de operações bancárias, será notificado na barra de estado para utilizar a VPN.

Assinaturas

O Bitdefender VPN oferece gratuitamente 200 MB de franquia por dispositivo para proteger a sua ligação sempre que precisar, além de ligá-lo automaticamente ao melhor local de servidor.

Para obter tráfego ilimitado e acesso irrestrito a conteúdos no mundo inteiro escolhendo um local da sua preferência, atualize para a versão Premium.

Pode atualizar para a versão Bitdefender Premium VPN a qualquer momento ao pressionar o botão **ATIVAR VPN PREMIUM** disponível no Painel de Controlo ou na janela da VPN.

A subscrição Bitdefender Premium da VPN é independente da subscrição do Bitdefender Mobile Security, ou seja, poderá usá-la durante todo o seu período de disponibilidade, não importando o estado da subscrição da sua segurança. Caso a subscrição do Bitdefender Premium VPN expire, mas Bitdefender Mobile Security continua ativa, voltará para o plano gratuito.

O Bitdefender VPN é um produto multiplataforma, disponível nos produtos Bitdefender compatíveis com Windows, macOS, Android e iOS. Quando atualizar para o plano Premium, poderá usar a sua subscrição em todos os seus produtos, desde que faça login com a mesma conta Bitdefender.

26. FUNCIONALIDADES ANTI FURTO

Bitdefender pode ajudá-lo a localizar o seu dispositivo e impedir que os seus dados pessoais caiam nas mãos erradas.

Tudo o que necessita de fazer é ativar o Anti-roubo a partir do dispositivo e, quando necessário, aceder à **Bitdefender Central** a partir de qualquer Web browser, em qualquer lugar.

Mesmo que não possa aceder à internet, ainda pode proteger o seu dispositivo e os seus dados ao enviar **comandos via SMS** de qualquer telemóvel para o seu smartphone através de mensagens de texto normais.

Bitdefender Mobile Security oferece as seguintes funcionalidades Anti Furto:

Localização Remota

Visualize a localização atual do seu dispositivo no Google Maps. A localização é atualizada a cada 5 segundos para que possa controlá-lo se estiver em movimento.

A precisão da localização depende do quanto o Bitdefender é capaz de o determinar:

- Caso o GPS esteja ativado no dispositivo, a sua localização pode ser determinada no alcance de dois metros, desde que esteja ao alcance dos satélites GPS (ou seja, fora de um edifício).
- Se o dispositivo estiver dentro de um edifício, a sua localização pode ser determinada no alcance de 10 metros caso o Wi-Fi esteja ativado e existam rede sem fios disponíveis no seu alcance.
- Caso contrário, a localização será determinada utilizando apenas as informações da rede móvel, que pode oferecer uma precisão não melhor que várias centenas de metros.

Mostrar IP

Exibe o último endereço de IP para o dispositivo selecionado. **MOSTRAR IP** - exibe o último endereço de IP para o dispositivo selecionado.

Limpeza Remota

Remova todos os dados pessoais do seu dispositivo roubado.

Bloqueio Remoto

Bloqueie o ecrã do seu dispositivo e defina uma palavra-passe para desbloquear o mesmo.

Enviar alerta para o dispositivo (Scream)

Envie uma mensagem remotamente para ser exibida no ecrã do dispositivo ou para emitir um som alto no altifalante do dispositivo.

Caso venha a perder o seu dispositivo, pode informar a quem o encontrar como pode ser devolvido, exibindo uma mensagem no ecrã do dispositivo.

Caso tenha perdido o seu dispositivo e exista a possibilidade de não estar longe de si (por exemplo, em algum lugar em casa ou no escritório), que melhor maneira de encontrá-lo do que fazê-lo tocar um som alto? O som será reproduzido mesmo se o dispositivo estiver no modo silencioso.

A ativar o Anti Furto

Para ativar a função Anti Furto, basta completar o processo de configuração do cartão Anti Furto disponível no Painel de Controlo.

Também pode ativar a função Anti Furto seguindo estas instruções:

1. Abrir o Bitdefender Mobile Security.
2. Pressione o botão **Menu** e selecione **Anti Furto** da lista de opções.
3. Toque em **ATIVAR**.
4. O seguinte procedimento será iniciado para ajudá-lo na ativação desta função:

   Nota

   São necessárias permissões adicionais no Android 6 para a função Anti Furto. Para ativá-la, siga os passos abaixo:

   - Toque em **Ativar Anti Furto**, depois toque em **LIGAR**.
   - Ative as permissões nas seguintes opções:
     a. Permitir que o **Antivírus** envie e visualize mensagens SMS?
     b. Permitir que o **Antivírus** aceda à localização deste dispositivo?
     c. Permitir que o **Antivírus** aceda aos seus contactos?

   a. **Conceder privilégios de administrador**

   Estes privilégios são essenciais para o funcionamento da função Anti Furto e devem ser concedidas antes de continuar.

b. **Definir PIN para a aplicação**

Para garantir que quaisquer mudanças feitas nas configurações da função Anti Furto passem pela sua autorização, deve ser definido um código PIN. Sempre que houver uma tentativa de modificação das configurações da função Anti Furto, o código PIN deverá ser inserido antes das mudanças serem aplicadas. De forma alternativa, em dispositivos que suportam a autenticação por leitura de impressão digital, uma confirmação por digital pode ser utilizada em vez do código PIN configurado.

Nota
O mesmo código PIN é utilizado pelo Bloqueio de Aplicação para proteger as suas aplicações instaladas.

c. **Ativar o Tirar Foto**

Sempre que alguém tentar aceder às suas aplicações instaladas enquanto a opção Tirar Foto estiver ligada, o Bitdefender tirará uma foto da pessoa. Para mais detalhes sobre esta função, aceda a "Tirar foto" (p. 307).

d. **Definir o número de confiança para o Antifurto**

Seleccione la pestaña **CONTROL SMS**, escriba un número de teléfono de confianza o seleccione uno de la lista de contactos y, a continuación, toque **GUARDAR NÚMERO**. O número fiável deve conter um código de país e pode ser o número de alguém que conhece ou o número de outro telefone que utiliza.

Quando for inserido um cartão SIM diferente no seu dispositivo, o Bitdefender Mobile Security irá enviar automaticamente uma mensagem de texto para o número de confiança com o novo número de telefone.

Deste modo, pode enviar comandos para o seu telefone por SMS mesmo que o SIM seja trocado e o seu número mude.

Importante
Este não é um passo obrigatório, mas é recomendável que defina um número de confiança durante a instalação inicial. O comando Limpeza funciona apenas quando é enviado a partir de um número de confiança predefinido.

Quando o Anti Furto é ativado, pode ativar ou desativar as funcionalidades de controlo Web ou controlo via SMS individualmente no ecrã Anti Furto ao tocar nos ícones correspondentes.

A utilizar as funcionalidades Anti Furto de Bitdefender Central (Controlo via Web)

Nota
Todas as funcionalidades de Anti Furto necessitam que a opção **Dados em segundo plano** esteja ativa nas configurações de Dados do seu dispositivo.

Para aceder às funções anti-furto da sua conta Bitdefender:

1. Aceda Bitdefender Central.
2. Pressione o ícone no canto superior esquerdo do ecrã e, em seguida, selecione **Os meus dispositivos**.
3. Na janela **OS MEUS DISPOSITIVOS**, selecione o cartão de dispositivo pretendido.
4. Selecione o separador **Anti Furto**.
5. No último campo da janela, toque no ícone e, em seguida, no botão com a função correspondente que deseja utilizar:

   Localizar - exibe a localização do seu dispositivo no Google Maps.
   Alerta - escreva uma mensagem para ser exibida no ecrã do seu dispositivo e/ou para fazer com que o seu dispositivo emita um alarme sonoro.
   Bloquear - bloqueie o seu dispositivo e defina um PIN para desbloqueá-lo.
   Limpar - eliminar todos os dados do seu dispositivo.

   Importante
   Após apagar toda a informação de um dispositivo, todas as funcionalidades Anti-Roubo deixam de funcionar.

   MOSTRAR IP - exibe o último endereço de IP para o dispositivo selecionado.

A utilizar os recursos Anti Furto através de comandos via SMS (Controlo via SMS)

Quando os comandos via SMS são ativados, pode enviar os seguintes comandos para o seu smartphone via SMS a partir qualquer outro telemóvel:

- **LOCATE** - enviar uma mensagem contendo a localização do dispositivo para o número de telefone a partir do qual o comando foi enviado. A mensagem contém uma ligação do Google Maps que pode ser aberta no navegador do telemóvel.
- **SCREAM** - tocar um som alto no altifalante do dispositivo.
- **LOCK** - bloqueie o ecrã do dispositivo com o código PIN que definido por si.
- **WIPE** - apagar todos os dados do seu dispositivo.

  Importante
  O comando Limpeza funciona apenas quando é enviado a partir de um número de confiança predefinido.

- **CALLME** - marque o número de telefone a partir do qual o comando foi enviado com o altifalante ativado. Assim, poderá ouvir silenciosamente a pessoa que estiver com o seu telefone.
- **HELP** - enviar uma mensagem contendo todos os comandos disponíveis para o número de telefone a partir do qual o comando foi enviado.
- **SIM Change** - o número de confiança que configurou receberá um SMS com o novo número de telefone assim que o seu SIM for substituído por um novo. Para configurar o número de telefone do seu amigo, pressione a opção **Número de confiança**. Digite o número dele incluindo o código do país, ou escolha o seu cartão da lista de contactos.

Todos os comandos via SMS devem ser enviados utilizando o seguinte formato:

bd-<PIN> <command>

Nota
Os símbolos indicam variáveis e não devem aparecer no comando.

Por exemplo, se definiu o PIN de segurança como 123456 e pretende receber uma mensagem com a localização do seu telefone, envie a seguinte mensagem de texto para o seu número de telefone:

BD-123456 LOCATE

27. BLOQUEIO DE APLICATIVO

Aplicações instaladas, como e-mails, fotos ou mensagens, podem conter dados pessoais que gostaria que permanecessem privados, limitando o acesso a estes de forma seletiva.

O Bloqueio de Aplicação ajuda-o a bloquear o acesso indesejado às aplicações, através da configuração de um código PIN de acesso de segurança. O código PIN deve ter no mínimo 4 dígitos e no máximo 8 e será solicitado sempre que pretender aceder às aplicações restritas.

De forma alternativa, em dispositivos que suportam a autenticação por leitura de impressão digital, uma confirmação por digital pode ser utilizada em vez do código PIN configurado.

A ativar o Bloqueio de Aplicação

Para restringir o acesso a aplicações específicas, configure o Bloqueio de Aplicação através do cartão exibido no Painel de Controlo após a ativação da função Anti Furto.

Também pode ativar o Bloqueio de Aplicação seguindo estas instruções:

1. Abrir o Bitdefender Mobile Security.
2. Pressione o botão **Menu** e selecione **Bloqueio de Aplicação** da lista de opções.
3. Pressione **ATIVAR** e permita o acesso aos dados de utilização para o Bitdefender selecionando a caixa de verificação correspondente.

   Nota
   São necessárias permissões adicionais no Android 6 para a função Tirar Foto.
   Para ativá-la, permita que o **Antivírus** tire fotos e grave vídeos.

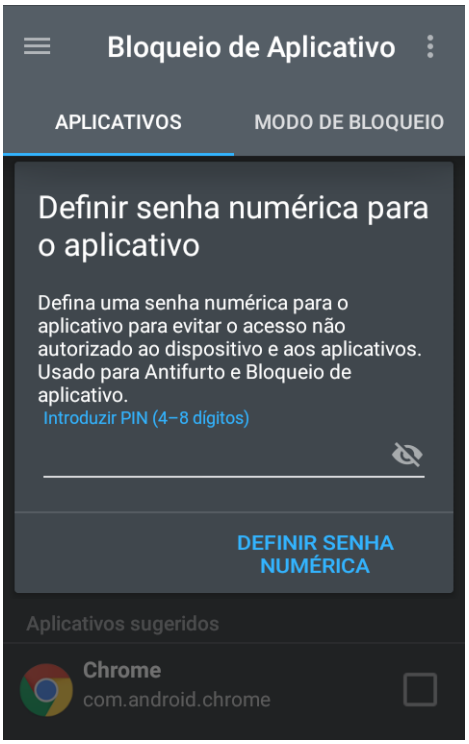
4. Volte à aplicação, configure o código de acesso e pressione **DEFINIR PIN**.

   Nota
   Este passo será apenas necessário se não tiver configurado o PIN na função Anti Furto.

5. Permite que a opção Tirar Foto apanhe qualquer intruso que tente aceder aos seus dados pessoais.
6. Selecione as aplicações que gostaria de proteger:

Utilizar o PIN ou a impressão digital errada cinco vez seguidas ativará uma pausa de 30 segundos. Dessa forma, qualquer tentativa de aceder às aplicações protegidas será bloqueada.

Nota
O mesmo código PIN é utilizado pelo Anti Furto para ajudá-lo a localizar o seu dispositivo.



Bloqueio de Aplicativo

MODO DE BLOQUEIO

Aqui pode escolher quando a função Bloqueio de Aplicações deve proteger as aplicações instaladas no seu dispositivo.

Pode selecionar entre uma das seguintes opções:

- **Bloquear sempre** - o código PIN ou digital que configurou deverá ser utilizado sempre que tentar aceder às aplicações bloqueadas.
- **Desbloquear até o ecrã apagar** - o acesso às suas aplicações será válido até o ecrã apagar.
- **Permitir uma saída rápida** - pode sair e aceder novamente às suas aplicações desbloqueadas dentro de 30 segundos.
- **Ativar desbloqueio inteligente** - quando ativado e ligado a uma rede definida como fiável, as outras configurações ficam indisponíveis. Isso significa que nenhuma confirmação por PIN ou digital é necessária quando as aplicações bloqueadas são acedidas.

Definições do Bloqueio de Aplicação

Pressione o botão no menu de funções do Bloqueio de Aplicação e selecione **Configurações** para uma configuração mais avançada do seu Bloqueio de Aplicação.

Em **Configurações** do Bloqueio de Aplicação pode fazer o seguinte:

- Ativar o Tirar Foto quando forem realizadas três tentativas erradas de desbloqueio.
- Bloquear notificações para aplicações recentemente instaladas.
- Mudar o seu código PIN.

Tirar foto

Com o Tirar Foto (Snap Photo) da Bitdefender pode apanhar os seus amigos ou familiares em flagrante. Assim pode educá-los a não bisbilhotar os seus ficheiros pessoais ou as aplicações que utiliza.

A função funciona de forma fácil: sempre que o código PIN ou a confirmação por impressão digital que definiu para proteger as suas aplicações for inserido de forma errada três vezes seguidas, será tirada uma foto com a

câmara frontal. A foto será guardada com a informação sobre o dia, hora e motivo, e poderá ser visualizada quando abrir o Bitdefender Mobile Security e aceder à função do Bloqueio de Aplicação.

Nota
Esta função está disponível apenas para telefones que têm uma câmara frontal.

Para configurar a função Tirar foto (Snap Photo):

1. Abrir o Bitdefender Mobile Security.
2. Pressione o botão **Menu** e selecione **Bloqueio de Aplicação** da lista de opções.
3. Pressione o botão no menu da função Bloqueio de Aplicação e selecione **Definições**.
4. Ative o botão de **Tirar foto quando forem realizadas 3 tentativas erradas de desbloqueio**.

As fotos tiradas quando é introduzido o PIN incorreto são exibidas no menu de Bloqueio de Aplicação e podem ser visualizadas em ecrã completo.

De forma alternativa, eles podem ser vistos na sua conta Bitdefender:

1. Vá para: https://central.bitdefender.com.
2. Aceda à sua conta.
3. Pressione o ícone no canto superior esquerdo do ecrã e, em seguida, selecione **Os meus dispositivos**.
4. Selecione o seu dispositivo na janela **OS MEUS DISPOSITIVOS** e, em seguida, o separador **Antifurto**.

   As fotos são exibidas.

São guardadas apenas as 3 fotos mais recentes.

Desbloqueio Inteligente

Um método fácil para que a função Desbloqueio de Aplicação deixe de solicitar o código PIN ou a confirmação por impressão digital para as aplicações protegidas sempre que acede é ativar o Desbloqueio Inteligente.

Com o Desbloqueio Inteligente pode configurar as redes Wi-Fi que costuma utilizar como fiáveis e quando estiver ligado a elas, as definições de bloqueio do Bloqueio de Aplicação serão desativadas para as aplicações protegidas.

Para ativar a função Desbloqueio Inteligente:

1. Abrir o Bitdefender Mobile Security.
2. Pressione o botão **Menu** e selecione **Bloqueio de Aplicação** da lista de opções.
3. Selecione o separador **MODO DE BLOQUEIO** e ative o botão correspondente.

   A rede sem fios à qual está ligado é exibida.

   Para definir a ligação Wi-Fi que está a utilizar como fiável, pressione o ícone .

Nota
Esta definição apenas estará disponível se a função Desbloqueio Inteligente estiver ativa.

Sempre que mudar de opinião, desative a função e as redes Wi-Fi que configurou como fiáveis serão tratadas como não fiáveis.

28. RELATÓRIOS

O recurso Relatórios mantém um registo detalhado de eventos relacionados com a atividade de análise do seu dispositivo.

Sempre que acontecer algo relevante para a segurança do seu dispositivo, será adicionada uma nova mensagem aos Relatórios.

Para aceder à secção Relatórios:

1. Abrir o Bitdefender Mobile Security.
2. Pressione o botão **Menu** e selecione **Relatórios** da lista de opções.

Os seguintes separadores estão disponíveis na janela Relatórios:

- **RELATÓRIOS SEMANAIS** - aqui tem acesso ao estado de segurança e às tarefas executadas da semana atual e anterior. O relatório semanal é gerado todos os domingos e irá receber uma notificação com a informação sobre a sua disponibilidade.

  Todas as semanas será exibida uma nova dica nesta secção, então lembre-se de conferir regularmente para obter o máximo do que a sua aplicação pode oferecer.

- **REGISTO DE ATIVIDADES** - aqui poderá aceder a informações detalhadas sobre as atividades da sua aplicação Bitdefender Mobile Security, desde quando foi instalada no seu dispositivo Android.

  Para apagar o registo de atividade disponível, pressione o botão no canto superior direito do ecrã e depois selecione **Limpar o registo de atividades**.

29. WEARON

Com WearON do Bitdefender, pode encontrar facilmente o seu smartphone, esteja ele na sala de reunião do escritório ou sob uma almofada no sofá. O dispositivo pode ser encontrado mesmo se o modo silencioso estiver ativado.

Mantenha esta função ativada para garantir que terá sempre o seu smartphone por perto.

Nota
A função funciona com Android 4.3 e Android Wear.

A ativar o WearON

Para utilizar o WearON, só precisa de ligar o seu smartwatch à aplicação do Bitdefender Mobile Security e ativar a função com o seguinte comando de voz:

Start:<Where is my phone>

O **Bitdefender WearON** tem dois comandos:

1. **Alerta de Telefone**

   Com o recurso Alerta do Telefone encontra rapidamente o seu smartphone, sempre que se afastar muito dele.

   Se estiver com seu smartwatch, ele deteta automaticamente a aplicação no seu telefone e vibra sempre que estiver a menos de dez metros de distância do seu dispositivo.

   Para ativar esta função, abra o Bitdefender Mobile Security, toque em **Configurações Globais** no menu e selecione o botão correspondente na secção WearON.

2. **Toque alto**

   Encontrar o seu telefone nunca foi tão fácil. Quando se esquecer onde deixou o seu telefone, toque no comando Apitar no seu relógio para fazer o seu telefone apitar.

30. DEFINIÇÕES

A área Definições é onde pode alterar as seguintes opções:

- **Código PIN de Segurança** — pode alterar o código PIN definido para desbloquear aplicações ou comandos antirroubo.
- **Analisador de Malware** — pode decidir se o armazenamento deve ser analisado.
- **Deteção na nuvem** — pode decidir se pretende enviar relatórios que nos podem ajudar a melhorar a proteção na nuvem.
- **Privacidade de Conta** — pode decidir se pretende ser informado quando as suas contas não estiverem envolvidas em fugas.
- **Bloqueio de Aplicações** — pode decidir se pretende bloquear notificações de aplicações recentemente instaladas.
- **Tirar Fotografia** — pode decidir se pretende tirar uma captura de ecrã depois de três tentativas falhadas para aceder às aplicações.
- **Antirroubo** — pode alterar o número que definiu como fidedigno caso o seu dispositivo caia em mãos alheias.
- **Relatórios** — pode decidir se pretende receber notificações de relatórios.
- **Enviar relatórios anónimos** — pode decidir se pretende enviar-nos relatórios com informações sobre como utilizar o produto. Esta informação é essencial para melhorar o produto e pode ajudar-nos a oferecer-lhe uma experiência melhor no futuro.

31. SOBRE

Para mais informações sobre a versão do Bitdefender Mobile Security que tem instalada, aceda à área **Informações**. Na mesma área, pode entrar em contacto connosco para obter suporte, aceder e ler o Contrato de Subscrição e a Política de Privacidade e visualizar as licenças de código aberto.

32. BITDEFENDER CENTRAL

Bitdefender Central é a plataforma Web onde tem acesso às funcionalidades e serviços online do produto, e pode realizar remotamente tarefas importantes nos dispositivos em que o Bitdefender estiver instalado. Pode iniciar sessão na sua conta Bitdefender a partir de qualquer computador ou dispositivo móvel ligado à internet através https://central.bitdefender.com. Assim que tiver obtido acesso, pode realizar o seguinte:

- Transfira e instale o Bitdefender nos sistemas operativos Windows, macOS, iOS e Android. Os produtos disponíveis para download são:
  - Bitdefender Mobile Security
  - Bitdefender Mobile Security for iOS
  - O Antivírus Bitdefender para Mac
  - A linha de produtos Windows da Bitdefender
- Gerir e renovar as suas subscrições do Bitdefender.
- Adicionar novos dispositivos à sua rede e gerir as suas funcionalidades onde quer que esteja.

Aceder à sua conta Bitdefender

Para aceder à sua conta Bitdefender, basta:

1. Abrir um navegador em qualquer dispositivo com acesso à internet.
2. Vá para: https://central.bitdefender.com.
3. Inicie sessão na sua conta com o seu endereço de e-mail e palavra-passe.

Meus dispositivos

A seção **OS MEUS DISPOSITIVOS** na sua conta Bitdefender permite-lhe instalar, gerir e realizar ações remotas no seu Bitdefender em qualquer dispositivo, desde que esteja ativado e ligado à Internet. Os cartões de dispositivos exibem o nome do dispositivo, o estado da proteção e se há algum risco de segurança afetando a proteção dos seus dispositivos.

Para identificar facilmente os seus dispositivos, pode personalizar o nome de cada um:

1. Aceda Bitdefender Central.

2. Pressione o ícone no canto superior esquerdo do ecrã e, em seguida, selecione **Os meus dispositivos**.
3. Toque no cartão de dispositivo pretendido e, em seguida, o ícone no canto superior direito do ecrã.
4. Selecione **Definições**.
5. Digite um novo nome no campo **Nome do dispositivo** e selecione **GUARDAR**.

Pode criar e atribuir um proprietário a cada um dos seus dispositivos para uma melhor gestão:

1. Aceda Bitdefender Central.
2. Pressione o ícone no canto superior esquerdo do ecrã e, em seguida, selecione **Os meus dispositivos**.
3. Toque no cartão de dispositivo pretendido e, em seguida, o ícone no canto superior direito do ecrã.
4. Selecione **Perfil**.
5. Clique em **Add owner** e, em seguida, preencha os respetivos campos. Personalize o perfil adicionando uma fotografia e selecionando a data de nascimento.
6. Toque em **ADICIONAR** para guardar o perfil.
7. Selecione o proprietário pretendido na lista **Proprietário do dispositivo** e, em seguida, toque em **ATRIBUIR**.

Para mais ações remotas e informações sobre o seu produto Bitdefender num dispositivo específico, selecione o cartão de dispositivo pretendido.

Quando selecionar no cartão de dispositivo, ficam disponíveis os seguintes separadores:

- **Painel**. Nesta janela, pode visualizar os detalhes sobre o dispositivo selecionado, verificar o seu estado de proteção, o estado do Bitdefender VPN e quantas ameaças foram bloqueadas nos últimos sete dias. O estado de proteção pode estar verde, quando não houver problemas a afetar o seu dispositivo, amarelo, quando o dispositivo exigir a sua atenção, ou vermelho, quando o dispositivo estiver em risco. Quando houver problemas a afetar o seu dispositivo, clique a seta pendente na área de estado acima

para saber mais detalhes. A partir daqui poderá resolver manualmente os problemas que afetam a segurança dos seus dispositivos.

- **Proteção**. a partir desta janela pode executar uma Análise remota no seu dispositivo. Toque no botão **ANALISAR** para iniciar o processo. Também pode conferir quando é que a última verificação foi realizada no dispositivo e aceder a um relatório da última verificação, contendo as informações mais importantes.
- **Antirroubo**. Caso tenha perdido o seu dispositivo, pode localizá-lo e realizar ações remotas com a função Anti Furto. Toque em **LOCALIZAR** para descobrir a localização do seu dispositivo. A última localização conhecida será exibida, juntamente com a hora e com a data. Para mais detalhes sobre esta função, aceda a "*Funcionalidades Anti Furto*" (p. 299).

As minhas subscrições

A plataforma da Bitdefender Central possibilita-lhe controlar facilmente as subscrições que possui para todos os seus dispositivos.

Verificar subscrições disponíveis

Para verificar as suas subscrições disponíveis:

1. Aceda Bitdefender Central.
2. Pressione o ícone ☰ no canto superior esquerdo do ecrã e selecione **As minhas Assinaturas**.

Aqui pode aceder às informações sobre a disponibilidade das subscrições que possui e o número de dispositivos a utilizar cada uma delas.

Pode adicionar um novo dispositivo a uma subscrição ou renová-la selecionando um cartão de subscrição.

Adicionar um novo dispositivo

Se a sua assinatura abranger mais de um dispositivo, pode adicionar um novo dispositivo e instalar nele o seu Bitdefender Mobile Security, conforme descrito em "A instalar Bitdefender Mobile Security" (p. 284).

Renovar subscrição

Se lhe restam menos de 30 dias de assinatura e desativou a renovação automática, é possível renová-la manualmente seguindo os seguintes passos:

1. Aceda Bitdefender Central.
2. Pressione o ícone no canto superior esquerdo do ecrã e selecione **As minhas Assinaturas**.
3. Selecione o cartão de subscrição pretendido.
4. Toque em **RENOVAR** para continuar.

Uma página abrirá no seu navegador onde poderá renovar a sua subscrição do Bitdefender.

33. PERGUNTAS FREQUENTES

Porque é que o Bitdefender Mobile Security requer a ligação à internet?

A aplicação precisa de comunicar com os servidores do Bitdefender para determinar o estado de segurança das aplicações que analisa e das páginas web que visita e também para receber os comandos da sua conta Bitdefender quando utilizar a função Anti Furto.

Para que é que o Bitdefender Mobile Security precisa de cada permissão?

- Acesso à Internet -> utilizado para comunicação na nuvem.
- Analisa o estado do telefone e identidade -> utilizado para detetar se o dispositivo está ligado à internet e para extrair determinadas informações do dispositivo necessárias para criar um ID exclusivo ao comunicar com Bitdefender nuvem.
- Ler e escrever marcadores do navegador -> o módulo Web Protection apaga sites maliciosos do seu histórico de navegação.
- Ler o registo de dados -> o Bitdefender Mobile Security deteta traços de atividades de ameaças dos registos Android.
- Leitura/escrita de SMS, contactos, dados da conta e de armazenamento externo -> Necessário para a função de limpeza remota.
- Localização -> Necessária para a localização remota.
- Câmara -> necessária para Tirar foto (Snap photo).
- Armazenamento -> utilizado para permitir que o Analisador de Malware verifique o cartão SD.

Onde posso ver mais informações sobre a atividade do aplicação?

O Bitdefender Mobile Security mantém um registo de todas as ações importantes, mudanças de estado e outras mensagens críticas relacionadas com a sua atividade. Para aceder a essa informação, abra o Bitdefender Mobile Security e pressione o botão do **Menu** e então selecione **Relatórios** da lista de opções.

Esqueci-me do código PIN que defini para proteger a minha aplicação. What do I do?

1. Aceda Bitdefender Central.

2. Pressione o ícone no canto superior esquerdo do ecrã e, em seguida, selecione **Os meus dispositivos**.
3. Toque no cartão de dispositivo pretendido e, em seguida, o ícone no canto superior direito do ecrã.
4. Selecione **Definições**.
5. Recupere o PIN no campo **PIN da Aplicação**.

Como é que o Bitdefender Mobile Security irá influenciar o desempenho do meu dispositivo e na autonomia da minha bateria?

O impacto é muito baixo. A aplicação só é executada quando é fundamental — inclusive durante a instalação e quando navega pela interface da aplicação — ou quando pretende realizar uma verificação de segurança. O Bitdefender Mobile Security não funciona em plano de fundo quando liga para amigos, envia mensagens ou joga.

Como posso desligar a função Bloqueio de Aplicação?

Não há qualquer opção para desligar a função Bloqueio de Aplicação, mas pode desativá-la facilmente ao desmarcar as caixas próximas às aplicações selecionadas depois que validar o PIN ou impressão digital definida.

Como posso definir outra rede sem fios como fiável?

Se quiser definir outra rede sem fios como fiável:

1. Abrir o Bitdefender Mobile Security.
2. Pressione o botão **Menu** e selecione **Bloqueio de Aplicação** da lista de opções.
3. Selecione o separador **MODO DE BLOQUEIO** e selecione o ícone .
4. Valide o PIN ou impressão digital para confirmar a sua escolha.
5. Clique no ícone ao lado da rede que pretende definir como fiável.

Como posso parar de ver fotografias associadas tiradas nos meus dispositivos?

Para parar de tornar visíveis as fotografias associadas tiradas nos seus dispositivos:

1. Aceda Bitdefender Central.
2. Toque no ícone no canto superior direito do ecrã.

3. Clique em **A Minha Conta** no menu deslizante.
4. Selecione o separador **Definições**.
5. Desative a opção **Mostrar/não mostrar fotografias tiradas nos seus dispositivos** .

Como posso manter as minhas compras online seguras?

As compras online têm riscos elevados quando alguns detalhes são ignorados. Para não ser vítima de fraude, recomendamos o seguinte:

- Matenha a aplicação de segurança atualizada.
- Efetue pagamentos online apenas com proteção do comprador.
- Utilize uma VPN ao estabelecer ligação com a internet a partir de redes sem fios não protegidas e públicas.
- Preste atenção às palavras-passe que atribuiu às suas contas online. Têm de ser fortes e incluir letras maiúsculas e minúsculas, números e símbolos (@, !, %, #, etc.).
- Certifique-se de que as informações são enviadas por ligações seguras. A extensão do site Web online tem de ser HTTPS:// e não HTTP://.

Quando devo usar o Bitdefender VPN?

Tem de ter cuidado quando aceder, transferir ou enviar conteúdos na internet. Para garantir que fica em segurança enquanto navega na Web, recomendamos que utilize o Bitdefender VPN quando:

- quiser ligar-se a redes sem fios públicas
- quiser aceder a conteúdos que normalmente são restritos em áreas específicas, não importa se estiver em casa ou fora
- quiser manter os seus dados pessoais privados (nomes de utilizador, palavras-passe, informações de cartão de crédito, etc.)
- desejar esconder o seu endereço IP

O Bitdefender VPN vai ter um impacto negativo na bateria do meu dispositivo?

O Bitdefender VPN foi concebido para proteger os seus dados pessoais, esconder o seu endereço IP enquanto estiver ligado a redes sem fios não seguras e aceder a conteúdo restrito em certos países. Para evitar um consumo desnecessário de bateria do seu dispositivo, recomendamos que

use o VPN apenas quando precisar, e que o desconecte quando estiver offline.

Por que estou a deparar-me com lentidão na Internet enquanto uso o Bitdefender VPN?

O Bitdefender VPN foi concebido para suavizar a sua experiência enquanto navega na Internet. No entanto, a lentidão pode ser causada pela sua conectividade com a internet ou pela distância do servidor ao qual está ligado. Nesse caso, se não for uma necessidade ligar a um servidor distante com respeito à sua localização (por exemplo, dos EUA ou China), recomendamos que permita ao Bitdefender VPN ligá-lo automaticamente ao servidor mais próximo, ou encontrar um servidor próximo da sua localização atual.

Posso modificar a conta Bitdefender associada ao meu dispositivo?

Sim, pode alterar facilmente a conta Bitdefender associada ao seu dispositivo seguindo estes passos:

1. Abrir o Bitdefender Mobile Security.
2. Pressione o botão **Menu** e selecione **Minha Conta** da lista de opções.
3. Toque em **SAIR** e, em seguida, confirme a sua escolha.
4. Toque em **UTILIZAR CONTA CENTRAL** e, em seguida, introduza o seu novo endereço de e-mail e palavra-passe da conta Bitdefender.

O que é o Administrador do Dispositivo?

O Administrador do Dispositivo é uma função do Android que dá ao Bitdefender Mobile Security as permissões necessárias para realizar determinadas tarefas remotamente. Sem esses privilégios, o bloqueio remoto não funcionaria e a limpeza do dispositivo não conseguiria remover completamente os seus dados. Se pretende remover a aplicação, certifique-se de que retira esses privilégios antes de tentar desinstalar em **Definições > Segurança > Selecione os administradores do dispositivo**.

Para que serve o número de confiança?

Se o seu telefone chegar às mãos de uma pessoa sem a intenção de devolvê-lo ao seu legítimo proprietário, é provável que o cartão SIM seja trocado rapidamente. Sempre que o Bitdefender Mobile Security detetar que o cartão SIM no seu telefone foi alterado, ele irá enviar automaticamente uma mensagem de texto contendo o novo número de telefone para o número que definiu. Deste modo, pode enviar comandos para o seu telefone por

SMS mesmo que o SIM seja trocado e o seu número mude. Pode ser o número de alguém que conheça e confie ou o número de outro telefone que utilize.

O número de confiança pode ser alterado depois de definido?

Para definir um número de confiança diferente:

1. Abrir o Bitdefender Mobile Security.
2. Pressione o botão do **Menu** e selecione **Definições** da lista de opções.
3. Na secção **Anti Furto**, pressione **Número de confiança**.

   O PIN será solicitado para que possa alterar o número de confiança.

Quanto irá custar enviar comandos por SMS?

Os comandos via SMS são enviados como mensagens de texto normais e, portanto, são cobrados como tais pela sua operadora. O Bitdefender não cobra nenhuma taxa adicional.

Como solucionar o erro "Nenhum Token Google" que aparece ao iniciar sessão no Bitdefender Mobile Security.

Este erro ocorre quando o dispositivo não está associado a uma conta Google, ou está associado, mas um problema temporário está a evitar que se ligue ao Google. Tente uma das seguintes soluções:

- Vá para as Definições > do Android; Aplicações > Gerir Aplicações > Bitdefender Mobile Security e toque em **Limpar dados**. Tente iniciar sessão novamente.
- Certifique-se de que o seu dispositivo está associado a uma conta Google.

  Para verificar isto, vá a Definições > Conta & sincronize e veja se a conta Google está listada sob **Gestão de Contas**. dicione a sua conta se não estiver listada, reinicie o seu dispositivo e então tente iniciar sessão no Bitdefender Mobile Security.
- Reinicie o seu dispositivo e, em seguida, tente iniciar sessão novamente.

Em que idiomas é que o Bitdefender Mobile Security está disponível?

Atualmente o Bitdefender Mobile Security está disponível nos seguintes idiomas:

- Brasileiro
- Checo

- Holandês
- Inglês
- Francês
- German
- Grego
- Húngaro
- Italiano
- Japonês
- Coreano
- Polaco
- Português
- Romanian
- Russo
- Spanish
- Tailandês
- Turco
- Vietnamita

Serão adicionados outros idiomas em versões futuras. Para alterar o idioma da interface do Bitdefender Mobile Security, aceda às definições do seu dispositivo **Idioma & teclado** e defina o idioma que pretende utilizar no dispositivo.

CONTACTE-NOS

34. PEDIR AJUDA

O Bitdefender fornece aos seus clientes um nível de suporte rápido e eficaz. Se encontrar algum problema ou se tiver alguma questão sobre o nosso produto Bitdefender, pode utilizar vários recursos online para encontrar uma solução ou resposta. Ou, se preferir, poderá contactar a equipa de Suporte ao Cliente do Bitdefender. Os nossos técnicos de apoio responderão atempadamente às suas questões e dar-lhe-ão a ajuda que precisar.

A secção "*Resolver incidências comuns*" (p. 188) fornece as informações necessárias relativamente às incidências mais frequentes que poderá encontrar ao utilizar este produto.

Se não encontrar a resposta à sua pergunta nos recursos disponibilizados, pode contactar-nos diretamente:

- "Contacte-nos diretamente do seu produto Bitdefender Total Security" (p. 325)
- "Contacte-nos através do nosso Centro de Suporte Online" (p. 326)

Contacte-nos diretamente do seu produto Bitdefender Total Security

Se possuir uma ligação ativa à Internet, pode contactar o apoio do Bitdefender diretamente a partir da interface do produto.

Siga os seguintes passos:

1. Clique no ícone na barra lateral esquerda da interface do Bitdefender.
2. Tem as seguintes opções:
   - **GUIA DO UTILIZADOR**

     Aceda à nossa base de dados e procure a informação necessária.
   - **CENTRO DE SUPORTE**

     Aceda aos nossos artigos e vídeos de tutoriais online.
   - **CONTACTO DE SUPORTE**

     Clique **Contatar Suporte** para executar a Ferramenta de Suporte do Bitdefender e contatar o Departamento de Apoio ao Cliente.

     a. Complete o formulário de envio com os dados necessários:

i. Selecione o tipo de problema que encontrou.

ii. Digite uma descrição do problema encontrado.

iii. Clique em **TENTAR REPRODUZIR ESTE PROBLEMA** caso esteja a encontrar um problema no produto. Continue com os passos necessários.

Aguarde alguns minutos enquanto o Bitdefender reúne informações relacionadas com o produto. Esta informação irá ajudar os nossos engenheiros a encontrar uma solução para o seu problema.

iv. Clique em **CONFIRMAR PEDIDO DE SUPORTE**.

b. Continue a preencher o formulário com os dados necessários:

i. Digite o seu nome completo.

ii. Digite o seu endereço de e-mail.

iii. Marque a caixa de verificação do acordo.

iv. Clique em **ENVIAR PEDIDO DE SUPORTE**.

Aguarde alguns minutos até o seu pedido de suporte ser criado e as informações reunidas serem enviadas para o Departamento de Atendimento ao Cliente do Bitdefender.

c. Clique em **FECHAR** para sair do assistente. Será contactado assim que possível por um dos nossos representantes.

Contacte-nos através do nosso Centro de Suporte Online

Se não conseguir aceder às informações necessárias com o produto Bitdefender, consulte o nosso Centro de Suporte online:

1. Vá para https://www.bitdefender.com/support/consumer.html.

   O Centro de Suporte da Bitdefender possui inúmeros artigos que contêm soluções para incidências relacionadas com o Bitdefender.

2. Utilize a barra de pesquisa na parte superior da janela para encontrar artigos que possam fornecer uma solução definitiva para o seu problema. Para pesquisar, basta digitar o termo na barra de pesquisa e clicar em **Pesquisar**.

3. Leia os artigos ou os documentos e experimente as soluções propostas.
4. Se a solução não resolver o seu problema, aceda a https://www.bitdefender.com/support/contact-us.htmle contate os nossos representantes do suporte.

35. RECURSOS ONLINE

Estão disponíveis vários recursos online para o ajudar a resolver problemas e a responder a questões relacionados com o Bitdefender.

- Centro de Suporte Bitdefender:

  https://www.bitdefender.com/support/consumer.html

- Fórum de Suporte Bitdefender:

  https://forum.bitdefender.com

- o portal de segurança informática HOTforSecurity:

  https://www.hotforsecurity.com

Também pode utilizar o seu motor de busca favorito para saber mais sobre a segurança de computadores, os produtos Bitdefender e a empresa.

35.1. Centro de Suporte Bitdefender

O Centro de Suporte do Bitdefender é um repositóio de informação online sobre os produtos Bitdefender. Armazena, num formato facilmente acessível, apresenta relatórios sobre os resultados do suporte técnico em curso e atividades de correção de falhas do suporte e equipas de desenvolvimento do Bitdefender, para além de artigos mais gerais sobre prevenção de ameaças, a gestão de soluções do Bitdefender com explicações detalhadas e muitos outros artigos.

O Centro de Suporte da Bitdefender está aberto ao público e é pesquisável. A informção extensiva que contém é mais um meio de proporcionar aos clientes do Bitdefender informações técnicas e conhecimento de que necessitam. Todos os pedidos válidos de informação ou relatórios de falhas oriundos de clientes do Bitdefender são eventualmente direcionados para o Centro de Apoio do Bitdefender, como relatórios de correção de falhas, fichas de resolução de problemas ou artigos informacionais como suplemento dos ficheiros de ajuda.

O Centro de Suporte da Bitdefender encontra-se disponível a qualquer altura

https://www.bitdefender.com/support/consumer.html.

35.2. Fórum de Suporte Bitdefender

O Fórum de Suporte do Bitdefender proporciona aos utilizadores do Bitdefender uma forma fácil de obter ajuda e ajudar os outros.

Se o seu produto Bitdefender não estiver a funcionar corretamente, se não conseguir remover determinadas ameaças do seu computador ou se tiver alguma questão sobre a forma como opera, coloque o seu problema ou a sua questão no fórum.

Os técnicos de apoio da Bitdefender supervisionam o fórum, à espera de novas mensagens para fornecer ajuda. Também pode receber uma resposta ou solução de um utilizador mais experiente do Bitdefender.

Antes de publicar o seu problema ou questão, pesquise o fórum por um tópico semelhante ou relacionado.

O Fórum de Suporte do Bitdefender está disponível em https://forum.bitdefender.com, em 5 idiomas diferentes: inglês, alemão, francês, espanhol e romeno. Clique na hiperligação **Proteção Casa & Casa/Escritório** para aceder à secção dedicada aos produtos de consumidor.

35.3. Portal HOTforSecurity

HOTforSecurity é uma fonte rica de informações sobre segurança de computadores. Aqui, pode ficar a conhecer as várias ameaças a que o seu computador fica exposto quando ligado à Internet (malware, phishing, spam, cibercriminosos).

Os novos artigos são publicados regularmente para o manter atualizado sobre as últimas ameaças descobertas, as atuais tendências de segurança e outras informações sobre a indústria de segurança informática.

A página web do HOTforSecurity é https://www.hotforsecurity.com.

36. INFORMAÇÃO DE CONTACTO

Comunicação eficiente é a chave de um negócio bem-sucedido. Desde 2001, a BITDEFENDER estabeleceu uma reputação sólida ao visar constantemente uma melhor comunicação, excedendo, assim, as expetativas dos nossos clientes e parceiros. Por favor não hesite em contactar-nos acerca de qualquer questão ou assunto que nos queira colocar.

36.1. Endereços Web

Departamento Comercial: comercial@bitdefender.pt
Centro de Suporte:https://www.bitdefender.com/support/consumer.html
Documentação: documentation@bitdefender.com
Distribuidores locais:https://www.bitdefender.com/partners
Programa de parcerias: partners@bitdefender.com
Relações com os media: pr@bitdefender.com
Carreiras: jobs@bitdefender.com
Submissões de ameaças: virus_submission@bitdefender.com
Submeter Spam: spam_submission@bitdefender.com
Relatórios de Abusos: abuse@bitdefender.com
Website:https://www.bitdefender.com

36.2. Distribuidores locais

Os distribuidores locais Bitdefender estão preparados para responder a quaisquer dúvidas relacionadas com as suas áreas de operação, quer sejam comerciais ou assuntos gerais.

Para encontrar um distribuidor Bitdefender no seu país:

1. Vá para https://www.bitdefender.com/partners/partner-locator.html.
2. Escolha o seu país e cidade utilizando as opções correspondentes.
3. Se não encontrar um distribuidor Bitdefender no seu país, não hesite em contactar-nos por correio eletrónico através do endereço sales@bitdefender.com. Escreva a sua mensagem em inglês para podermos responder imediatamente.

36.3. Escritórios Bitdefender

Os escritórios locais Bitdefender estão preparados para responder a quaisquer dúvidas relacionadas com as suas áreas de operação, quer sejam

comerciais ou assuntos gerais. Os seus respectivos endereços e contactos estão listados abaixo.

E.U.A.

Bitdefender, LLC
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
Telefone (office&sales): 1-954-776-6262
Vendas: sales@bitdefender.com
Suporte Técnico: https://www.bitdefender.com/support/consumer.html
Web: https://www.bitdefender.com

UK e Irlanda

BITDEFENDER LTD
C/O Howsons Winton House, Stoke Road, Stoke on Trent
Staffordshire, United Kindon, ST4 2RW
Email: info@bitdefender.co.uk
Tel: (+44) 2036 080 456
Vendas: sales@bitdefender.co.uk
Suporte Técnico: https://www.bitdefender.co.uk/support/
Web: https://www.bitdefender.co.uk

Alemanha

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Escritório: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Vendas: vertrieb@bitdefender.de
Suporte Técnico: https://www.bitdefender.de/support/consumer.html
Web: https://www.bitdefender.de

Denmark

Bitdefender APS
Agern Alle 24, 2970 Hørsholm, Denmark
Escritório: +45 7020 2282

Suporte Técnico: http://bitdefender-antivirus.dk/
Web: http://bitdefender-antivirus.dk/

Espanha

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Tel: +34 902 19 07 65
Vendas: comercial@bitdefender.es
Suporte Técnico: https://www.bitdefender.es/support/consumer.html
Website: https://www.bitdefender.es

Roménia

BITDEFENDER SRL
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
Bucharest
Fax: +40 21 2641799
Telefone Comercial: +40 21 2063470
Email vendas: sales@bitdefender.ro
Suporte Técnico: https://www.bitdefender.ro/support/consumer.html
Website: https://www.bitdefender.ro

Emirados Árabes Unidos

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Telefone Comercial: 00971-4-4588935 / 00971-4-4589186
Email vendas: mena-sales@bitdefender.com
Suporte Técnico: https://www.bitdefender.com/support/consumer.html
Website: https://www.bitdefender.com

Glossário

ActiveX

O ActiveX é um modelo para fazer programas de forma a que outros programas e o sistema operativo os possam chamar. A tecnologia do ActiveX é usada com o Microsoft Internet Explorer para criar páginas da Web interactivas, que parecem e comportam-se como programas de computador, em vez de páginas estáticas. Com o ActiveX, os utilizadores podem efectuar perguntas ou responder a questões, usando botões para carregar, e interagir de outras formas com a página da web. Os controlos do ActiveX são frequentemente escritos utilizando o Visual Basic.

O Active X é notável para um leque completo de controlos de segurança; os especialistas de segurança dos computadores desencorajam o seu uso na Internet.

Adware

O adware é com frequência combinado com uma aplicação hospedeira que é fornecida sem custo desde que o utilizador concorde em aceitar o adware. Por causa das aplicações adware serem normalmente instaladas após o utilizador concordar com uma licença de uso que define o propósito da aplicação, nenhuma ilegalidade é na verdade cometida.

No entanto, anúncios tipo pop-up podem tornar-se bastante incomodativos, e em alguns casos podem mesmo degradar a performance do sistema. Também, a informação que algumas dessas aplicações recolhem podem causar algumas preocupações de privacidade aos utilizadores que não estão completamente conscientes dos termos da licença de uso.

Ameaça

Um programa ou um pedaço de código que é carregado no seu computador sem o seu conhecimento e executa-se contra a sua vontade. A maioria das ameaças também se pode replicar. Todas as ameaças de computador são criadas pelo homem. Uma simples ameaça pode copiar-se várias vezes e é relativamente fácil de produzir. Mesmo uma simples ameaça é perigosa porque pode rapidamente utilizar toda memória disponível e fazer o sistema parar. O tipo de ameaça mais

perigoso é aquele que é capaz de se transmitir através de uma rede ou contornando sistemas de segurança.

Ameaça persistente avançada

A ameaça persistente avançada (APA) explora as vulnerabilidades dos sistemas para roubar informações importantes e fornecê-las à fonte. Grandes grupos como organizações, empresas ou governos são os alvos desta ameaça.

O objetivo de uma ameaça persistente avançada é permanecer não detetada durante um longo período de tempo, sendo capaz de monitorizar e recolher informações importantes sem danificar as máquinas atacadas. O método utilizado para injetar a ameaça na rede é através de um ficheiro PDF ou documento do Office que pareça inofensivo, de forma a que todo os utilizadores possam abrir os ficheiros.

Arquivo

Um disco, cassete, ou diretório que contém ficheiros que foram armazenados.

Um ficheiro que contém um ou mais ficheiros num formato comprimido.

Atualização

Uma nova versão de um produto de software ou hardware desenhada para substituir uma versão antiga do mesmo produto. Em adição, a instalação de rotina da actualização verifica se a versão anterior já está instalada no seu computador; se não estiver, não poderá instalar a actualização.

O Bitdefender tem a sua própria funcionalidade de atualização que lhe permite verificar atualizações manualmente, ou permitir atualizar o produto automaticamente.

Atualização das informações sobre a ameaça

O padrão binário de uma ameaça é utilizado pela solução de segurança para detetá-la e eliminá-la.

Botnet

O termo "botnet" é composto pelas palavras "robot" (robô) e "network" (rede). Os botnets são dispositivos ligados à Internet infetados com ameaças e podem ser utilizados para enviar e-mails de spam, roubar dados, controlar remotamente dispositivos vulneráveis e outros tipos

de ameaças. O objetivo é infetado o máximo de dispositivos ligados possível, tais como PC, servidores, dispositivos móveis ou IoT que pertencem a grandes empresas ou indústrias.

Caixa do sistema
Introduzido com o Windows 95, o tabuleiro do sistema está localizado na barra de tarefas do Windows (normalmente em baixo, junto ao relógio) e contém ícones em miniatura para um acesso fácil às funções do sistema, tais como fax, impressora, modem, volume, etc. Faça duplo-clique ou clique com o botão direito sobre o ícone para ver e aceder aos detalhes e controlos.

Caminho
As direcções exactas para um ficheiro num computador. Estas direções são normalmente descritas por meios de preenchimento hierárquico do topo para baixo.

A rota entre dois dados pontos, tal como os canais de comunicação entre dois.

Cliente de mail
Um cliente de e-mail é uma aplicação que lhe permite enviar e receber e-mail.

Código de activação
É um código exclusivo que pode ser adquirido a retalho e utilizado para ativar um produto ou serviço específico. Um código de ativação permite a ativação de uma subscrição válida por um determinado período de tempo e determinados dispositivos, e também pode ser utilizado para prolongar uma subscrição com a condição de ser gerada para o mesmo produto ou serviço.

Componente (drive) do disco
É uma máquina que lê os dados do disco e escreve dados num disco.

Uma componente de disco rígido lê e escreve discos rígidos.

Uma componente de disquetes acede às disquetes.

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

Cookie

Dentro da indústria da Internet, as cookies são descritas como pequenos ficheiros, que contêm informação acerca de computadores individuais, que podem ser analizados e usados pelos publicitários para seguir o rasto online do seus interesses e gostos. Neste domínio, a tecnologia das cookies ainda está a ser desenvolvida e a sua intenção é procurar atingi-lo com publicidade naquilo que disse serem os seus interesses. É uma espada de dois gumes para muitas pessoas, porque, por um lado é eficiente e pertinente já que apenas vê anúncios do seu interesse. Por outro lado, envolve realmente "seguir o rasto" e "perseguir" onde vai e no que clica. Compreensivelmente, existe um debate acerca da privacidade e muitas pessoas sentem-se ofendidas ao terem a noção que estão a ser vistas como um "número SKU " (sabe, o código de barras por detrás das embalagens que é verificado na mercearia). Apesar deste ponto de vista parecer ser extremo, em alguns casos é exacto.

Download

Para copiar dados (normalmente um ficheiro interno) de uma fonte principal para um aparelho periférico. O termo é frequentemente utilizado para descrever o processo de copiar um ficheiro de um serviço online para o seu próprio computador. O download também se pode referir à cópia de um ficheiro de um servidor de ficheiros de rede, para um computador na rede.

Email

Correio electrónico. É um serviço que envia mensagens de computadores via redes locais ou globais.

Escrita

Outro termo para macro ou ficheiro de porção, uma escrita é uma lista de comandos que podem ser executados sem a interação do utilizador.

Eventos

Uma ação ou ocorrência detetada por um programa. Os eventos podem ser ações do utilizador, tais como clicar no botão do rato ou carregar numa tecla, ou ocorrências do sistema, tal como ficar sem memória.

Extensão do nome do ficheiro

A porção de um nome de ficheiro, que segue o ponto final, a qual indica o tipo de dados armazenados no ficheiro.

Muitos sistemas operativos usam extensões do nome do ficheiro, por ex. Unix, VMS, e MS-DOS. Elas são normalmente de uma a três letras (alguns SOs antigos não suportam mais do que três). Os exemplos íncluem ".c" para C de código da fonte, ".ps" para PostScript, ".txt" para texto arbitrário.

Falso positivo

Ocorre quando o verificador identifica um ficheiro como infectado, quando na verdade ele não está.

Ficheiro de reporte

Um ficheiro que lista acções que ocorreram. O Bitdefender um ficheiro de reporte que lista o caminho examinado, as pastas, o número de arquivos e ficheiros examinados, e quantos ficheiros suspeitos e infectados foram encontrados.

Heurístico

Um método baseado em regras de identificação de novas ameaças. Este método de verificação não utiliza uma base de dados de informações de ameaças específico. A vantagem da análise heurística é que não se deixa enganar por uma nova variante de uma ameaça existente. Contudo, pode reportar ocasionalmente códigos suspeitos em programas normais, gerando o chamado "falso positivo".

IP

Internet Protocol - Um rótulo de protocolo no protocolo TCP/IP séquito que é responsável dos endereços de IP, rotas, e a fragmentação e reabertura dos pacotes de IP.

Itens de Arranque

Qualquer ficheiro colocado nesta pasta, irá abrir quando o computador iniciar. Por exemplo, um ecrã de arranque, um ficheiro de som a ser reproduzido quando o computador arranca, um calendário de lembretes ou aplicações podem ser itens de arranque. Normalmente, é colocado um pseudónimo deste ficheiro nesta pasta, em vez do ficheiro em si.

Java applet

Um programa em Java é desenhado para funcionar apenas numa página web. Para usar uma applet numa página web, deverá especificar o nome da applet e o tamanho (comprimento e largura - em pixels) que a applet pode utilizar. Quando a página da web é acedida, o motor de busca

descarrega a applet de um servidor e executa-a na máquina do utilizador (o cliente). As applets diferem das aplicações, pois são administradas por um protocolo de segurança restrito.

Por exemplo, apesar de as applets se executarem no cliente, elas não podem escrever nem ler dados na máquina do cliente. Adicionalmente, as applets são restritas para que possam apenas ler e escrever dados provenientes do mesmo domínio do qual elas são servidas.

Keylogger

Um keylogger é uma aplicação que regista tudo o que digita.

Os keyloggers não são por natureza maliciosos. Podem ser usados com objectivos legítimos, tais como monitorizar a actividade de funcionários ou das crianças. No entanto, são cada vez mais usados por cibercriminosos com objectivos maliciosos (por exemplo, para recolher dados privados, tais como credenciais de acesso e números da segurança social).

Linha de comando

Numa interface de linha do comando, o utilizador introduz comandos no espaço providenciado diretamente no ecrã, usando a linguagem de comando.

Macro vírus

Um tipo de ameaça de computador que está codificado como uma macro retido num documento. Muitas aplicações, tais como Microsoft Word e Excel, contêm poderosas linguagens macro.

Estas aplicações permitem-lhe reter uma macro num documento, e ter a macro pronta a ser executada sempre que o documento for aberto.

Memória

Áreas internas de armazenamento no computador. O termo memória identifica armazenamento de dados que vêm na forma de chips, e a palavra armazenar é usada para a memória que existe em cassetes ou discos. Todo o computador vem com uma certa quantidade de memória física, normalmente referida como memória principal ou RAM.

Minhoca

Um programa que se propaga a si próprio ao longo de uma rede, reproduzindo-se à medida que avança. Não pode ligar-se sozinho a outros programas.

Não-heurístico

Este método de verificação não depende de uma base de dados de informações de ameaças específica. A vantagem da análise não heurística é que não pode ser enganada por algo que pode parecer uma ameaça e não gera falsos alarmes.

Navegador

É um software de aplicação utilizado para localizar e mostrar páginas da Web. Os navegadores mais populares são o Microsoft Internet Explorer, Mozilla Firefox e Google Chrome. Estes são motores de busca gráficos, o que significa que eles tanto podem mostrar gráficos como texto. Em adição, a maioria dos motores de busca modernos podem apresentar informação multimédia, incluíndo som e vídeo, apesar de requererem plug-ins para alguns formatos.

Phishing

O acto de enviar um e-mail onde são proferidas declarações falsas relativamente à origem e natureza do cargo desempenhado pelo remetente, numa tentativa de burlar o remetente e assim obter ilicitamente informação privada que será utilizada em esquemas de roubo de identidade. O email encaminha o utilizador para um site onde lhé solicitada a actualização de informação pessoal - palavras passe, cartão de crédito, segurança social, contas bancárias - que a entidade legítima já possui. O site web, no entanto, é falso e está feito apenas para roubar a informação ao utilizador.

Photon

Photon é uma tecnologia inovadora não intrusiva da Bitdefender, concebida para minimizar o impacto da solução de segurança. Ao monitorizar a atividade do seu PC em segundo plano, ele cria padrões de utilização que ajudam a otimizar os processos de arranque e de análise.

Porta

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

Nas redes TCP/IP e UDP, um ponto final para uma ligação lógica. O número da porta identifica que tipo de porta se trata. Por exemplo, a porta 80 é usada para o tráfego HTTP.

Porta das traseiras

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

Pote de mel

Um sistema de computador "decoy" estabelecido para atrair hackers, destinado a estudar a forma como agem e identificar os métodos que utilizam para recolher informações do sistema. As empresas e corporações estão mais interessadas em implementar e utilizar "potes de mel" para melhorar o seu estado geral de segurança.

Programas compactados

Um ficheiro num formato compactado. Muitos sistemas operativos e aplicações contêm comandos que lhe permitem compactar um ficheiro, para que ocupe menos memória. Por exemplo, suponha que tem um ficheiro de texto contendo dez espaços de caracteres consecutivos. Normalmente, isto iria requerer dez bytes de armazenamento.

Contudo, um programa que compacta ficheiros iria substituir o espaço dos caracteres por uma série-de-espaços de caracteres especial, seguida pelo número de espaços a serem substituidos. Neste caso, os dez espaços iriam requerer apenas dois bytes. Esta é apenas uma técnica de compactar - existem muitas mais.

Ransomware

Ransomware é um programa malicioso que tenta lucrar com os utilizadores através do bloqueio dos seus sistemas vulneráveis.

CryptoLocker, CryptoWall e TeslaWall são apenas algumas variantes que perseguem os sistemas pessoais dos utilizadores.

A infeção pode ser espalhada através do acesso a um e-mail de spam, transferência de anexos de e-mail ou da instalação de aplicações, sem que o utilizador saiba o que está a acontecer no seu sistema. Os utilizadores diários e as empresas são os alvos dos hackers ransomware.

Rede Privada Virtual (VPN)

É uma tecnologia que ativa uma ligação direta temporária e encriptada para uma certa rede sobre uma rede menos segura. Desta forma, enviar e receber dados é seguro e encriptado, difícil de se tornar alvo de espiões. Uma prova de segurança é a autenticação, que pode ser feita somente com a utilização de um nome de utilizador e palavra-passe.

Rootkit

Um rootkit é um pacote de ferramentas de software que proporcionam um nível de acesso de administrador a um sistema. O termo foi usado em primeiro lugar nos sistemas operativos UNIX e referia-se a ferramentas recompiladas que proporcionavam aos intrusos direitos de administração, permitindo-lhes ocultar a sua presença de forma a não serem vistos pelos administradores do sistema.

O papel principal dos rootkits é ocultar processos, ficheiros, logins e registos. Eles também podem intercetar dados dos terminais, ligações de rede ou periféricos, se eles incorporarem o software para tal.

Os rootkits não são maliciosos por natureza. Por exemplo, os sistemas e mesmo algumas aplicações ocultam ficheiros críticos usando rootkits. No entanto, são principalmente utilizados para ocultar ameaças ou esconder a presença de um intruso no sistema. Quando combinados com ameaças, os rootkits são uma grande ameaça à integridade e à segurança de um sistema. Eles podem monitorizar tráfego, criar backdoors no sistema, alterar ficheiros e relatórios e evitarem ser detetados.

Sector de saída

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

Spam

Lixo de correio electrónico ou lixo de avisos de newsgroups. Geralmente atribuído a qualquer e-mail não solicitado.

Spyware

Qualquer software que encobertamente reune informação do utilizador através da ligação à Internet do utilizador sem o seu conhecimento, normalmente para propósitos de publicidade. As aplicações de spyware são tipicamente adicionadas como um elemento oculto de programas freeware ou shareware que podem ser download a partir da Internet; no entanto salientamos que a maioria das aplicações freeware ou shareware não possuem spyware. Uma vez instalado, o spyware monitoriza a actividade do utilizador na Internet e transmite essa informação em background para alguém. O spyware pode também ser capaz de obter endereços de e-mail e até mesmo palavras-passe e números de cartão de crédito.

O spyware é similar a uma ameaça Cavalo de Troia em que os utilizadores o instalam sem saberem, enquanto estão a instalar outra coisa qualquer. Uma forma comum de ser uma vítima de spyware é fazer download de determinado ficheiro peer-to-peer de produtos de swapping que se encontram actualmente disponíveis.

Para além destas questões de ética e privacidade, o spyware priva o utilizador de recursos de memória e também de largura de banda pois para enviar informação do utilizador para a fonte do spyware usa a ligação à Internet do utilizador. Por causa do spyware utilizar memória e recursos do sistema, as aplicações que estão a funcionar em background podem causar crashes no sistema ou uma grande instabilidade geral.

Subscrição

Acordo de compra que dá ao utilizador o direito de utilizar um produto ou serviço específico num número específico de dispositivos e durante um período de tempo determinado. Uma subscrição expirada pode ser automaticamente renovada utilizando as informações fornecidas pelo utilizador na primeira compra.

TCP/IP

Transmission Control Protocol/Internet Protocol - Um conjunto de protocolos de uma rede de trabalho abrangentemente usados Internet

que permite comunicações ao londo de redes de computadores interconectadas com várias arquitecturas de hardware e vários sistemas operaticos. O TCP/IP ínclui padrões de como os computadores comunicam e convenções para ligar redes e conduzir o tráfego.

Tróiano

Um programa destrutivo que se mascara de aplicação benigna. Ao contrário de programas de software maliciosos e worms, os Trojans não se replicam, mas podem ser igualmente destrutivos. Um dos tipos mais insidiosos de ameaças de cavalo de Troia é um programa que afirma remover as ameaças do seu computador, mas, em vez disso, introduz ameaças no seu computador.

O termo provém de uma história da Ilíada de Homero, na qual os Gregos deram um cavalo gigante de Madeira aos seus inimigos, os Troianos, como uma oferta majestosa. Mas após os Troianos levarem o cavalo para dentro das muralhas da sua cidade, os soldados Gregos saíram para fora do cavalo e abriram os portões da cidade, permitindo que os seus compatriotas entrassem e dominassem Tróia.

Vírus de saída

Uma ameaça que infeta o setor de arranque de um disco fixo ou de uma unidade de disquetes. A tentativa de arrancar por uma disquete infetada por um vírus de arranque irá causar a ativação da ameaça em memória. Sempre que iniciar o seu sistema a partir daquele ponto, terá a ameaça ativa em memória.

Vírus polimórfico

Uma ameaça que muda a sua forma com cada ficheiro que infeta. Como não têm um padrão binário consistente, essas ameaças são difíceis de identificar.