Bitdefender ANTIVIRUS PLUS

MANUAL DO UTILIZADOR

Bitdefender Antivirus Plus
Manual do Utilizador

Editado 07/20/2020

Aviso Legal

Bitdefender

Índice

Instalação 1

1. A preparar a instalação 2
2. Requisitos do sistema 3
   2.1. Requisitos de Software 3
3. Instalação do seu produto Bitdefender 5
   3.1. Instalar da Bitdefender Central 5
   3.2. Instalar a partir do disco de instalação 8

Introdução 13

4. Os básicos 14
   4.1. A abrir a janela do Bitdefender 15
   4.2. Notificações 16
   4.3. Perfis 17
      4.3.1. Configure a ativação automática de perfis 17
   4.4. Definições de proteção da palavra-passe de Bitdefender 18
   4.5. Relatórios do produto 19
   4.6. Notificações de ofertas especiais 19
5. Interface Bitdefender 20
   5.1. Ícone na área de notificação 20
   5.2. Menu de navegação 22
   5.3. Painel 23
      5.3.1. Área de estado de segurança 23
      5.3.2. Autopilot 23
      5.3.3. Ações rápidas 24
   5.4. As secções do Bitdefender 25
      5.4.1. **Proteção** 26
      5.4.2. **Privacidade** 27
      5.4.3. **Utilitários** 28
   5.5. Mude o idioma do produto 28
6. Bitdefender Central 30
   6.1. A aceder Bitdefender Central 30
   6.2. Autenticação de dois fatores 31
      6.2.1. Adicionar dispositivos fiáveis 33
   6.3. As minhas subscrições 33
      6.3.1. Verificar subscrições disponíveis 33
      6.3.2. Adicionar um novo dispositivo 34
      6.3.3. Renovar subscrição 35
      6.3.4. Ativar subscrição 35
   6.4. Meus dispositivos 35
   6.5. Actividade 38
   6.6. Notificações 38

7. Mantenha o seu Bitdefender atualizado. 39
7.1. Verifique se o Bitdefender está atualizado 39
7.2. A efetuar uma atualização 40
7.3. Ligar ou desligar a atualização automática 40
7.4. Ajuste das configurações da atualização 41
7.5. Atualizações contínuas 42

Como 43

8. Instalação 44
8.1. Como instalar o Bitdefender num segundo dispositivo? 44
8.2. Como posso reinstalar Bitdefender? 44
8.3. Onde posso transferir o meu produto Bitdefender? 45
8.4. Como é que posso alterar o idioma do meu produto Bitdefender? 46
8.5. Como utilizo a minha subscrição do Bitdefender após uma atualização do Windows? 46
8.6. Como posso atualizar para a mais recente versão de Bitdefender? 49

9. Bitdefender Central 51
9.1. Como faço para iniciar sessão na conta da Bitdefender com outra conta? 51
9.2. Como é que desativo as mensagens de ajuda da Bitdefender Central? 51
9.3. Esqueci-me da palavra-passe que defini para a minha conta Bitdefender. Como é que a reponho? 52
9.4. Como posso gerir os inícios de sessão associados à minha conta do Bitdefender? 53

10. A analisar com Bitdefender 54
10.1. Como posso analisar um ficheiro ou uma pasta? 54
10.2. Como posso analisar o seu sistema? 54
10.3. Como programar uma verificação? 54
10.4. Como posso criar uma tarefa de análise personalizada? 55
10.5. Como excluir uma pasta da análise? 57
10.6. O que fazer se o Bitdefender identificar um ficheiro limpo como infectado? 58
10.7. Como posso saber que ameaças o Bitdefender detetou? 59

11. Privacy protection 60
11.1. Como posso ter a certeza de que a minha transação online é segura? 60
11.2. Como removo um ficheiro permanentemente com o Bitdefender? 60
11.3. Como posso restaurar manualmente ficheiros encriptados quando o processo de restauração falhar? 61

12. Informações Úteis 62
12.1. Como posso testar a minha solução de segurança? 62
12.2. Como posso remover o Bitdefender? 62
12.3. Como removo o Bitdefender VPN? 63
12.4. Como é que removo a extensão Antitracker da Bitdefender? 64
12.5. Como desligo automaticamente o meu dispositivo após terminar a análise? 65
12.6. Como posso configurar Bitdefender para usar um proxy de ligação à Internet? 66
12.7. Estou a utilizar uma versão de 32 ou 64 Bit do Windows? 67

12.8. Como posso mostrar objetos ocultos no Windows? ... 68
12.9. Como posso remover outras soluções de segurança? ... 69
12.10. Como posso reiniciar no Modo de Segurança? ... 70

Gerir a sua segurança ... 72

13. Proteção Antivírus ... 73
13.1. Análise no acesso (proteção em tempo real) ... 74
13.1.1. Ligar ou desligar a proteção em tempo real ... 74
13.1.2. Configuração das definições avançadas de proteção em tempo real ... 74
13.1.3. Restaurar as predefinições ... 78
13.2. Verificação por ordem ... 78
13.2.1. Procurar ameaças num ficheiro ou pasta ... 78
13.2.2. Executar uma Análise Rápida ... 79
13.2.3. Executar uma Análise do Sistema ... 79
13.2.4. Configurar uma análise personalizada ... 80
13.2.5. Assistente de Análise Antivírus ... 83
13.2.6. Ver os relatórios da análise ... 87
13.3. Análise automática de média removíveis ... 87
13.3.1. Como funciona? ... 88
13.3.2. Gerir análise de média removível ... 89
13.4. Analisar ficheiro hosts ... 89
13.5. A configurar exceções de análise ... 89
13.5.1. Excluindo ficheiros e pastas da análise ... 90
13.5.2. Excluir extensões de ficheiros da análise ... 90
13.5.3. Ativar exceções de análise ... 91
13.6. Gerir ficheiros da quarentena ... 92

14. Advanced Threat Defense ... 94
14.1. Ativar ou desativar o Advanced Threat Defense ... 94
14.2. A verificar ataques maliciosos detectados ... 94
14.3. A adicionar processos a exceções ... 95
14.4. Deteção de exploits ... 95

15. Prevenção de Ameaças Online ... 97
15.1. Alertas de Bitdefender no navegador ... 98

16. Vulnerabilidade ... 100
16.1. Procurar vulnerabilidades no seu sistema ... 100
16.2. Usar monitorização de vulnerabilidade automática ... 102
16.3. Consultor Segurança Wi-Fi ... 104
16.3.1. Ativar ou desativar as notificações do Consultor de Segurança Wi-Fi ... 105
16.3.2. Configurar a rede Wi-Fi doméstica ... 105
16.3.3. Configurar a rede Wi-Fi do trabalho ... 106
16.3.4. Wi-Fi público ... 106
16.3.5. Verificar informações sobre redes Wi-Fi ... 107

17. Remediação de Ransomware ... 109
17.1. Ativar ou desativar a Remediação de Ransomware ... 109
17.2. A ativar ou desativar a restauração automática ... 109
17.3. Ver ficheiros restaurados automaticamente ... 109

17.4. Restauração manual de ficheiros encriptados ... 110
17.5. Adicionar aplicações às exceções ... 111

18. Proteção do Gestor de palavras-passe para as suas credenciais ... 112
18.1. Criar uma nova base de dados Carteira ... 113
18.2. Importar uma base de dados existente ... 113
18.3. Exportar a base de dados da Carteira ... 114
18.4. Sincronize as suas carteiras na nuvem ... 114
18.5. Gerir as suas credenciais da Carteira ... 115
18.6. Ativar ou desativar a proteção do Gestor de palavras-passe ... 116
18.7. Gerir as definições do Gestor de Palavras-passe ... 116

19. Antitracker ... 120
19.1. Interface do Antitracker ... 120
19.2. Desligar o Antitracker da Bitdefender ... 121
19.3. Permitir a monitorização de um site ... 121

20. VPN ... 123
20.1. A abrir a VPN ... 123
20.2. Interface da VPN ... 123
20.3. Assinaturas ... 125

21. Segurança Safepay para transações online ... 126
21.1. A utilizar o Bitdefender Safepay™ ... 127
21.2. Configurar definições ... 128
21.3. Gerir bookmarks ... 129
21.4. Desligar as notificações do Safepay ... 130
21.5. Utilizar VPN com o Safepay ... 130

22. USB Immunizer ... 131

Utilitários ... 132

23. Perfis ... 133
23.1. Perfil Trabalho ... 134
23.2. Perfil de Filme ... 135
23.3. Perfil de Jogo ... 136
23.4. Perfil Wi-Fi Público ... 137
23.5. Perfil do Modo de Bateria ... 138
23.6. Otimização em tempo real ... 139

24. Proteção de dados ... 140
24.1. Apagar ficheiros permanentemente ... 140

Solução de problemas ... 142

25. Resolver incidências comuns ... 143
25.1. O meu sistema parece estar lento ... 143
25.2. A análise não inicia ... 144
25.3. Já não posso utilizar uma aplicação ... 147

25.4. O que fazer quando a Bitdefender bloqueia um site, domínio, endereço de IP ou aplicação online segura ... 148
25.5. Como atualizar o Bitdefender numa ligação à Internet lenta ... 149
25.6. Os serviços Bitdefender não estão a responder ... 149
25.7. A funcionalidade Preenchimento automático na minha Carteira não funciona ... 150
25.8. Remoção de Bitdefender falhou ... 151
25.9. O meu sistema não reinicia após a instalação de Bitdefender ... 152
26. Remover ameaças do seu sistema ... 156
26.1. Ambiente de Resgate ... 156
26.2. O que fazer quando o Bitdefender encontra ameaças no seu dispositivo? ... 157
26.3. Como posso limpar uma ameaça num ficheiro? ... 159
26.4. Como posso limpar uma ameaça num ficheiro de e-mail? ... 160
26.5. O que fazer se suspeitar que um ficheiro é perigoso? ... 161
26.6. O que são os ficheiros protegidos por palavra-passe no relatório de análise? ... 161
26.7. O que são os itens ignorados no relatório de análise? ... 162
26.8. O que são os ficheiros muito comprimidos no relatório de análise? ... 162
26.9. Por que é que Bitdefender eliminou automaticamente um ficheiro infectado? ... 162
Contact us ... 163
27. Pedir Ajuda ... 164
28. Recursos online ... 167
28.1. Centro de Suporte Bitdefender ... 167
28.2. Fórum de Suporte Bitdefender ... 168
28.3. Portal HOTforSecurity ... 168
29. Contact information ... 169
29.1. Endereços Web ... 169
29.2. Distribuidores locais ... 169
29.3. Escritórios Bitdefender ... 169
Glossário ... 172

INSTALAÇÃO

1. A PREPARAR A INSTALAÇÃO

Antes de instalar o Bitdefender Antivirus Plus, complete estes procedimentos para assegurar uma boa instalação:

- Assegure-se que o dispositivo onde deseja instalar o Bitdefender tem os requisitos de sistema mínimos. Caso o dispositivo não cumpra os requisitos de sistema, o Bitdefender não será instalado ou caso seja instalado, não irá trabalhar de forma apropriada e irá causar lentidão e instabilidade do sistema. Para ver a lista completa dos requisitos mínimos do sistema, consulte o "*Requisitos do sistema*" (p. 3).
- Ligue-se ao dispositivo utilizando uma conta de Administrador.
- Remova quaisquer outros softwares semelhantes do seu dispositivo. 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.
- Recomenda-se que o seu dispositivo esteja ligado à Internet durante a instalação, mesmo quando realizar 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.

2. REQUISITOS DO SISTEMA

Só pode instalar o Bitdefender Antivirus Plus nos dispositivos que tenham os seguintes sistemas operativos:

- Windows 7 com o Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10

- 2,5 GB de espaço disponível em disco rígido (pelo menos 800 MB na unidade do sistema)
- 2 GB de memória (RAM)

Importante
O desempenho do sistema pode ser afetado em dispositivos com CPUs de geração antiga.

Nota
Para saber qual é o sistema operativo Windows executado no seu dispositivo 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.

2.1. Requisitos de Software

Para conseguir utilizar o Bitdefender e todas as suas funcionalidades, o seu dispositivo 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

3. INSTALAÇÃO DO SEU PRODUTO BITDEFENDER

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

Se a sua compra abrange mais do que um dispositivo (por exemplo, adquiriu o Bitdefender Antivirus Plus para 3 PCs), repita o processo de instalação e ative o seu produto com a mesma conta em cada um dos dispositivos. A conta a ser utilizada deve ser igual à que contém a sua subscrição ativa do Bitdefender.

3.1. 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 Antivirus Plus é ativado.

Para transferir o Bitdefender Antivirus Plus da Bitdefender Central:

1. Aceda Bitdefender Central.
2. Selecione o painel **Os meus dispositivos**, e clique em **INSTALAR PROTEÇÃO**.
3. Escolha uma das duas opções disponíveis:
   - **Proteger este dispositivo**
     a. Selecione esta opção e, em seguida, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique no botão correspondente.
     b. Guarde o ficheiro de instalação.
   - **Proteger outros dispositivos**
     a. Selecione esta opção e, em seguida, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique no botão correspondente.
     b. Prima **ENVIAR HIPERLIGAÇÃO DE DOWNLOAD**.
     c. Escreva um endereço de email no campo correspondente e clique em **ENVIAR EMAIL**.

Observe que a hiperligação de download gerada será válida apenas durante as próximas 24 horas. Se a hiperligação expirar, precisará de gerar uma nova seguindo os mesmos passos.

d. No dispositivo em que deseja instalar o seu produto Bitdefender, verifique a conta de e-mail que escreveu e clique no botão de download correspondente.

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 do sistema para a instalação Bitdefender, será informado das áreas que precisam 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 dispositivo para concluir a remoção das soluções de segurança detetadas.

O pacote de instalação do Bitdefender Antivirus Plus 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 Antivirus Plus.

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 Antivirus Plus.

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 de produto** 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.

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.

Passo 4 - Análise do dispositivo

Agora ser-lhe-á perguntado se deseja realizar uma análise do seu dispositivo, para garantir que ele está seguro. Durante este passo, o Bitdefender irá verificar áreas críticas do sistema. Clique em **Iniciar análise de dispositivo** para a iniciar.

Pode ocultar a interface da análise ao clicar em **Executar análise em segundo plano**. Em seguida, escolha se deseja ser informado quando a análise terminar ou não.

Quando a análise estiver concluída, clique em **Abrir Interface do Bitdefender**.

Nota
Como alternativa, se não deseja realizar a análise, basta clicar em **Ignorar**.

Passo 5 - Introdução

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

Clique em **FINALIZAR** para aceder à interface do Bitdefender Antivirus Plus.

3.2. 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 do sistema para a instalação Bitdefender, será informado das áreas que precisam 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 dispositivo 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 Antivirus Plus.

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 Antivirus Plus.

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 de produto** 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.

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.

Passo 4 - Análise do dispositivo

Agora ser-lhe-á perguntado se deseja realizar uma análise do seu dispositivo, para garantir que ele está seguro. Durante este passo, o Bitdefender irá verificar áreas críticas do sistema. Clique em **Iniciar análise de dispositivo** para a iniciar.

Pode ocultar a interface da análise ao clicar em **Executar análise em segundo plano**. Em seguida, escolha se deseja ser informado quando a análise terminar ou não.

Quando a análise estiver concluída, clique em **Continuar com a Criação da conta**.

Nota
Como alternativa, se não deseja realizar a análise, basta clicar em **Ignorar**.

Passo 5 - Conta Bitdefender

Após completar a configuração inicial, aparecerá a janela da Conta do Bitdefender. É necessária uma conta Bitdefender para ativar o produto e utilizar as suas ferramentas online. Para mais informação, dirija-se a "*Bitdefender Central*" (p. 30).

Proceda consoante a sua situação.

- **Quero criar uma conta Bitdefender**

  1. Digite as informações solicitadas nos campos correspondentes. Os dados que nos fornecer serão mantidos confidenciais. A palavra-passe deve ter no mínimo 8 carateres, incluindo pelo menos um número ou símbolo, um carater minúsculo e um maiúsculo.
  2. Antes de continuar, deve concordar com os Termos de utilização. Aceda aos Termos de Utilização e leia-os com atenção, pois eles contêm os termos e condições segundo os quais pode utilizar o Bitdefender.

     Além disso, pode aceder e ler a Política de Privacidade.
  3. Clique em **CRIAR CONTA**.

  Nota
  Uma vez que a conta for criada, pode utilizar o endereço de e-mail e palavra-passe fornecidos para entrar na sua conta em https://central.bitdefender.com, ou na aplicação da Bitdefender Central, desde que esteja instalado num dos seus dispositivos Android ou iOS. Para instalar a app Bitdefender Central no Android, precisa de aceder ao Google Play, pesquisar por Bitdefender Central e, em seguida, tocar na opção de instalação correspondente. Para instalar a app Bitdefender Central no iOs, precisa de aceder à App Store, pesquisar por Bitdefender Central e, em seguida, tocar na opção de instalação correspondente.

- **Já tenho uma conta Bitdefender**

  1. Clique em **Sign in**.

2. Introduza o endereço de e-mail no campo correspondente e clique em **PRÓXIMO**.
3. Introduza a sua palavra-passe e depois clique em **ENTRAR**.

   Se tiver esquecido a palavra-passe da sua conta ou caso queira repô-la:

   a. Clique em **Esqueceu a palavra-passe?**.

   b. Introduza o seu endereço de e-mail e depois clique em **PRÓXIMO**.

   c. Verifique a sua conta de e-mail, introduza o código de segurança que recebeu e depois clique em **PRÓXIMO**.

      Ou pode clicar em **Alterar palavra-passe** no e-mail que recebeu.

   d. Introduza a nova palavra-passe que pretende definir e, em seguida, introduza-a novamente. Clique em **GUARDAR**.

> **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 6 - 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 7 - Introdução

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

Clique em **FINALIZAR** para aceder à interface do Bitdefender Antivirus Plus.

INTRODUÇÃO

4. OS BÁSICOS

Uma vez instalado o Bitdefender Antivirus Plus, o seu dispositivo fica protegido contra todos os tipos de ameaças (como malware, spyware, ransomware, exploits, botnets e cavalos de Troia).

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. A razão principal é porque defraudadores 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. 123).

Pode controlar as suas palavras-passe e contas online armazenando-as "*Proteção do Gestor de palavras-passe para as suas credenciais*" (p. 112) numa carteira. Com uma única palavra-passe principal pode proteger a sua privacidade contra intrusos que podem tentar deixá-lo sem dinheiro.

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 Segurança Wi-Fi*" (p. 104).

Agora ficheiros encriptados por ransomware podem ser recuperados sem que precise de gastar dinheiro para qualquer resgate exigido. Para informações sobre como recuperar ficheiros encriptados, veja "*Remediação de Ransomware*" (p. 109).

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. 133).

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. 16).

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 dispositivo e os seus dados.

Para utilizar as funcionalidades online do Bitdefender Antivirus Plus, gerir as suas subscrições e os dispositivos, aceda à sua conta Bitdefender. Para mais informação, dirija-se a "*Bitdefender Central*" (p. 30).

A "Como" (p. 43) 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. 143) secção de possíveis soluções para os problemas mais comuns.

4.1. A abrir a janela do Bitdefender

Para aceder à interface principal do Bitdefender Antivirus Plus, clique no ícone no seu ambiente de trabalho.

Se necessário, também pode seguir os passos abaixo:

- No **Windows 7**:
  1. Clique em **Iniciar** e vá para **Todos os Programas**.
  2. Clique em **Bitdefender**.
  3. Clique em **Bitdefender Antivirus Plus** 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. 20).

4.2. Notificações

O Bitdefender mantém um registo detalhado dos eventos relacionados com a sua atividade no seu dispositivo. 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 dispositivo, etc. Adicionalmente, pode realizar outras ações, se necessário, ou alterar ações tomadas pelo Bitdefender.

Para aceder ao registo de notificações, clique em **Notificações** no menu de navegação da interface do Bitdefender. Sempre que acontecer este evento crítico, pode ser observado um contador no ícone 2.

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.

4.3. 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.

4.3.1. 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.

A primeira vez que aceder os **Perfis** será solicitado a ativar os perfis automáticos. Para fazer isso, pode simplesmente clicar em **ATIVAR** na janela mostrada.

Pode clicar em **AGORA NÃO** se quiser ativar a funcionalidade mais tarde.

Para permitir que o Bitdefender ative perfis automaticamente:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Perfis**, clique em **Definições**.
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, ligue o botão correspondente. Dos primeiros três perfis, apenas um pode ser manualmente ativado imediatamente.

Para mais informações sobre Perfis, aceda a"*Perfis*" (p. 133)

4.4. Definições de proteção da palavra-passe de Bitdefender

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

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

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. Na janela **Geral**, ative a **Proteção por palavra-passe**.
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 em **Definições** no menu de navegação na interface do Bitdefender.
2. Na janela **Geral**, desative a **Proteção por palavra-passe**.

3. Digite a palavra-passe e, em seguida, clique em **OK**.

> **Nota**
> Para alterar a palavra-passe do seu produto, clique em **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.

4.5. Relatórios do produto

Os relatórios do produto contêm informações sobre como utiliza o produto Bitdefender instalado. 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.

Se durante o processo de instalação tiver escolhido enviar relatórios aos servidores Bitdefender e agora gostaria de interromper o processo:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. Selecione o separador **Avançado**.
3. Desligue **Relatórios do produto**.

4.6. 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 em **Definições** no menu de navegação na interface do Bitdefender.
2. Na janela **Geral**, ative ou desative o botão correspondente.

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

5. INTERFACE BITDEFENDER

O Bitdefender Antivirus Plus 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 o ícone do ângulo direito para continuar a ser guiado ou **Ignorar** para fechar o assistente.

O ícone na bandeja do sistema do Bitdefender está disponível a qualquer momento, não importa se quiser abrir a janela principal, realizar uma atualização do produto ou ver informações sobre a versão instalada.

A janela principal fornece informações relevantes sobre o seu estado de segurança. Com base nas necessidades e utilização do seu dispositivo, o Autopilot exibe aqui diferentes tipos de recomendação para ajudá-lo a melhorar a segurança e desempenho do seu dispositivo. Além disso, pode adicionar ações rápidas que utiliza mais, para que as tenha à disposição sempre que precisar.

No menu de navegação do lado esquerdo, pode aceder à área de definições, notificações e as sessões do Bitdefender para definições detalhadas e tarefas administrativas avançadas.

Na parte superior da interface principal, pode aceder à sua conta Bitdefender. E também pode nos contactar para obter suporte caso tenha perguntas ou algo inesperado apareça.

5.1. 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:

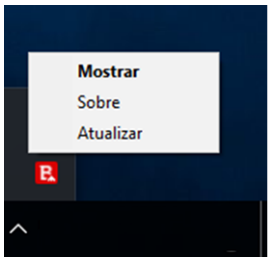
- No **Windows 7, Windows 8 e Windows 8.1**:
  1. Clique na seta no canto inferior direito do écran.
  2. Clique **Personalizar...** para abrir a janela de ícones da Área de Notificação.

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 **Definições da barra de tarefas**.
2. Desça e clique na hiperligação **Selecione os ícones que aparecem na barra de tarefas** sob **Área de notificações**.
3. 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.



Tray Icon

- **Mostrar** - abre a janela principal do Bitdefender.
- **Informação** - abre uma janela na qual poderá consultar informação sobre o Bitdefender, onde procurar ajuda se acontecer algo inesperado, onde aceder e visualizar o Acordo de Subscrição, os Componentes de Terceiros e a Política de Privacidade.
- **Atualizar agora** - executa uma atualização imediata. Pode seguir o estado das atualizações no painel de Atualizações da janela principal do Bitdefender.

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

Nenhum problema está a afetar a segurança do seu sistema.
Problemas críticos estão a afetar a segurança do seu sistema. Eles requerem atenção imediata e devem ser reparados o mais breve possível.

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.

5.2. Menu de navegação

No lado esquerdo da interface do Bitdefender está o menu de navegação, que lhe permite aceder rapidamente aos recursos e ferramentas do Bitdefender que precisa para utilizar o seu produto. Os separadores disponíveis nesta área são:

- **Painel**. Daqui, pode reparar rapidamente problemas de segurança, ver recomendações de acordo com as necessidades do seu sistema e padrões de utilização e realizar ações rápidas.
-
- **Proteção**. Aqui, pode executar e configurar análises antivírus, recuperar dados encriptados por ransomware e configurar a proteção enquanto navega na internet.
- **Privacidade**. Aqui, pode criar gestores de palavra-passe para as suas contas online, fazer pagamentos online num ambiente seguro e abrir a aplicação do VPN.
- **Utilidades**. Aqui, pode gerir perfis e aceder à funcionalidade de Proteção de Dados.
- **Notificações**. A partir daqui pode aceder às notificações geradas.
- **Definições**. A partir daqui pode aceder às definições gerais.

No lado superior da interface principal, encontrará as funcionalidades **A Minha Conta** e **Suporte**.

- **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 Antivirus Plus.
- **A minha conta**. Daqui, pode aceder à sua conta Bitdefender para verificar as suas subscrições e realizar tarefas de segurança nos dispositivos que controla. Detalhes sobre a conta Bitdefender e subscrição em utilização também estão disponíveis.

5.3. Painel

A janela do painel 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 é organizada em três áreas principais:

Área de estado de segurança
: É aqui que pode conferir o estado de segurança do seu dispositivo.

Autopilot
: Aqui é onde pode conferir as recomendações do Autopilot para assegurar uma funcionalidade adequada do sistema.

Ações rápidas
: Aqui pode executar diferentes tarefas para manter o seu sistema protegido.

5.3.1. Área de estado de segurança

O Bitdefender utiliza um sistema de emissão de monitorização para detetar e informá-lo sobre os problemas que podem afetar a segurança do seu dispositivo e dos seus dados. As incidências detetadas incluem definições de proteção importantes que estão desligadas e outras condições que podem representar um risco de segurança.

Sempre que problemas afetarem a segurança do seu dispositivo, o estado que aparece na parte superior da Interface do Bitdefender muda para vermelho. O estado exibido indica a natureza do problema a afetar o seu sistema. Além disso, o ícone na bandeja do sistema muda para e se mover o cursor sobre o ícone, uma pop-up confirmará a existência de problemas pendentes.

Como os problemas pendentes podem impedir que o Bitdefender o proteja contra ameaças ou representam um grande risco de segurança, recomendamos que esteja atento e os repare o mais depressa possível. Para reparar um problema, clique no botão próximo ao problema detetado.

5.3.2. Autopilot

Para lhe oferecer uma operação efetiva e proteção reforçada enquanto realiza diferentes atividades, o Bitdefender Autopilot agirá como o seu

consultor de segurança pessoal. Dependendo da atividade que realizar, seja trabalhar, fazer pagamentos online, ver filmes ou jogar, o Bitdefender Autopilot fornecerá recomendações contextuais com base na utilização e necessidades do seu dispositivo. As recomendações propostas também podem estar relacionadas às ações que precisa de executar para manter o seu produto a funcionar na capacidade máxima.

Para começar a utilizar um recurso sugerido ou a fazer melhorias no seu produto, clique no botão correspondente.

Desligar as notificações do Autopilot

Para chamar a sua atenção para as recomendações do Autopilot, o Bitdefender é configurado para notificá-lo por meio de uma janela pop-up.

Para desligar as notificações do Autopilot:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. Na janela **Geral**, desative as **Notificações de recomendações**.

5.3.3. Ações rápidas

Utilizando as ações rápidas, pode executar com rapidez tarefas que considera importantes para manter o seu sistema protegido e melhorar a sua forma de trabalhar.

O Bitdefender vem com algumas ações rápidas de fábrica que podem ser substituídas por aquelas que utiliza mais. Para substituir uma ação rápida:

1. Clique no ícone no canto superior direito do cartão que deseja remover.
2. Selecione a tarefa que deseja adicionar à interface principal, em seguida, clique em **ADICIONAR**.

As tarefas que pode adicionar à interface principal são:

- **Análise Rápida**. Realizar uma verificação rápida para detetar imediatamente as possíveis ameaças que podem estar presentes no seu dispositivo.
- **Análise do Sistema**. Execute uma análise do sistema para garantir que o dispositivo está livre de ameaças.
- **Ver Vulnerabilidades**. Verifique o seu dispositivo para identificar vulnerabilidades e assegurar que todos as aplicações instaladas, além do sistema operacional, estão atualizadas e a funcionar corretamente.

- **Consultor de Segurança do Wi-Fi**. Abra a janela do Consultor de Segurança do Wi-Fi no módulo de Vulnerabilidade.
- **Carteiras**. Veja e administre as suas carteiras.
- **Abrir Safepay**. Abra o Bitdefender Safepay™ para proteger os seus dados pessoais enquanto efetua transações online.
- **Abrir a VPN**. Abra o Bitdefender VPN para adicionar uma camada extra de proteção enquanto está ligado à Internet.
- **Destruidor de Ficheiros**. Abra o Destruidor de Ficheiros para remover os traços de dados sensíveis do seu dispositivo.

Para começar a proteger dispositivos adicionais com o Bitdefender:

1. Clique em **Instalar noutro dispositivo**.

   Aparece uma nova janela no seu ecrã.

2. Clique em **PARTILHAR HIPERLIGAÇÃO DE TRANSFERÊNCIA**.

3. Siga os passos no ecrã para instalar o Bitdefender.

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

- Bitdefender Antivirus Plus nos dispositivos Windows.
- Bitdefender Antivirus for Mac em dispositivos macOS.
- Bitdefender Mobile Security nos dispositivos Android.
- Bitdefender Mobile Security em dispositivos iOS.

5.4. 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 no menu de navegação da interface do Bitdefender:

-  Proteção
-  Privacidade
-  Utilitários

5.4.1. Proteção

Na secção de Proteção, pode configurar as definições avançadas de segurança, funcionalidades de Prevenção contra ameaças online, verificar e reparar potenciais vulnerabilidades do sistema e avaliar a segurança das redes 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
- Ambiente de Resgate

Para mais informações sobre tarefas de análise e como configurar a proteção antivírus, consulte "*Proteção Antivírus*" (p. 73).

PREVENÇÃO CONTRA AMEAÇAS ONLINE

A Prevenção contra ameaças online 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 "*Prevenção de Ameaças Online*" (p. 97).

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. 94).

VULNERABILIDADE

O módulo Vulnerabilidade ajuda a manter o seu sistema operativo e as aplicações que utiliza regularmente atualizados e a identificar as redes

sem fio inseguras às quais se liga. Clique em **Abrir** no módulo de Vulnerabilidade para aceder às suas funcionalidades.

A funcionalidade de **Análise de Vulnerabilidades** permite identificar atualizações essenciais do Windows, atualizações de aplicações, palavras-passe fracas pertencentes a contas do Windows e redes sem fios que não são seguras. Clique em **Iniciar Análise** para realizar uma análise no seu dispositivo.

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

Para mais informações sobre como configurar a proteção de vulnerabilidade, consulte "*Vulnerabilidade*" (p. 100).

REMEDIAÇÃO DE RANSOMWARE

A ferramenta de Remediação de Ransomware ajuda a recuperar ficheiros caso eles sejam encriptados por ransomware.

Para informações sobre como recuperar ficheiros encriptados, veja "*Remediação de Ransomware*" (p. 109).

5.4.2. Privacidade

Na seção de privacidade, pode abrir o Bitdefender VPN, proteger as suas transações online e manter a sua navegação segura.

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. 123).

PASSWORD MANAGER

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. 112).

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.

Para mais informações sobre o Bitdefender Safepay™, consulte "*Segurança Safepay para transações online*" (p. 126).

ANTITRACKER

A funcionalidade Antitracker ajuda-o a evitar o tráfico, para que os seus dados permaneçam privados enquanto navega online e ainda reduz o tempo que os websites demoram a carregar.

Para obter mais informações sobre a funcionalidade Antitracker, consulte "*Antitracker*" (p. 120).

5.4.3. Utilitários

Proteção de dados

O Destruidor de Ficheiros do Bitdefender ajuda a eliminar permanentemente dados removendo-os fisicamente do seu disco rígido.

Para mais informações, dirija-se a "*Proteção de dados*" (p. 140).

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.

Para mais informações sobre esta funcionalidade, consulte "*Perfis*" (p. 133).

5.5. Mude o idioma do produto

A interface do Bitdefender está disponível em várias línguas e pode ser alterada ao seguir os passos seguintes:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. Na janela **Geral**, clique em **Alterar língua**.
3. Selecione a língua desejada na lista e, em seguida, clique em **GUARDAR**.
4. Aguarde alguns momentos até que sejam aplicadas as definições.

6. BITDEFENDER CENTRAL

Bitdefender Central é a plataforma onde tem acesso às funções e serviços online do produto, e pode realizar remotamente tarefas importantes nos dispositivos em que o Bitdefender estiver instalado. Pode aceder à sua conta Bitdefender desde qualquer dispositivo ligado à internet, indo para https://central.bitdefender.com, ou diretamente pela aplicação da Bitdefender Central em dispositivos Android e iOS.

Para instalar a aplicação da Bitdefender Central nos seus dispositivos:

- **No Android** - procure por Bitdefender Central no Google Play e descarregue e instale a aplicação Siga os passos necessários para completar a instalação.
- **No iOS** - procure por Bitdefender Central na App Store e descarregue e instale a aplicação. Siga os passos necessários para completar a instalação.

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 Antivirus Plus
  - O Antivírus Bitdefender para Mac
  - Bitdefender Mobile Security para Android
  - Bitdefender Mobile Security for iOS
- Gerir e renovar as suas subscrições do Bitdefender.
- Adicionar novos dispositivos à sua rede e gerir as suas funcionalidades onde quer que esteja.

6.1. A aceder Bitdefender Central

Existem diversas formas de aceder à Bitdefender Central:

- A partir da interface principal do Bitdefender:
  1. Clique em **Minha Conta** no menu de navegação da interface do Bitdefender.
  2. Clique em **Ir para a Central 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.
- No seu dispositivo Android ou iOS:

  Abra a aplicação da Bitdefender Central que instalou.

Nota
Neste material, recebe as opções e instruções disponíveis na plataforma web.

6.2. Autenticação de dois fatores

O método de autenticação em 2 fatores adiciona uma camada extra de segurança à sua conta do Bitdefender, ao solicitar um código de autenticação além das credenciais de início de sessão. Assim, irá impedir o roubo da conta e irá prevenir diversos tipos de ciberataques, como keyloggers, ataques de força bruta e de dicionário.

Ativar autenticação de dois fatores

Ao permitir a autenticação de dois fatores, irá deixar a sua conta Bitdefender muito mais segura. A sua identidade será verificada sempre que iniciar sessão num dispositivo diferente, já seja para instalar um dos produtos Bitdefender, verificar o estado da sua assinatura ou executar tarefas remotamente nos seus dispositivos.

Para ativar a autenticação de dois fatores:

1. Aceda Bitdefender Central.
2. Clique no ícone no canto superior direito do ecrã.
3. Clique em **Conta da Bitdefender** no menu deslizante.
4. Selecione o separador **Palavra-passe e segurança**.
5. Clique em **Autenticação de dois fatores**.
6. Clique em **COMEÇAR**.

Selecione uma das seguintes opções:

- **Aplicação de autenticação** - utilize uma apliação de autenticação para gerar um código sempre que quiser aceder à sua conta Bitdefender.

  Caso queira utilizar a aplicação de autenticação, mas não tem a certeza de qual escolher, aparecerá uma lista com as aplicações de autenticação recomendadas.

  a. Clique em **UTILIZAR APLICAÇÃO DE AUTENTICAÇÃO** para começar.

  b. Para uniciar sessão num dispositivo Android ou iOS, utilize o seu dispositivo para digitalizar o código QR.

     Para iniciar sessão utilizando um portátil ou um ambiente de trabalho, pode adicionar manualmente o código apresentado.

     Clique em **CONTINUAR**.

  c. Insira o código fornecido pela aplicação ou o apresentado no passo anterior e, em seguida, clique em **ATIVAR**.

- **E-mail** - sempre que iniciar sessão na sua conta Bitdefender, o código de verificação será enviado para a sua caixa de e-mail. Verifique a sua conta de e-mail e introduza o código fornecido.

  a. Clique em **UTILIZAR E-MAIL** para começar.

  b. Verifique a sua conta de e-mail e introduza o código fornecido.

     Lembre que tem cinco minutos para verificar a sua conta de e-mail e introduzir o código gerado. Se o tempo expirar, deverá gerar uma nova hiperligação seguindo os mesmos passos.

  c. Clique em **ATIVAR**.

  d. Receberá dez códigos de ativação. Pode copiar, transferir ou imprimir a lista e usá-la caso perca o seu endereço de e-mail, caso contrário não poderá iniciar sessão. Cada código pode ser utilizado apenas uma vez.

  e. Clique em **TERMINADO**.

Caso queira deixar de utilizar a autenticação de dois fatores:

1. Clique em **DESATIVAR A AUTENTICAÇÃO EM DOIS FATORES**.
2. Verifique a sua aplicação ou conta de e-mail e introduza o código que recebeu.

Caso tenha escolhido receber o código de autenticação por e-mail, terá cinco minutos para verificar a sua conta de e-mail e introduzir o código gerado. Se o tempo expirar, deverá gerar uma nova hiperligação seguindo os mesmos passos.

3. Confirme a sua escolha.

6.2.1. Adicionar dispositivos fiáveis

Para garantir que apenas pode aceder à sua conta Bitdefender, poderemos solicitar o código de segurança primeiro. Caso pretenda ignorar este passo sempre que se ligar com o mesmo dispositivo, recomendamos identificá-lo como um dispositivo fiável.

Para adicionar dispositivos como dispositivos fiáveis:

1. Aceda Bitdefender Central.
2. Clique no ícone no canto superior direito do ecrã.
3. Clique em **Conta da Bitdefender** no menu deslizante.
4. Selecione o separador **Palavra-passe e segurança**.
5. Clique em **Dispositivos fiáveis**.
6. Será mostrada a lista com os dispositivos Bitdefender instalados. Clique no dispositivo desejado.

Pode adicionar os dispositivos que pretender, desde que tenham o Bitdefender instalado e a sua subscrição seja válida.

6.3. As minhas subscrições

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

6.3.1. 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).

6.3.2. Adicionar um novo dispositivo

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

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

     Selecione esta opção e, em seguida, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique no botão correspondente.
   - **Proteger outros dispositivos**

     Selecione esta opção e, em seguida, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique no botão correspondente.

     Prima **ENVIAR HIPERLIGAÇÃO DE DOWNLOAD**. Escreva um endereço de email no campo correspondente e clique em **ENVIAR EMAIL**. Observe que a hiperligação de download gerada será válida apenas durante as próximas 24 horas. Se a hiperligação expirar, precisará de gerar uma nova seguindo os mesmos passos.

     No dispositivo em que deseja instalar o seu produto Bitdefender, verifique a conta de e-mail que escreveu e clique no botão de download correspondente.
4. Aguarde pela conclusão da transferência, em seguida, execute o instalador:

6.3.3. Renovar subscrição

Caso tenha desativado a renovação automática da 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.

6.3.4. 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** para instalar o produto num de seus dispositivos.

6.4. 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**.

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 seu dispositivo Windows:

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 Secção 13.2.3, "*Executar uma Análise do Sistema*" e "*Executar uma Análise Rápida*" (p. 79).
- **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. 100).

6.5. Actividade

Na área de Atividades, tem acesso à informação sobre os dispositivos que têm o Bitdefender instalado.

Ao aceder a janela **Atividade**, os seguintes cartões são disponibilizados:

- **Meus dispositivos**. Aqui pode visualizar o número de dispositivos ligados e o seu estado de proteção. Para resolver problemas remotamente nos dispositivos detectados, clique em **Resolver problemas** e, em seguida, clique em **ANALISAR E RESOLVER PROBLEMAS**.

  Para visualizar detalhes sobre os problemas detectados, clique em **Visualizar problemas**.

  Informações sobre ameaças detectadas não podem ser recuperadas de dispositivos iOS.

- **Ameaças bloqueadas**. Aqui pode visualizar um gráfico que mostra uma estatística geral que inclui informação sobre as ameaças bloqueadas nas últimas 24 horas e nos últimos sete dias. A informação exibida vai depender do comportamento malicioso detectado e os ficheiros, aplicações e URLs acedidos.
- **Utilizadores principais com ameaças bloqueadas**. Aqui pode visualizar uma lista que mostra onde o maior número ameaças para os utilizadores foram identificadas.
- **Dispositivos principais com ameaças bloqueadas**. Aqui pode visualizar uma lista mostrando onde foram encontrados os dispositivos com o maior número de ameaças.

6.6. 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.

7. 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 predefinição, ele verifica se há atualizações quando liga o seu dispositivo e todas as **horas** após isso. Se for detetada uma atualização, esta é automaticamente descarregada e instalada no seu dispositivo.

O processo de actualização é executado "on the fly", o que significa que os ficheiros são substituídos progressivamente. Desta forma, o processo de atualização não afetará a operação do produto, e ao mesmo tempo, qualquer vulnerabilidade será eliminada.

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 dispositivo se ligar a Internet através de um servidor proxy, deve configurar as definições do proxy conforme escrito em "*Como posso configurar Bitdefender para usar um proxy de ligação à Internet?*" (p. 66).
- 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. 40).

7.1. Verifique se o Bitdefender está atualizado

Para verificar quando foi a última atualização do seu Bitdefender:

1. Clique em **Definições** no menu de navegação na 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.

7.2. A efetuar uma atualização

Para realizar actualizações, é necessária uma ligação à Internet.

Para iniciar uma atualização, clique com o botão direito no ícone do Bitdefender na bandeja do sistema e, em seguida, 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 dispositivo quando a atualização 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 seu dispositivo Windows:

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**.

7.3. Ligar ou desligar a atualização automática

Para desativar a atualização automática:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. Selecione o separador **Atualizar**.
3. Ative ou desative o botão 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 as atualizações automáticas por 5, 15 ou 30 minutos, por uma hora ou até à próxima reinicialização 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.

7.4. 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 em **Definições** no menu de navegação na interface do Bitdefender.
2. Selecione o separador **Atualizar** e ajuste as definições de acordo com 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.

Regras de atualização

Sempre que uma atualização estiver disponível, o Bitdefender irá transferir e implementar automaticamente a atualização sem exibir notificações. Desligue a opção **Atualização silenciosa** se quiser ser notificado sempre que uma nova atualização estiver disponível.

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 dispositivo. Isto serve para evitar que o processo de actualização de Bitdefender interfira com o trabalho do utilizador.

Se quiser ser notificado quando uma atualização precisar de reiniciar, ative a **Notificação de reinicialização**.

7.5. 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 2020 instalado.

COMO

8. INSTALAÇÃO

8.1. Como instalar o Bitdefender num segundo dispositivo?

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

Para instalar o Bitdefender num segundo dispositivo:

1. Clique na hiperligação **Instalar noutro dispositivo** no canto inferior esquerdo da interface do Bitdefender.

   Aparece uma nova janela no seu ecrã.

2. Clique em **PARTILHAR HIPERLIGAÇÃO DE TRANSFERÊNCIA**.
3. Siga as instruções no ecrã para instalar o Bitdefender.

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

8.2. 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 Antivirus Plus** e selecione **Desinstalar**.
  3. Clique em **REINSTALAR** na janela que aparece.
  4. Precisa de reiniciar o dispositivo 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 Antivirus Plus** e selecione **Desinstalar**.
4. Clique em **REINSTALAR** na janela que aparece.
5. Precisa de reiniciar o dispositivo 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 Antivirus Plus** e selecione **Desinstalar**.
  4. Clique em **Desinstalar** novamente para confirmar a sua escolha.
  5. Clique em **REINSTALAR**.
  6. Precisa de reiniciar o dispositivo 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.

8.3. Onde posso transferir o meu produto Bitdefender?

Pode instalar o Bitdefender do disco de instalação ou através do instalador transferido no seu dispositivo 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 dispositivo, 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**.
3. Escolha uma das duas opções disponíveis:
   - **Proteger este dispositivo**

Selecione esta opção e, em seguida, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique no botão correspondente.

- **Proteger outros dispositivos**

  Selecione esta opção e, em seguida, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique no botão correspondente.

  Prima **ENVIAR HIPERLIGAÇÃO DE DOWNLOAD**. Escreva um endereço de email no campo correspondente e clique em **ENVIAR EMAIL**. Observe que a hiperligação de download gerada será válida apenas durante as próximas 24 horas. Se a hiperligação expirar, precisará de gerar uma nova seguindo os mesmos passos.

  No dispositivo em que deseja instalar o seu produto Bitdefender, verifique a conta de e-mail que escreveu e clique no botão de download correspondente.

4. Execute o Bitdefender que transferiu.

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

A interface do Bitdefender está disponível em várias línguas e pode ser alterada ao seguir os passos seguintes:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. Na janela **Geral**, clique em **Alterar língua**.
3. Selecione a língua desejada na lista e, em seguida, clique em **GUARDAR**.
4. Aguarde alguns momentos até que sejam aplicadas as definições.

8.5. 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 Antivirus Plus** 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 Antivirus Plus** 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 de Configurações e, em seguida, selecione **Aplicações**.
3. Encontre o **Bitdefender Antivirus Plus** 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**.
     c. Escolha uma das duas opções disponíveis:
        - **Proteger este dispositivo**

          Selecione esta opção e, em seguida, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique no botão correspondente.
        - **Proteger outros dispositivos**

          Selecione esta opção e, em seguida, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique no botão correspondente.

Prima **ENVIAR HIPERLIGAÇÃO DE DOWNLOAD**. Escreva um endereço de email no campo correspondente e clique em **ENVIAR EMAIL**. Observe que a hiperligação de download gerada será válida apenas durante as próximas 24 horas. Se a hiperligação expirar, precisará de gerar uma nova seguindo os mesmos passos.

No dispositivo em que deseja instalar o seu produto Bitdefender, verifique a conta de e-mail que escreveu e clique no botão de download correspondente.

2. Execute o Bitdefender que transferiu.

Para obter mais informações sobre o processo de instalação do Bitdefender, consulte "*Instalação do seu produto Bitdefender*" (p. 5).

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

A partir de agora, 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 2020, 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**. Espere que o dispositivo seja reiniciado.

   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.

9. BITDEFENDER CENTRAL

9.1. Como faço para iniciar sessão na conta da Bitdefender com outra conta?

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

Para iniciar sessão com outra conta da Bitdefender:

1. Clique no nome da sua conta no canto superior da Interface do Bitdefender.
2. Clique em **Alterar Conta** no canto superior direito do ecrã para trocar a conta vinculada ao dispositivo.
3. Introduza o endereço de e-mail no campo correspondente e clique em **PRÓXIMO**.
4. Introduza a sua palavra-passe e depois 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 contactar a Bitdefender para obter suporte, como descrito na secção "*Pedir Ajuda*" (p. 164).

9.2. 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. Clique em **Definições** no menu deslizante.
5. Desative a opção **Ativar/desativar mensagens de ajuda**.

9.3. 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 em **Minha Conta** no menu de navegação da interface do Bitdefender.
  2. Clique no botão **Alterar Conta** no canto superior direito do ecrã.

     Aparece uma nova janela.
  3. Introduza o seu endereço de e-mail e clique em **PRÓXIMO**.

     Aparece uma nova janela.
  4. Clique em **Esqueceu a palavra-passe?**.
  5. Clique em **SEGUINTE**.
  6. Verifique a sua conta de e-mail, introduza o código de segurança que recebeu e depois clique em **PRÓXIMO**.

     Ou pode clicar em **Alterar palavra-passe** no e-mail que recebeu.
  7. Introduza a nova palavra-passe que pretende definir e, em seguida, introduza-a novamente. Clique em **GUARDAR**.
- Do seu navegador Web:
  1. Vá para: https://central.bitdefender.com.
  2. Clique em **INICIAR SESSÃO**.
  3. Introduza o seu endereço de e-mail e depois clique em **PRÓXIMO**.
  4. Clique em **Esqueceu a palavra-passe?**.
  5. Clique em **SEGUINTE**.
  6. 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.

9.4. 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 **Sessões** no menu deslizante.
4. Na área **Sessões ativas**, selecione a opção **TERMINAR SESSÃO** junto ao dispositivo que pretende terminar a sessão.

10. A ANALISAR COM BITDEFENDER

10.1. 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.
- Verifique uma partilha de rede antes de copiar os ficheiros para o seu dispositivo.

10.2. Como posso analisar o seu sistema?

Para realizar uma análise completa no sistema:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Clique no botão **Executar Análise** ao lado de **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. 83).

10.3. 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 dispositivo.

Para agendar uma análise:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Clique em ••• ao lado do tipo de verificação que deseja programar, Análise de Sistema ou Análise Rápida na parte inferior da interface e, em seguida, selecione **Editar**.

   Como alternativa, pode criar um tipo de verificação que corresponda às suas necessidades clicando em **+Criar análise** ao lado de **Gerir análises**.
4. Personalize a análise de acordo com as suas necessidades e, em seguida, clique em **Seguinte**.
5. Marque a caixa ao lado de **Escolha quando agendar esta tarefa**.

   Selecione uma das opções correspondentes para definir uma agenda:

   - No iniciar do sistema
   - Diária
   - Semanal
   - Mensal

   Para escolher Diariamente, Mensalmente ou Semanalmente, arraste o marcador pela barra de frequência para definir o intervalo em que a análise programada deve começar.

Se escolher criar uma nova análise personalizada, a janela **Tarefa de análise** aparecerá. Aqui, pode selecionar os locais que deseja analisar.

10.4. Como posso criar uma tarefa de análise personalizada?

Se quer analisar localizações específicas no seu dispositivo 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. No painel **ANTIVÍRUS**, clique em **Abrir**.
2. Clique em **+Criar análise** ao lado de **Gerir análises**.

3. No campo de nome da tarefa, introduza o nome da verificação e selecione os locais que deseja analisar e, em seguida, clique em **SEGUINTE**.
4. Configure as seguintes opções gerais:
   - **Analisar apenas aplicações**. Você pode configurar o Bitdefender para só analisar as aplicações acedidas.
   - **Verificar prioridade de tarefa**. Pode escolher o impacto que o processo de análise deve ter no desempenho do seu sistema.
     - Automática - A prioridade do processo de análise dependerá da atividade do sistema. Para que o processo de análise não afete a atividade do sistema, o Bitdefender decide se o processo de análise deve ser executado com prioridade alta ou baixa.
     - Alta - A prioridade do processo de análise será alta. Ao escolher esta opção, permite que outros programas sejam executados mais devagar, diminuindo o tempo necessário para o processo de análise ser concluído.
     - Baixa - A prioridade do processo de análise será baixa. Ao escolher essa opção, permite que outros programas sejam executados mais rápido, aumentando o tempo necessário para o processo de análise ser concluído.
   - **Ações pós-verificação**. Escolha a ação que o Bitdefender deve realizar se não forem encontradas ameaças:
     - Mostrar janela de resumo
     - Desligar dispositivo
     - Fechar janela da Análise
5. Se deseja configurar as opções de análise detalhadamente, clique em **Mostrar opções avançadas**.

   Clique **Seguinte**.
6. Pode ativar a opção **Programar tarefa de análise** e, se quiser, escolha quando a análise personalizada que criou deve começar.
   - No iniciar do sistema
   - Diária
   - Mensal

- Semanal

  Para escolher Diariamente, Mensalmente ou Semanalmente, arraste o marcador pela barra de frequência para definir o intervalo em que a análise programada deve começar.

7. Clique em **Guardar** para guardar as definições e fechar a janela de configuração.

   Dependendo das localizações a serem analisadas, a análise pode demorar um pouco. Se forem encontradas ameaças durante o processo de análise, deve escolher as ações a serem tomadas para os ficheiros detectados.

Se quiser, pode voltar a executar rapidamente uma análise personalizada anterior ao clicar na entrada correspondente na lista disponível.

10.5. Como 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 Exceções:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Clique na barra **Definições** .
4. Clique em **Gerir Exceções**.
5. Clique em **+Adicionar uma Exceção**.
6. Introduza no campo correspondente o caminho da pasta que pretende adicionar à lista de exceção da análise.

   Como alternativa, pode navegar até a pasta ao clicar no botão navegar no lado direito da interface, selecioná-la e clicar em **OK**.

7. Ligue o interruptor junto à funcionalidade de proteção que não deve analisar a pasta. Há três opções:
   - Antivírus
   - Prevenção de Ameaças Online
   - Advanced Threat Defense
8. Clique em **Guardar** para guardar as alterações e fechar a janela.

10.6. 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 em **Definições** no menu de navegação na interface do Bitdefender.
   b. No painel **ANTIVÍRUS**, clique em **Abrir**.
   c. Na janela **Avançada**, desative o **Escudo do Bitdefender**.

      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. 68).
3. Restaurar o ficheiro da área de Quarentena:
   a. Clique em **Definições** no menu de navegação na interface do Bitdefender.
   b. No painel **ANTIVÍRUS**, clique em **Abrir**.
   c. Vá para a janela **Definições** e clique em **Gerir a quarentena**.
   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 excluir uma pasta da análise?*" (p. 57).

Por predefinição, a Bitdefender adiciona automaticamente ficheiros restaurados à lista de exceções.

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. 164).

10.7. 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 em **Definições** no menu de navegação na 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**.

11. PRIVACY PROTECTION

11.1. 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 em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel do **SAFEPAY**, clique em **Definições**.
3. Nas janelas do **Safepay**, clique em **Iniciar Safepay**.
4. Clique no ícone para aceder ao **Teclado Virtual**.

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

11.2. 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 dispositivo utilizando o menu contextual Windows ao seguir 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. Clique em **Eliminar permanentemente** e, em seguida, confirme que deseja continuar com o processo.

Aguarde que o Bitdefender termine a destruição dos ficheiros.

3. Os resultados são apresentados. Clique em **TERMINAR** para sair do assistente.

11.3. Como posso restaurar manualmente ficheiros encriptados quando o processo de restauração falhar?

Caso ficheiros encriptados não possam ser automaticamente restaurados, pode restaurá-los manualmente seguindo estes passos:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador**Todas**, selecione a notificação referente ao último comportamento de ransomware detectado e, em seguida, clique em **Ficheiros Encriptados**.
3. Será exibida a lista dos ficheiros encriptados.

   Clique em **Recuperar ficheiros** para continuar.
4. Caso o processo de recuperação falhe inteira ou parcialmente, deve escolher o local em que os ficheiros encriptados devem ser guardados. Clique em **Restaurar localização** e, em seguida, escolha uma localização no seu PC.
5. Aparece uma janela de confirmação.

   Clique em **Finalizar** para terminar o processo de restauração.

Ficheiros com as seguintes extensões podem ser restaurados caso sejam encriptados:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

12. INFORMAÇÕES ÚTEIS

12.1. 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. 164).

12.2. Como posso remover o Bitdefender?

Se pretender remover o seu Bitdefender Antivirus Plus:

- No **Windows 7**:
  1. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
  2. Encontre o **Bitdefender Antivirus Plus** 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 Antivirus Plus** 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 de Configurações e, em seguida, selecione **Aplicações**.
3. Encontre o **Bitdefender Antivirus Plus** 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.

12.3. Como removo o Bitdefender VPN?

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

- 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.

12.4. Como é que removo a extensão Antitracker da Bitdefender?

Dependendo do navegador que esteja a utilizar, siga estes passos para desinstalar a extensão Antitracker da Bitdefender:

- Internet Explorer
  1. Clique em  ao lado da barra de pesquisa e, em seguida, selecione Gerir suplementos.

     Será exibida a lista das extensões instaladas.
  2. Clique em Antitracker da Bitdefender.
  3. Clique em **Desativar** no canto inferior direito.
- Google Chrome
  1. Clique em ao lado da barra de pesquisa.
  2. Selecione **Mais ferramentas** e depois em **Extensões**.

Será exibida a lista das extensões instaladas.

3. Clique em **Remover** no cartão Antitracker da Bitdefender.
4. Clique em **Remover** na janela pop-up que aparece.

- Mozilla Firefox

1. Clique em ☰ ao lado da barra de pesquisa.
2. Selecione **Suplementos** e, em seguida, selecione **Extensões**.

   Será exibida a lista das extensões instaladas.

3. Clique em ••• e, em seguida, selecione **Remover**.

12.5. Como desligo automaticamente o meu dispositivo 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 dispositivo pode demorar muito mais tempo a concluir 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.

Considere este exemplo: terminou o seu trabalho e quer ir dormir. Gostaria que o seu sistema fosse completamente analisado quanto a ameaças pelo Bitdefender.

Para desligar o dispositivo uma vez finalizada a Análise Rápida ou a Análise de Sistema:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela de **Análises**, clique em ••• próximo para Análise Rápida e, em seguida, selecione **Editar**.
4. Personalize a análise de acordo com as suas necessidades e clique em **Seguinte**.
5. Marque a caixa ao lado de **Escolher quando agendar esta tarefa** e, em seguida, escolha quando a tarefa deve começar.

Para escolher Diariamente, Mensalmente ou Semanalmente, arraste o marcador pela barra de frequência para definir o intervalo em que a análise programada deve começar.

6. Clique em **Guardar**.

Para desligar o dispositivo ao finalizar uma análise personalizada:

1. Clique em ••• ao lado da análise personalizada que criou.
2. Clique em **Seguinte** e, em seguida, clique em **Seguinte** novamente.
3. Marque a caixa ao lado de **Escolher quando agendar esta tarefa** e, em seguida, escolha quando a tarefa deve começar.
4. Clique em **Guardar**.

Se não forem encontradas ameaças, o dispositivo desligar-se-á.

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. 83).

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

Se o seu dispositivo se ligar à Internet através de um servidor proxy, 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 em **Definições** no menu de navegação na interface do Bitdefender.
2. Selecione o separador **Avançado**.
3. Ative o **Servidor proxy**.
4. Clique em **Mudança de proxy**.
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.

12.7. 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.

12.8. 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**.

12.9. 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 dispositivo, o sistema torna-se instável. O instalador do Bitdefender Antivirus Plus 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 de Configurações e, em seguida, selecione **Aplicações**.
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.

12.10. 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 dispositivo.
  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.

GERIR A SUA SEGURANÇA

13. PROTEÇÃO ANTIVÍRUS

Bitdefender protege o seu dispositivo 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 dispositivo, 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 media removível que esteja ligado ao dispositivo para garantir um acesso em segurança. Para mais informação, dirija-se a "*Análise automática de média removíveis*" (p. 87).

Os utilizadores avançados poderão configurar excepções se não desejarem que ficheiros ou tipos de ficheiros específicos sejam analisados. Para mais informação, dirija-se a "*A configurar exceções de análise*" (p. 89).

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. 92).

Se o seu dispositivo estiver infetado com ameaças, consulte "*Remover ameaças do seu sistema*" (p. 156). Para o ajudar a limpar as ameaças do dispositivo que não podem ser removidas no sistema operativo Windows, o Bitdefender proporciona-lhe o "*Ambiente de Resgate*" (p. 156). Este é um

ambiente fiável, concebido sobretudo para a remoção de ameaças, que lhe permite arrancar o seu dispositivo independentemente do Windows. Quando o dispositivo é executado no Ambiente de Resgate, as ameaças do Windows estão inativas, tornando-as mais fáceis de remover.

13.1. Análise no acesso (proteção em tempo real)

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

13.1.1. Ligar ou desligar a proteção em tempo real

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

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Avançada**, ative ou desative o **Escudo do Bitdefender**.
4. 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.

13.1.2. 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 em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Avançado**, pode configurar as definições da verificação conforme necessário.

Informação sobre as opções de análise

Poderá achar esta informação útil:

- **Analisar apenas aplicações.** Você pode configurar o Bitdefender para só analisar as aplicações acedidas.
- **Analisar aplicações potencialmente indesejadas.** Selecione esta opção para analisar aplicações indesejadas. Uma aplicação potencialmente indesejada (PUA) ou programa potencialmente indesejado (PUP) é um software que normalmente vem com software freeware e mostrará pop-ups ou instalará uma barra de ferramentas no navegador padrão. Alguns deles mudarão a homepage ou o mecanismo de busca, outros executarão vários processos em segundo plano, deixando seu PC lento ou mostrando vários anúncios. Esses programas podem ser instalados sem o seu consentimento (também chamados de adware) ou serão incluídos por defeito no seu kit de instalação expresso (apoiado por anúncios).
- **Analisar scripts.** A funcionalidade de análise de scripts permite ao Bitdefender analisar scripts da powershell e documentos de escritório que podem conter malware à base de scripts.
- **Analisar partilhas de rede.** Para aceder a uma rede remota com segurança desde o seu dispositivo, recomendamos que mantenha a opção de Analisar partilhas de rede ativa.
- **Analisar 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 escolher esta opção, ative-a e, em seguida, arraste o marcador pela escala para excluir da análise ficheiros mais longos do que um valor dado em MB (Megabites).

- **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.
- **Verificar apenas ficheiros novos e modificados.** Ao verificar apenas ficheiros novos e modificados, pode melhorar significativamente a resposta geral do sistema com um sacrifício mínimo da 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.
- **Verificação de arranque antecipado.** 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 em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Avançado**, role a página para baixo até ver a opção **Ações de ameaças**.
4. 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. 92).

  > **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 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. 92).

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

13.1.3. 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 em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Avançado**, role a página para baixo até ver a opção **Repor as definições avançadas**. Selecione esta opção para repor as predefinições do antivírus.

13.2. Verificação por ordem

O objetivo principal do Bitdefender é manter o seu dispositivo livre de ameaças. Isto é feito ao manter as novas ameaças fora do seu dispositivo 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 dispositivo depois de instalar o Bitdefender. E é definitivamente uma boa ideia analisar frequentemente o seu dispositivo 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 dispositivo 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 dispositivo ou configurar as opções de análise, pode configurar e executar uma análise personalizada.

13.2.1. 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.

13.2.2. 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 em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Análises**, clique no botão **Executar análise** ao lado de **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.

13.2.3. Executar uma Análise do Sistema

A tarefa de Análise do Sistema procura em todo o dispositivo 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 utilizar o seu dispositivo.

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. Verificar o seu dispositivo utilizando bases de dados de informação de ameaças desatualizadas pode impedir que o Bitdefender detecte novas ameaças criadas desde a última

atualização. Para mais informação, dirija-se a "*Mantenha o seu Bitdefender atualizado.*" (p. 39).

- Encerre todos os programas abertos.

Se quer analisar localizações específicas no seu dispositivo ou configurar as opções de análise, pode configurar e executar uma análise personalizada. Para mais informação, dirija-se a "*Configurar uma análise personalizada*" (p. 80).

Para realizar uma análise do sistema:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Análises**, clique no botão **Executar Análise** ao lado de **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.

13.2.4. Configurar uma análise personalizada

Sempre que achar que o seu dispositivo precisar de ser analisado quanto a ameaças potenciais, pode configurar a Bitdefender para realizar análises utilizando a janela **Gerir análises**. Pode programar uma Análise de Sistema, uma Análise Rápida, ou pode criar uma análise personalizada segundo as suas necessidades.

Para configurar uma nova análise personalizada detalhadamente:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Nas janelas **Análises**, clique em **+Criar análise**.
4. No campo **Nome da tarefa**, introduza o nome da análise e, em seguida, selecione os locais que deseja analisar e, em seguida, clique em **Seguinte**.
5. Configure as seguintes opções gerais:

- **Analisar apenas aplicações**. Você pode configurar o Bitdefender para só analisar as aplicações acedidas.
- **Verificar prioridade de tarefa**. Pode escolher o impacto que o processo de análise deve ter no desempenho do seu sistema.
  - Automática - A prioridade do processo de análise dependerá da atividade do sistema. Para que o processo de análise não afete a atividade do sistema, o Bitdefender decide se o processo de análise deve ser executado com prioridade alta ou baixa.
  - Alta - A prioridade do processo de análise será alta. Ao escolher esta opção, permite que outros programas sejam executados mais devagar, diminuindo o tempo necessário para o processo de análise ser concluído.
  - Baixa - A prioridade do processo de análise será baixa. Ao escolher essa opção, permite que outros programas sejam executados mais rápido, aumentando o tempo necessário para o processo de análise ser concluído.
- **Ações pós-verificação**. Escolha a ação que o Bitdefender deve realizar se não forem encontradas ameaças:
  - Mostrar janela de resumo
  - Desligar dispositivo
  - Fechar janela da Análise

6. Se deseja configurar as opções de análise detalhadamente, clique em **Mostrar opções avançadas**. Poderá encontrará informações sobre as análises listadas no final desta seção.

   Clique **Seguinte**.

7. Pode ativar a opção **Programar tarefa de análise** se quiser e, em seguida, escolha quando a análise personalizada que criou deve começar.
   - No iniciar do sistema
   - Diária
   - Mensal
   - Semanal

Para escolher Diariamente, Mensalmente ou Semanalmente, arraste o marcador pela barra de frequência para definir o intervalo em que a análise programada deve começar.

8. Clique em **Guardar** para guardar as definições e fechar a janela de configuração.

   Dependendo das localizações a serem analisadas, a análise pode demorar um pouco. Se forem encontradas ameaças durante o processo de análise, deve escolher as ações a serem tomadas para os ficheiros detectados.

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.
- **Analisar aplicações potencialmente indesejadas.** Selecione esta opção para analisar aplicações indesejadas. Uma aplicação potencialmente indesejada (PUA) ou programa potencialmente indesejado (PUP) é um software que normalmente vem com software freeware e mostrará pop-ups ou instalará uma barra de ferramentas no navegador padrão. Alguns deles mudarão a homepage ou o mecanismo de busca, outros executarão vários processos em segundo plano, deixando seu PC lento ou mostrando vários anúncios. Esses programas podem ser instalados sem o seu consentimento (também chamados de adware) ou serão incluídos por defeito no seu kit de instalação expresso (apoiado por anúncios).
- **Analisar arquivos.** 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.

  Arraste o marcador pela escala para excluir da análise ficheiros mais longos do que um dado valor em MB (Megabites).

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

- **Verificar apenas ficheiros novos e modificados.** Ao verificar apenas ficheiros novos e modificados, pode melhorar significativamente a resposta geral do sistema com um sacrifício mínimo da segurança.
- **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 dispositivo.
- **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.

13.2.5. 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 pedir uma palavra-passe e excluir este item da análise.** Selecione esta opção para saltar a análise deste arquivo.
- **Passar todos os itens protegidos por palavra-passe 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. 92).

  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.

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. 156).

13.2.6. 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 em **Definições** no menu de navegação na 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 relatório da análise, clique em **Ver Relatório**.

13.3. Análise automática de média removíveis

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

Os dispositivos detetados encaixam-se numa destas categorias:

- CDs/DVDs
- Dispositivos de armazenamento externos como pen USB 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.

13.3.1. Como funciona?

Ao detectar um dispositivo de armazenamento removível, o Bitdefender começa a analisá-lo à procura de ameaças (desde que a análise automática esteja ativa para esse tipo de dispositivo). Será notificado através de uma janela de pop-up que um novo dispositivo foi detetado e está a ser analisado.

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.

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.

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.

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. 156).

13.3.2. Gerir análise de média removível

Para gerir a verificação automática de dispositivos multimédia amovíveis:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Selecione a janela **Definições**.

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.

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

13.4. 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 em **Definições** no menu de navegação na interface do Bitdefender.
2. Selecione o separador **Avançado**.
3. Ligue ou desligue a **Análise do ficheiro do host**.

13.5. A configurar exceções de 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 utilizadas por utilizadores com conhecimentos

avançados de informática ou sob as recomendações de um representante da Bitdefender.

Pode configurar excepções para que sejam realizadas análises somente após acesso ou por demanda ou até mesmo ambas. Os objetos excetuados da análise após acesso não serão analisados, mesmo se forem acedidos por si ou por uma aplicação.

Nota

As exceções NÃO serão aplicadas à análise contextual. Análise Contextual é um tipo de análise a-pedido: você clica com o botão direito de rato sobre o ficheiro ou pasta que quer analisar e seleciona **Analisar com Bitdefender**.

13.5.1. Excluindo ficheiros e pastas da análise

Para excluir ficheiros e pastas específicas da análise:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Definições**, clique em **Gerir exceções**.
4. Clique em **+Adicionar uma Exceção**.
5. Introduza no campo correspondente o caminho da pasta que pretende adicionar à lista de exceção da análise.

   Como alternativa, pode navegar até a pasta ao clicar no botão navegar no lado direito da interface, selecioná-la e clicar em **OK**.
6. Ligue o interruptor junto à funcionalidade de proteção que não deve analisar a pasta. Há três opções:
   - Antivírus
   - Prevenção de Ameaças Online
   - Advanced Threat Defense
7. Clique em **Guardar** para guardar as alterações e fechar a janela.

13.5.2. 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 dispositivo. A exceção também se aplica a ficheiros em

meios removíveis, tais como CDs, DVDs, dispositivos de armazenamento USB ou unidades de rede.

Importante
Tenha cuidado ao excluir as extensões da análise, porque essas exceções podem deixar o seu dispositivo vulnerável a ameaças.

Para excluir extensões de ficheiros da análise:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Definições**, clique em **Gerir exceções**.
4. Clique em **+Adicionar uma Exceção**.
5. Escreva as extensões que deseja excluir da análise com um ponto antes e separando-as por ponto e vírgula (;).

   txt;avi;jpg
6. Ligue o interruptor junto à funcionalidade de proteção que não deve analisar a extensão.
7. Clique em **Guardar**.

13.5.3. Ativar exceções de análise

Se as exceções de análise configuradas já não forem necessárias, é recomendado que elimine ou desactive as exceções de análise.

Para gerir exceções da análise:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Definições**, clique em **Gerir exceções**. Uma lista com todas as suas exceções será exibida.
4. Para remover ou editar exceções da análise, clique num dos botões disponíveis. Proceder da seguinte forma:

   - Para remover uma entrada da lista, clique no botão ao lado dela.
   - Para editar uma entrada da tabela, clique no botão **Editar** ao lado dela. Uma nova janela aparece onde pode alterar a extensão ou o caminho a ser excluído e a funcionalidade de segurança do qual deseja que eles

sejam excluídos, conforme necessário. Faça as alterações necessárias e, em seguida, clique em **MODIFICAR**.

13.6. 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 em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Vá para a janela **Definições**.

   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:

   Verifique novamente a quarentena depois de atualizações às informações sobre ameaças

   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.

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

Criar exceções para ficheiros restaurados
Os ficheiros que você restaurar da quarentena serão colocados de volta na sua localização original sem que sejam reparados e excluídos 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**.

14. 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 dispositivo, procurando ações tipo ameaças. Cada uma destas acções é classificada e é calculada uma pontuação geral para cada processo.

Como medida de segurança, será notificado sempre que seja detectada e bloqueada uma ameaça ou um processo potencialmente malicioso.

14.1. Ativar ou desativar o Advanced Threat Defense

Para ativar ou desativar o Advanced Threat Defense:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ADVANCED THREAT DEFENSE**, clique em **Abrir**.
3. Vá para a janela **Definições** e clique no botão ao lado de **Defesa contra Ameaças Avançadas da Bitdefender**.

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

14.2. A verificar ataques maliciosos detectados

Cada vez que seja detectada uma ameaça ou um processo potencialmente malicioso, o Bitdefender irá bloqueá-lo para previr que o seu dispositivo seja infectado por ransomware ou outro malware. Pode comprovar a lista de ataques maliciosos detectados seguindo os seguintes passos:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ADVANCED THREAT DEFENSE**, clique em **Abrir**.
3. Vá para a janela **Defesa contra Ameaças**.

   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.

14.3. A adicionar processos a exceções

Você pode configurar as regras de exceção para aplicações fidedignas para que a Defesa Avançada Contra Ameaças as bloqueie caso executem ações típicas de ameaças.

Para começar a adicionar processos à lista de exceções da Defesa Avançada Contra Ameaças:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ADVANCED THREAT DEFENSE**, clique em **Abrir**.
3. Na janela **Definições**, clique em **Gerir exceções**.
4. Clique em **+Adicionar uma Exceção**.
5. Introduza no campo correspondente o caminho da pasta que pretende adicionar à lista de exceção da análise.

   Como alternativa, pode navegar para o executável ao clicar no botão navegar no lado direito da interface, selecioná-lo e clicar em **OK**.
6. Ligue o interruptor ao lado de **Defesa contra Ameaças Avançadas**.
7. Clique em **Guardar**.

14.4. Deteção de exploits

Uma forma utilizada pelos hackers para invadir sistemas é aproveitarem-se de certos bugs ou vulnerabilidades no software (aplicações e plug-ins) e hardware dos computadores. O Bitdefender utiliza a mais moderna tecnologia antiexploit para evitar que o seu dispositivo seja vítima de um desses ataques, que se costumam espalhar muito rapidamente.

Ativar ou desativar a deteção de exploits

Para ativar ou desativar a deteção de exploits:

- Clique em **Definições** no menu de navegação na interface do Bitdefender.
- No painel **ADVANCED THREAT DEFENSE**, clique em **Abrir**.
- Vá para a janela **Definições** e clique no interruptor ao lado de **Explorar deteção** para ligar ou desligar a funcionalidade.

Nota
A opção de Deteção de exploits está ativa por predefinição.

15. PREVENÇÃO DE AMEAÇAS ONLINE

A Prevenção contra ameaças online do Bitdefender garante uma navegação segura ao alertá-lo sobre páginas Web potencialmente maliciosas.

O Bitdefender fornece a prevenção de ameaças online em tempo real para:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

Para configurar a Prevenção contra ameaças online:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **PREVENÇÃO CONTRA AMEAÇAS ONLINE**, clique em **Definições**.

Na janela **Proteção na web** clique nos interruptores para ativar ou desativar:

- A prevenção contra ataques da web bloqueia ameaças provenientes da internet, incluindo downloads não autorizados.
- 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

- Encrypted web scan.

  Ataques mais sofisticados podem usar tráfego da web seguro para enganar as suas vítimas. Logo, recomendamos que mantenha ativa a opção Análise da web encriptada.

- Proteção antifraude.
- Proteção Phishing.

Role para baixo e chegará à seção **Prevenção de ameaças em rede**. Aqui tem a opção **Prevenção de ameaças em rede**. Para manter o seu dispositivo longe de ataques feitos por malware complexos (como ransomware) através da exploração de vulnerabilidades, mantenha a opção ativada.

Pode criar uma lista de sites, domínios e endereços de IP que não serão analisados pelos mecanismos antiameaça, antiphishing e antifraude da Bitdefender. A lista deve conter apenas sites, domínios e endereços de IP nos quais confia plenamente.

Para configurar e gerir sites, domínios e endereços de IP utilizando a Prevenção Contra Ameaças Online fornecida pelo Bitdefender:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **PREVENÇÃO CONTRA AMEAÇAS ONLINE**, clique em **Definições**.
3. Clique em **Gerir exceções**.
4. Clique em **+Adicionar uma Exceção**.
5. No campo correspondente, escreva o nome do site, do domínio ou do endereço IP que deseja adicionar às excepções.
6. Clique no botão ao lado de **Prevenção de Ameaças Online**.
7. Para remover uma entrada da lista, clique no botão ao lado dela.

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

15.1. 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:

- Voltar ao site ao clicar em **VOLTAR À SEGURANÇA**.
- Seguir para o site Web, apesar do alerta, clicando em **Compreendo os riscos, continuar mesmo assim**.
- Se tem certeza de que o site detectado é seguro, clique em **ENVIAR** para adicioná-lo às exceções. Recomendamos apenas sites nos quais confia plenamente.

16. VULNERABILIDADE

Um passo importante na proteção do seu dispositivo contra as ações e aplicações maliciosas é manter atualizado o seu sistema operativo e as aplicações que utiliza regularmente. Além disso, para evitar o acesso físico não autorizado ao seu dispositivo, palavras-passe fortes (palavras-passe que não são facilmente descobertas) devem ser configuradas para cada conta de utilizador do Windows e também para as redes Wi-Fi às quais se liga.

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.

16.1. Procurar vulnerabilidades no seu sistema

Para detectar vulnerabilidades, o Bitdefender requer uma ligação ativa à internet.

Para analisar o seu sistema em busca de vulnerabilidades:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **VULNERABILIDADE**, clique em **Abrir**.
3. No separador **Verificação de vulnerabilidades** clique em **Iniciar análise** e, em seguida, aguarde até que o Bitdefender verifique seu sistema em busca de vulnerabilidades. As vulnerabilidades detetadas são agrupadas nas três categorias:
   - **SISTEMA OPERATIVO**
     - **Segurança de sistemas operativos**

       Definições de sistema alteradas que podem comprometer o seu dispositivo e dados, como não exibir avisos quando ficheiros executados realizam alterações no seu sistema sem a sua permissão

ou quando dispositivos MTP como telefones ou câmaras se conectam e executam operações diferentes sem o seu conhecimento.

- **Atualizações Críticas do Windows**

  Será mostrada uma lista de atualizações importantes para o Windows que não estão instaladas no seu sistema. Talvez seja preciso reiniciar o sistema para a Bitdefender finalizar a instalação. As atualizações podem demorar a serem instaladas.

- **Contas do Windows fracas**

  Pode ver a lista dos utilizadores de contas Windows configurados no seu dispositivo e o nível de proteção que as suas palavras-passe garantem. 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 definir uma nova palavra-passe para o seu sistema, selecione **Definir a palavra-passe agora**.

  Para criar uma palavra-passe segura, recomendamos a utilização de uma combinação de maiúsculas e minúsculas, números e caracteres especiais (como #, $ ou @).

- **APLICAÇÕES**
  - **Segurança do Navegador**

    Altere as definições do seu dispositivo que permitem a execução de ficheiros e programas transferidos pelo Internet Explorer sem uma validação de integridade, o que pode levar ao comprometimento do seu dispositivo.

  - **Atualização de aplicações**

    Para visualizar informação sobre a aplicação que precisa de ser atualizada, clique no nome dela na lista.

    Caso uma aplicação não esteja atualizada, clique na ligação **Transferir nova versão** para transferir a última versão.

- **REDE**
  - **Rede e credenciais**

    A alteração das definições do sistema, como a ligação automática a redes de hotspot abertas sem o seu conhecimento ou a não encriptação do tráfego de saída de canal seguro.

- **Routers e redes Wi-Fi**

  Para obter mais informação sobre a rede Wi-Fi e o router ao qual está ligado, clique no seu nome da lista. Se receber uma recomendação para definir uma palavra-passe mais forte para a sua rede doméstica, siga as nossas instruções para continuar conectado sem se preocupar com a sua privacidade.

  Quando outras recomendações estiverem disponíveis, siga as instruções fornecidas para garantir que a rede da sua casa fica protegida contra hackers.

16.2. 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 em **Definições** no menu de navegação na 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 estiverem disponíveis atualizações 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 a desativar.
- 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 de WI-FI**.

Para configurar as definições de monitorização de vulnerabilidades:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **VULNERABILIDADE**, clique em **Abrir**.

> **Importante**
> Para ser notificado automaticamente sobre vulnerabilidades no sistema ou nas aplicações, mantenha a opção **Vulnerabilidade** ativada.

3. Vá para o separador **Definições**.
4. Escolha as vulnerabilidades do sistema que deseja que sejam regularmente verificadas usando os botões correspondentes.

   Windows updates
   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 do utilizador
   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 @).

Autorreprodução

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.

Consultor Segurança 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.

16.3. Consultor 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 de trabalho
- Redes Wi-Fi públicas

16.3.1. 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 em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **VULNERABILIDADE**, clique em **Abrir**.
3. Vá para a janela **Definições** e ative ou desative a opção **Consultor de Segurança do Wi-Fi**.

16.3.2. Configurar a rede Wi-Fi doméstica

Para começar a configurar a sua rede doméstica:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **VULNERABILIDADE**, clique em **Abrir**.
3. Vá para a janela **Consultor de Segurança do Wi-Fi** e clique em **Wi-Fi doméstico**.
4. No separador **Rede Wi-Fi doméstica**, clique em **SELECIONAR REDE WI-FI DOMÉSTICA**.

   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**.

Para adicionar uma nova rede Wi-Fi como doméstica, clique em **Selecionar nova rede WI-FI doméstica**.

16.3.3. Configurar a rede Wi-Fi do trabalho

Para começar a configurar sua rede de escritório:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **VULNERABILIDADE**, clique em **Abrir**.
3. Vá para a janela **Consultor de Segurança do Wi-Fi**, clique em **Wi-Fi do escritório**.
4. No separador **Wi-Fi do escritório**, clique em **SELECIONAR WI-FI DO ESCRITÓRIO**.

   Uma lista com redes sem fios às quais já esteve ligado é agora exibida.
5. Aponte para a sua rede de escritório e, em seguida, clique em **SELECIONAR**.

Se uma rede de escritório for considerada desprotegida ou não segura, serão exibidas recomendações para reforçar a sua segurança.

Para remover a rede sem fios que definiu como rede de escritório, clique no botão **REMOVER**.

Para remover a rede sem fios que definiu como rede de escritório, clique no botão **Selecionar nova rede WI-FI do escritório**.

16.3.4. 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 Antivirus Plus é definido automaticamente de modo a obter as seguintes definições de programa:

- Advanced Threat Defense ativado
- As seguintes definições da Prevenção contra ameaças online são ativadas:
  - Verificação de web criptografada
  - 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.

16.3.5. Verificar informações sobre redes Wi-Fi

Para verificar as informações sobre as redes sem fios a que é habitual ligar-se:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **VULNERABILIDADE**, clique em **Abrir**.
3. Vá para a janela **Consultor de Segurança do Wi-Fi**.
4. Dependendo das informações que precisar, selecione um dos três separadores, **Wi-Fi doméstica**, **Wi-Fi de escritório** ou **Wi-Fi pública**.
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.

17. REMEDIAÇÃO DE RANSOMWARE

A Remediação de Ransomware da Bitdefender faz uma cópia de segurança dos seus ficheiros, como documentos, fotos, vídeos ou música, para garantir que eles estejam protegidos contra danos ou perda em caso de encriptação por ransomware. Cada vez que um ataque de ransomware for detectado, o Bitdefender bloqueará todos os processos envolvidos no ataque e iniciará o processo de remediação. Assim, poderá recuperar o conteúdo total de seus ficheiros sem pagar qualquer resgate exigido.

17.1. Ativar ou desativar a Remediação de Ransomware

Para ativar ou desativar a Remediação de Ransomware:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **REMEDIAÇÃO DE RANSOMWARE**, ative ou desative o botão.

> **Nota**
> Para garantir que os seus ficheiros estejam protegidos contra ransomware, recomendamos que mantenha a Remediação de Ransomware ativada.

17.2. A ativar ou desativar a restauração automática

A Restauração Automática assegura que seus ficheiros sejam restaurados automaticamente em caso de encriptação por ransomware.

Para ativar ou desativar a restauração automática:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **REMEDIAÇÃO DE RANSOMWARE**, clique em **Gerenciar**.
3. Na janela Definições, ative ou desative o interruptor **Restauração automática**.

17.3. Ver ficheiros restaurados automaticamente

Quando o botão de **Restauração automática** esteja habilitado, o Bitdefender irá automaticamente restabelecer os ficheiros criptografados por ransomware. Assim, pode ter uma experiência na web sem preocupações, sabendo que os seus ficheiros estão seguros.

Para ver ficheiros restaurados automaticamente:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. Na tabela **Todas**, selecione a notificação referente ao último comportamento de ransomware remediado e, em seguida, clique em **Ficheiros Restaurados**.

   Será exibida a lista dos ficheiros restaurados. Neste local também pode ver o local onde seus ficheiros foram restaurados.

17.4. Restauração manual de ficheiros encriptados

Caso tenha que restaurar manualmente ficheiros criptografados por ransomware, siga estes passos:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador**Todas**, selecione a notificação referente ao último comportamento de ransomware detectado e, em seguida, clique em **Ficheiros Encriptados**.
3. Será exibida a lista dos ficheiros encriptados.

   Clique em **Recuperar Ficheiros** para continuar.
4. Caso o processo de recuperação falhe inteira ou parcialmente, deve escolher o local em que os ficheiros encriptados devem ser guardados. Clique em **Restaurar localização** e, em seguida, escolha uma localização no seu PC.
5. Aparece uma janela de confirmação.

   Clique em **Finalizar** para terminar o processo de restauração.

Ficheiros com as seguintes extensões podem ser restaurados caso sejam encriptados:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

17.5. Adicionar aplicações às exceções

Pode configurar regras de excepção para aplicações de confiança para que a função de Remediação de Ameaças não bloqueie caso executem ações típicas de ransomware.

Para adicionar aplicações à lista de excepções de Remediação de Ransomware:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **REMEDIAÇÃO DE RANSOMWARE**, clique em **Gerenciar**.
3. Vá para a janela **Exceções** e clique em **+Adicionar uma Exceção**.

18. PROTEÇÃO DO GESTOR DE PALAVRAS-PASSE PARA AS SUAS CREDENCIAIS

Utilizamos os nossos dispositivos 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

18.1. 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 em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **GESTOR DE PALAVRAS-PASSE**, clique em **Definições**.
3. Na janela **As Minhas Carteiras**, clique em **Adicionar carteira**.
4. Clique em **Criar nova**.
5. Digite as informações solicitadas nos campos correspondentes.
   - Nome 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.
   - 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, ao ativar o interruptor ao lado de **Sincronizar em todos os meus dispositivos**. 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**.

18.2. Importar uma base de dados existente

Para importar a base de dados da carteira armazenada localmente:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **GESTOR DE PALAVRAS-PASSE**, clique em **Definições**.
3. Na janela **As Minhas Carteiras**, clique em **Adicionar carteira**.
4. Clique em **Importar uma base de dados existente**.
5. Vá até ao local no seu dispositivo onde deseja guardar a base de dados da Carteira e selecione-a.

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**.

18.3. Exportar a base de dados da Carteira

Para exportar a sua base de dados do portfólio:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **GESTOR DE PALAVRAS-PASSE**, clique em **Definições**.
3. Vá para a janela **As Minhas Carteiras**.
4. Clique no ícone ••• na carteira pretendida e, em seguida, selecione **Exportar**.
5. Aceda ao local do seu dispositivo onde deseja guardar a base de dados da carteira e escolha um nome para ele.
6. Clique em **Guardar**.

Nota
A Carteira precisa de ser aberta para que a opção **Exportar** esteja disponível. Se a carteira que precisar de exportar estiver bloqueada, clique em **Ativar carteira** e, em seguida, introduza a palavra-passe designada quando for criada.

18.4. Sincronize as suas carteiras na nuvem

Para ativar ou desativar a sincronização das carteiras na nuvem:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **GESTOR DE PALAVRAS-PASSE**, clique em **Definições**.
3. Vá para a janela **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 sincronizar estiver bloqueada, clique em **ATIVAR CARTEIRA** e, em seguida, introduza a palavra-passe designada quando ela for criada.

18.5. Gerir as suas credenciais da Carteira

Para gerir as suas palavras-passe:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **GESTOR DE PALAVRAS-PASSE**, clique em **Definições**.
3. Vá para a janela **As Minhas Carteiras**.
4. Selecione a base de dados da carteira desejada e, em seguida, clique em **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
- páginas web
- Online banking
- E-mails
- Aplicações
- 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 na tabela, selecione-a e clique no botão **Editar** no lado direito.

- Para eliminar uma entrada, selecione-a e clique no botão **Eliminar**.

18.6. Ativar ou desativar a proteção do Gestor de palavras-passe

Para ativar ou desativar a proteção do Gestor de Palavras-passe:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **GESTOR DE PALAVRAS-PASSE**, ative ou desative o botão.

18.7. Gerir as definições do Gestor de Palavras-passe

Para configurar a palavra-passe principal de forma detalhada:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **GESTOR DE PALAVRAS-PASSE**, clique em **Definições**.
3. Vá para a janela **Definições**.

Na seção **Definições de segurança**, as seguintes opções estão disponíveis:

- **Solicitar a minha palavra-passe principal sempre que eu aceder ao meu dispositivo** - 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 dispositivo, um browser ou uma aplicação.
- **Bloquear automaticamente a Carteira quando deixo o meu dispositivo 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 em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **GESTOR DE PALAVRAS-PASSE**, clique em **Definições**.
3. Selecione a janela **Definições**.

   Ligue o interruptor ao lado de uma aplicação para utilizar o Administrador de Palavras-passe e melhore 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 em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **GESTOR DE PALAVRAS-PASSE**, clique em **Definições**.
3. Na janela **Definições**, vá para o separador **Definições de preenchimento automático**.
4. Configure as seguintes opções:

   - **Configure como o Gestor de Palavras-passe 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.
- Páginas da web - abre um submenu com todos os inícios de sessão em sites Web armazenados na Carteira. Clique em **Adicionar Páginas da 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.

19. ANTITRACKER

Uma grande parte dos sites que utiliza monitorizadores para recolher informação sobre o seu comportamento para compartilhar com empresas ou para mostrar publicidade direcionada para si. Devido a isso, os donos dos sites ganham dinheiro por proporcionar conteúdo de graça ou para continuarem a funcionar. Além de recolher informação, os monitorizadores podem desacelerar a sua navegação ou desperdiçar a sua banda larga.

Ao ativar a extensão Antitracker da Bitdefender no seu navegador, evita ser rastreado para que os seus dados permaneçam privados enquanto navega online, e ainda acelera o tempo que os sites precisam para carregarem.

A extensão do Bitdefender é compatível com os seguintes navegadores de internet:

- Internet Explorer
- Google Chrome
- Mozilla Firefox

Os monitorizadores que detectamos estão divididos nas seguintes categorias:

- **Publicidade** - utilizada para analisar o tráfego do site, o comportamento do utilizador ou os padrões de tráfego dos visitantes.
- **Interação com o cliente** - utilizados para medir a interação com o utilizador através de diferentes formas de entrada, como chat ou suporte.
- **Essenciais** - utilizados para monitorizar funcionalidades críticas do site.
- **Analíticas do site** - utilizadas para recolher dados sobre a utilização do site.
- **Redes Sociais** - utilizados para monitorizar o público em redes sociais, as suas atividades e o envolvimento dos utilizadores nas diferentes plataformas de redes sociais.

19.1. Interface do Antitracker

Ao ativar a extensão do Antitracker da Bitdefender, o ícone  aparece ao lado da barra de pesquisa no seu navegador. Cada vez que visitar um site, vai aparecer um contador no ícone referente aos monitorizadores detectados

e bloqueados. Para visualizar mais detalhes sobre os monitorizadores bloqueados, clique no ícone para abrir a interface. Além do número de monitorizadores bloqueados, pode visualizar o tempo que a página precisa para carregar e as categorias às quais os monitorizadores pertencem. Para ver a lista de sites que estão a monitorizar, clique na categoria desejada.

Para impedir que a Bitdefender bloqueie monitorizadores no site que está a visitar, clique em **Pausar proteção neste site**. Esta definição só se aplica enquanto tiver o site aberto, e volta ao estado inicial quando fechar o site.

Para permitir que os monitorizadores de uma categoria específica monitorizem a sua atividade, clique na atividade desejada e, em seguida, no botão correspondente. Se mudar de ideias, clique no mesmo botão novamente.

19.2. Desligar o Antitracker da Bitdefender

Para desligar o Antitracker da Bitdefender:

- Do seu navegador Web:
  1. Abra o seu navegador web.
  2. Clique no ícone ao lado da barra de endereços no seu navegador.
  3. Clique no ícone no canto superior direito.
  4. Utilize o interruptor correspondente para o desativar.

     O ícone da Bitdefender fica cinzento.
- A partir da interface do Bitdefender:
  1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
  2. No painel **ANTITRACKER**, clique em **Definições**.
  3. Desligue o interruptor correspondente do lado do navegador web no qual deseja desativar a extensão.

19.3. Permitir a monitorização de um site

Se desejar ser monitorizado ao visitar um site em particular, pode adicionar o seu endereço às excepções da seguinte forma:

1. Abra o seu navegador web.

2. Clique no ícone ao lado da barra de pesquisa.
3. Clique no ícone no canto superior direito.
4. Se estiver no site que precisa de adicionar às exceções, clique em **Adicionar o site atual à lista**.

   Se desejar adicionar outro site, escreva o seu endereço no campo correspondente e, em seguida, clique em .

20. 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.

20.1. 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 em **Definições** no menu de navegação na interface do Bitdefender.
  2. No painel do **VPN**, clique em **Abrir VPN**.

20.2. 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. 125).

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.

Enquanto estiver conectado, o tempo decorrido e a utilização de banda larga são exibidos na parte inferior da interface.

Para visualizar a área completa do **Menu**, clique 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.

  Clique em **Adicionar aqui** para adicionar um código de ativação para o Bitdefender Premium VPN.

- **Definições** – dependendo das suas necessidades, pode personalizar o comportamento do seu produto. As Definições estão agrupadas em duas categorias:

  - **Geral**
    - Notificações
    - Arranque - escolha se executar o Bitdefender VPN ao iniciar ou não
    - Relatórios do produto - envie relatórios de produtos anónimos para nos ajudar a melhorar a sua experiência
    - Modo escuro
    - Idioma
  - **Avançadas**
    - Internet Kill-Switch - esta funcionalidade suspende temporariamente todo o tráfego da internet se a ligação VPN cair acidentalmente. Assim que estiver online novamente, a ligação VPN é restabelecida.
    - Autoconnect - Ligue o Bitdefender VPN automaticamente quando aceder a uma rede Wi-Fi pública/insegura ou quando uma aplicação de partilha de ficheiros par-a-par for iniciada

- **Suporte** - pode aceder à plataforma do Centro de Suporte onde pode ler um artigo útil sobre como utilizar o VPN Bitdefender ou nos enviar um feedback.
- **Sobre** - são apresentadas informações sobre a versão instalada.

20.3. 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 em qualquer momento, ao clicar no botão **Atualizar** disponível na interface do produto.

A subscrição do Bitdefender Premium VPN é independente da subscrição do Bitdefender Antivirus Plus, 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 Antivirus Plus 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. Ao atualizar para o plano premium, pode utilizar a sua subscrição em todos os produtos, desde que faça login com a mesma conta da Bitdefender.

21. 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. 112).

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 embutida para ser utilizada quando o seu dispositivo 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™.

21.1. 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 dispositivo e pergunta se gostaria de utilizar o Bitdefender Safepay™.

Para aceder à interface principal do Bitdefender Safepay™, utilize um dos métodos a seguir:

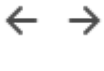
- A partir da interface do Bitdefender:
  1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
  2. No painel do **SAFEPAY**, clique em **Definições**.
  3. Na janela do **Safepay**, clique em **Iniciar Safepay**.
- Do Windows:
  - No **Windows 7**:
    1. Clique em **Iniciar** 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.

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 a informação importante clicando em e selecionando **Imprimir**.

Nota
Para alternar entre o Bitdefender Safepay™ e o ambiente de trabalho do Windows, pressione as teclas **Alt+Tab** ou clique na opção **Mudar para o ambiente de trabalho** no lado superior esquerdo da janela.

21.2. Configurar definições

Clique em e escolha **Definições** para configurar o Bitdefender Safepay™:

Aplicar as regras do Bitdefender Safepay aos domínios acedidos
Os sites que adicionou aos Favoritos com a opção **Abrir automaticamente no Safepay** ativa aparecerão aqui. Se quiser que um site da lista pare

de abrir automaticamente com o Bitdefender Safepay™, clique em × do lado da entrada desejada na coluna **Remover**.

Bloqueio 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.

Manage 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.

Clique em **IMPORTAR** e siga o assistente para utilizar os certificados no Bitdefender Safepay™.

Utilizar teclado virtual
O teclado virtual irá aparecer automaticamente quando o campo de palavra-passe for selecionado.

Utilize o botão correspondente para ativar ou desativar a função.

Confirmação de impressão
Ative esta opção se pretender dar a sua confirmação antes de iniciar o processo de impressão.

21.3. 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 em ••• e escolha **Marcadores** 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. Introduza o URL e o título do favorito, e depois 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.

21.4. Desligar as notificações do Safepay

Quando um site bancário for detectado, o produto Bitdefender é configurado para notificá-lo por meio de uma janela pop-up.

Para desligar as notificações do Safepay:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel do **SAFEPAY**, clique em **Definições**.
3. Na janela **Definições**, desative o botão ao lado de **Notificações do Safepay**.

21.5. Utilizar VPN com o Safepay

Para realizar pagamentos online num ambiente seguro enquanto estiver ligado a redes inseguras, o produto Bitdefender está configurado para executar automaticamente a aplicação do VPN ao mesmo tempo com o Safepay.

Para começar a utilizar o VPN juntamente com o Safepay:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel do **SAFEPAY**, clique em **Definições**.
3. Na janela **Definições**, ligue o interruptor ao lado de **Utilizar VPN com Safepay**.

22. USB IMMUNIZER

A funcionalidade Autorun embutida ao sistema operacional Windows é uma ferramenta bastante útil que permite aos dispositivos 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 dispositivo 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 a um dispositivo em Windows.

Para imunizar um dispositivo USB:

1. Ligue a drive flash ao seu dispositivo.
2. Explore o seu dispositivo 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 prevenir que o seu dispositivo execute ameaças de dispositivos USB não imunizados, desative a funcionalidade de media autorun. Para mais informação, dirija-se a "*Usar monitorização de vulnerabilidade automática*" (p. 102).

UTILITÁRIOS

23. 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 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 Antivirus Plus é definido automaticamente de modo a obter as seguintes definições de programa:

- Advanced Threat Defense ativado
- As seguintes definições da Prevenção contra ameaças online são ativadas:
  - Verificação de web criptografada
  - Proteção contra fraudes
  - Proteção contra phishing

23.1. 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 em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Perfis**, clique em **Definições**.
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 de trabalho**.

Para adicionar aplicações manualmente à Lista de aplicações de trabalho do Perfil de Trabalho:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Perfis**, clique em **Definições**.
3. Clique no botão **CONFIGURAR** na área do Perfil de Trabalho.
4. Na janela **Definições do perfil de trabalho**, clique em **Lista de aplicações**.
5. Clique em **ADICIONAR**.

   Aparece uma nova janela. Vá até ao ficheiro executável da aplicação, selecione-o e clique em **OK** para o adicionar à lista.

23.2. 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 em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Perfis**, clique em **Definições**.
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 Cinema quando abrir uma certa aplicação de reprodução de vídeo, pode adicioná-lo manualmente à **Lista de aplicações de filme**.

Para adicionar manualmente leitores de vídeo à Lista de aplicações de filme no Perfil de Filme:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Perfis**, clique em **Definições**.
3. Clique no botão **CONFIGURAR** na área do Perfil de Filme.
4. Na janela **Definições do perfil de trabalho**, clique em **Lista de aplicações**.
5. Clique em **ADICIONAR**.

   Aparece uma nova janela. Vá até ao ficheiro executável da aplicação, selecione-o e clique em **OK** para o adicionar à lista.

23.3. 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 em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Perfis**, clique em **Definições**.
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 quando abre um certo jogo ou aplicação, pode adicioná-lo manualmente à **Lista de aplicações de jogos**.

Para adicionar jogos manualmente à lista de aplicações de jogos no Perfil de Jogo:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Perfis**, clique em **Definições**.
3. Clique no botão **CONFIGURAR** na área do Perfil de Jogos.
4. Na janela **Definições do perfil de trabalho**, clique em **Lista de aplicações**.
5. Clique em **ADICIONAR**.

   Aparece uma nova janela. Navegue até o ficheiro executável do jogo, selecione-o e clique em **OK** para adicioná-lo à lista.

23.4. 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 em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Perfis**, clique em **Definições**.
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**.

23.5. 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 em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Perfis**, clique em **Definições**.
3. Clique no botão **Configurar** na área do Perfil do 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.

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.

23.6. 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 em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Perfis**, clique em **Definições**.
3. Desloque-se para baixo até ver a opção de otimização em tempo real e utilize o botão correspondente para a ativar ou desativar.

24. PROTEÇÃO DE DADOS

24.1. 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 dispositivo utilizando 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. Clique em **Eliminar permanentemente** e, em seguida, confirme que deseja continuar com o processo.

   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 em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **Proteção de dados**, clique em **Destruidor de Ficheiros**.
3. Siga o assistente do Destruidor de Ficheiros:
   a. Clique no botão **Adicionar pastas** para adicionar os ficheiros ou pastas que deseja remover permanentemente.

      Alternativamente, arraste estes ficheiros ou pastas para esta janela.
   b. Clique em **Eliminar permanentemente** e, em seguida, confirme que deseja 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.

SOLUÇÃO DE PROBLEMAS

25. 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. 143)
- "*A análise não inicia*" (p. 144)
- "*Já não posso utilizar uma aplicação*" (p. 147)
- "*O que fazer quando a Bitdefender bloqueia um site, domínio, endereço de IP ou aplicação online segura*" (p. 148)
- "*Como atualizar o Bitdefender numa ligação à Internet lenta*" (p. 149)
- "*Os serviços Bitdefender não estão a responder*" (p. 149)
- "*A funcionalidade Preenchimento automático na minha Carteira não funciona*" (p. 150)
- "*Remoção de Bitdefender falhou*" (p. 151)
- "*O meu sistema não reinicia após a instalação de Bitdefender*" (p. 152)

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. 164).

25.1. 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. 69).

- **Não estão cumpridos os requisitos do sistema para executar o Bitdefender.**

  Se o seu dispositivo não cumprir os Requisitos do Sistema, ficará lento, especialmente se estiver a executar várias aplicações ao mesmo tempo. Para mais informação, dirija-se a "*Requisitos do sistema*" (p. 3).

- **Instalou aplicações que não utiliza**.

  Qualquer dispositivo 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 dispositivo. 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 em **Definições** no menu de navegação na interface do Bitdefender.
  2. No painel **ANTIVÍRUS**, clique em **Abrir**.
  3. Na janela **Análises**, clique em **Executar Análise** ao lado de **Análise do Sistema**.
  4. Siga os passos do assistente.

25.2. 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 Antivirus Plus** 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 Antivirus Plus** 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 Antivirus Plus** 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. 69).
  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 Antivirus Plus** 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 Antivirus Plus** 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 Antivirus Plus** 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. 164).

25.3. 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 isso acontecer, poderá excluir a respectiva aplicação para que não seja monitorizada pela Defesa Avançada Contra Ameaças.

Para adicionar o programa à lista de exceções:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ADVANCED THREAT DEFENSE**, clique em **Abrir**.
3. Na janela **Definições**, clique em **Gerir exceções**.
4. Clique em **+Adicionar uma Exceção**.
5. Introduza o caminho do executável que deseja adicionar à lista de exceção da verificação no campo correspondente.

   Como alternativa, pode navegar para o executável ao clicar no botão navegar no lado direito da interface, selecioná-lo e clicar em **OK**.
6. Ligue o interruptor ao lado de **Defesa contra Ameaças Avançadas**.
7. Clique em **Guardar**.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 164).

25.4. O que fazer quando a Bitdefender bloqueia um site, domínio, endereço de IP ou 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, domínio, endereço de IP ou aplicação online seguros como inseguros, o que fará com que a análise de tráfego HTTP da Bitdefender os bloqueie incorretamente.

Caso a mesma página, domínio, endereço de IP ou aplicação online estejam a ser bloqueados repetidamente, eles poderão ser adicionados para não serem analisados pelos mecanismos da Bitdefender, assegurando uma experiência de navegação mais tranquila.

Para adicionar uma página web a **Exceções**:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **PREVENÇÃO CONTRA AMEAÇAS ONLINE**, clique em **Definições**.
3. Clique em **Gerir exceções**.
4. Clique em **+Adicionar uma Exceção**.
5. No campo correspondente, escreva o nome do site, do domínio ou do endereço IP que deseja adicionar às excepções.

6. Clique no botão ao lado de **Prevenção de Ameaças Online**.
7. Clique em **Guardar** para guardar as alterações e fechar a janela.

Apenas sites, domínios, endereços de IP e aplicações nos quais confia plenamente devem ser adicionados à lista. Estes serão 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. 164).

25.5. 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 em **Definições** no menu de navegação na interface do Bitdefender.
2. Selecione o separador **Atualizar**.
3. Desligar o botão **Atualização silenciosa**.
4. A próxima vez que uma atualização estiver disponível, ser-lhe-á pedido para selecionar a atualização que deseja descarregar. Selecionar apenas **Atualização de assinaturas**.
5. O Bitdefender transfere e instala apenas a base de dados de informações de ameaças.

25.6. 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 dispositivo, 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 dispositivo e aguarde alguns momentos até o Bitdefender iniciar. Abra o Bitdefender e veja se o erro se mantém. Reiniciar o dispositivo 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. 69).

Se o erro persistir, por favor contacte os nossos representantes do suporte conforme descrito na secção "*Pedir Ajuda*" (p. 164).

25.7. 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 no botão **Abrir menu** no canto superior direito do ecrã.
3. Clique em Suplementos.
4. Clique em Extensões.
5. Vá à **Carteira do Bitdefender** e clique no interruptor ao lado dela.

- No **Google Chrome:**
  1. Abra o Google Chrome.
  2. Aceda ao ícone Menu.
  3. Clique em Mais Ferramentas.
  4. Clique em Extensões.
  5. Vá à **Carteira do Bitdefender** e clique no botão correspondente.

> **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. 164).

25.8. 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 Antivirus Plus** 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 Antivirus Plus** 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 Antivirus Plus** 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.

25.9. 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. 70).
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 Antivirus Plus** 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 Antivirus Plus** 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 Antivirus Plus** 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. 70).
  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. 70).
2. Utilizar a opção de Restauração do Sistema do Windows para restaurar o dispositivo 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. 164).

26. 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.

- "*Ambiente de Resgate*" (p. 156)
- "*O que fazer quando o Bitdefender encontra ameaças no seu dispositivo?*" (p. 157)
- "*Como posso limpar uma ameaça num ficheiro?*" (p. 159)
- "*Como posso limpar uma ameaça num ficheiro de e-mail?*" (p. 160)
- "*O que fazer se suspeitar que um ficheiro é perigoso?*" (p. 161)
- "*O que são os ficheiros protegidos por palavra-passe no relatório de análise?*" (p. 161)
- "*O que são os itens ignorados no relatório de análise?*" (p. 162)
- "*O que são os ficheiros muito comprimidos no relatório de análise?*" (p. 162)
- "*Por que é que Bitdefender eliminou automaticamente um ficheiro infectado?*" (p. 162)

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. 164).

26.1. Ambiente de Resgate

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.

O Ambiente de Resgate do Bitdefender está integrado com o Windows RE,

Arranque do sistema no Ambiente de Recuperação

Só pode aceder ao Ambiente de Recuperação a partir do produto Bitdefender como se segue:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Clique em **Abrir** ao lado de **Ambiente de Resgate**.
4. Clique em **REINICIAR** na janela que aparece.

   O Ambiente de Recuperação do Bitdefender é carregado dentro de momentos.

Analisar o seu sistema no Ambiente de Recuperação

Para analisar o seu sistema no Ambiente de Recuperação:

1. Aceda ao Ambiente de Recuperação como descrito em "Arranque do sistema no Ambiente de Recuperação" (p. 157).
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.

26.2. O que fazer quando o Bitdefender encontra ameaças no seu dispositivo?

Pode descobrir que há uma ameaça no seu dispositivo numa dessas formas:

- O Bitdefender analisou o seu dispositivo e encontrou itens infetados.
- Um alerta de ameaças avisa que o Bitdefender bloqueou uma ou várias ameaças no seu dispositivo.

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 em **Definições** no menu de navegação na interface do Bitdefender.
   b. No painel **ANTIVÍRUS**, clique em **Abrir**.
   c. Na janela **Avançada**, desative o **Escudo do Bitdefender**.
2. Mostrar objetos ocultos no Windows. Para saber como o fazer, consulte "*Como posso mostrar objetos ocultos no Windows?*" (p. 68).
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. 70).
2. Mostrar objetos ocultos no Windows. Para saber como o fazer, consulte "*Como posso mostrar objetos ocultos no Windows?*" (p. 68).
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. 164).

26.3. 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 em **Definições** no menu de navegação na interface do Bitdefender.
   b. No painel **ANTIVÍRUS**, clique em **Abrir**.
   c. Na janela **Avançada**, desative o **Escudo do Bitdefender**.
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. 164).

26.4. 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 em **Definições** no menu de navegação na interface do Bitdefender.
   b. No painel **ANTIVÍRUS**, clique em **Abrir**.
   c. Na janela **Avançada**, desative o **Escudo do Bitdefender**.
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. 164).

26.5. 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. 54).
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. 164).

26.6. 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 esses conteúdos pudessem ser extraídos, o analisador em tempo real do Bitdefender analisaria-os automaticamente para manter o seu dispositivo

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.

26.7. 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.

26.8. 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.

26.9. 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.

CONTACT US

27. 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. 143) 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:

- "Contate-nos diretamente desde o Bitdefender Antivirus Plus" (p. 164)
- "Contacte-nos através do nosso Centro de Suporte Online" (p. 165)

Contate-nos diretamente desde o Bitdefender Antivirus Plus

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 botão **Suporte**, representado por um **ponto de interrogação**, na parte superior 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.
   - **CONTACTAR**

     Clique **Contactar Suporte** para executar a Ferramenta de Suporte da Bitdefender e contactar 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. Reproduza o problema e, em seguida, clique em **FINALIZAR** no quadro REPRODUZINDO O 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 **CRIAR PACOTE DE DEBUG**.

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.

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.

28. 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.

28.1. 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.

28.2. 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 certas ameaças do seu dispositivo 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.

28.3. 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 dispositivo 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.

29. CONTACT INFORMATION

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.

29.1. 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

29.2. 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.

29.3. 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
Phone: (+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
Phone: +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
Orhideea Towers Building, 15A Orhideelor Street, 11th fllor, district 6
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.

Ataque de dicionário

Foi utilizado um ataque de adivinhação de palavras-passe para invadir o sistema de um computador introduzindo uma combinação de palavras comuns para gerar possíveis palavras-passe. É utilizado o mesmo método para adivinhar palavras-passe de mensagens ou documentos encriptados. Os ataques de dicionário funcionam devido à tendência de muitas pessoas escolherem palavras-passe curtas ou de uma palavra que acabam por ser fáceis de serem adivinhadas.

Ataque de força bruta

Foi utilizado um ataque de adivinhação de palavras-passe para invadir o sistema de um computador introduzindo possíveis combinações de palavras-passe, começando pelas mais fáceis de adivinhar.

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.

Boot sector

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.

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.

Cyberbullying

Quando colegas ou estranhos cometem atos abusivos contra crianças de propósito para as ferir fisicamente. Para causar danos emocionais,

os agressores enviam mensagens ou fotos mal-intencionadas, que fazem com que as suas vítimas se isolem de outros e se sintam frustradas.

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.

Explorações

Uma forma de se aproveitarem de diferentes bugs ou vulnerabilidades presentes num computador (software ou hardware). Assim, os hackers podem obter controlo de computadores ou redes.

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 incluem ".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.

Predadores online

Pessoas que procuram atrair menores de idade ou adolescentes para conversas com o objetivo de os envolver em atividades sexuais ilegais. As redes sociais são o local ideal para caçar e seduzir facilmente crianças vulneráveis para realizar atividades sexuais, tanto online como cara a cara.

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.

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.