

# Bitdefender<sup>®</sup> ANTIVIRUS FREE



GUIA DO USUÁRIO





# Antivírus Bitdefender Gratuito

## Guia do usuário

Data de publicação 27/07/2023  
Copyright © 2023 Bitdefender

## Notícia legal

**Todos os direitos reservados.** Nenhuma parte deste livro pode ser reproduzida ou transmitida de qualquer forma ou por qualquer meio, eletrônico ou mecânico, incluindo fotocópia, gravação ou por qualquer sistema de armazenamento e recuperação de informações, sem permissão por escrito de um representante autorizado da Bitdefender. A inclusão de breves citações em resenhas pode ser possível apenas com a menção da fonte citada. O conteúdo não pode ser modificado de forma alguma.

**Aviso e isenção de responsabilidade.** Este produto e sua documentação são protegidos por direitos autorais. As informações neste documento são fornecidas "como estão", sem garantia. Embora todas as precauções tenham sido tomadas na preparação deste documento, os autores não terão qualquer responsabilidade perante qualquer pessoa ou entidade com relação a qualquer perda ou dano causado ou supostamente causado direta ou indiretamente pelas informações contidas neste trabalho.

Este livro contém links para sites de terceiros que não estão sob o controle da Bitdefender, portanto, a Bitdefender não é responsável pelo conteúdo de qualquer site vinculado. Se você acessar um site de terceiros listado neste documento, o fará por sua conta e risco. A Bitdefender fornece esses links apenas como uma conveniência, e a inclusão do link não implica que a Bitdefender endosse ou aceite qualquer responsabilidade pelo conteúdo do site de terceiros.

**Marcas registradas.** Nomes de marcas registradas podem aparecer neste livro. Todas as marcas comerciais registradas e não registradas neste documento são de propriedade exclusiva de seus respectivos proprietários e são reconhecidas com respeito.

Bitdefender®



## Índice

<b>Sobre este guia .....</b>	<b>1</b>
Objetivo e público-alvo .....	1
Como usar este guia .....	1
Convenções utilizadas neste guia .....	1
Convenções Tipográficas .....	1
Avisos .....	2
Pedido de Comentários .....	2
<b>1. Instalação .....</b>	<b>4</b>
1.1. A preparar a instalação .....	4
1.2. Requisitos do sistema .....	4
1.3. Requisitos de Software .....	5
1.4. Instalação do seu produto Bitdefender .....	6
1.4.1. A instalar a partir da Central Bitdefender .....	6
1.4.2. Instalar a partir do disco de instalação .....	9
<b>2. Começar .....</b>	<b>14</b>
2.1. Os básicos .....	14
2.1.1. Notificações .....	15
2.1.2. Perfis .....	16
2.1.3. Definições de proteção da palavra-passe de Bitdefender ...	17
2.1.4. Relatórios do produto .....	18
2.1.5. Notificações de ofertas especiais .....	19
2.2. Interface do Bitdefender .....	19
2.2.1. Ícone na área de notificação .....	20
2.2.2. Menu de navegação .....	21
2.2.3. Painel .....	22
2.2.4. Secções do Bitdefender .....	25
2.2.5. Mude o idioma do produto .....	29
2.3. Bitdefender Central .....	30
2.3.1. Sobre a Central Bitdefender .....	30
2.3.2. Aceda à Central Bitdefender .....	31
2.3.3. Autenticação de dois fatores .....	31
2.3.4. Adicionar dispositivos fiáveis .....	33
2.3.5. Actividade .....	34
2.3.6. As minhas subscrições .....	34
2.3.7. Meus dispositivos .....	36
2.3.8. Notificações .....	40
2.4. Manter o Bitdefender atualizado .....	40
2.4.1. Verificar se o Bitdefender está atualizado .....	40
2.4.2. A efetuar uma atualização .....	41



2.4.3. Ligar ou desligar a atualização automática .....	41
2.4.4. Ajuste das configurações da atualização .....	42
2.4.5. Atualizações contínuas .....	43
<b>3. Gerir a sua segurança .....</b>	<b>44</b>
3.1. Proteção Antivírus .....	44
3.1.1. Análise no acesso (proteção em tempo real) .....	45
3.1.2. Verificação por ordem .....	49
3.1.3. Ver os relatórios da análise .....	58
3.1.4. Análise automática de média removíveis .....	59
3.1.5. A configurar exceções de análise .....	61
3.1.6. Gerir ficheiros da quarentena .....	63
3.2. Defesa Avançada contra Ameaças .....	64
3.2.1. Ativar ou desativar o Advanced Threat Defense .....	64
3.2.2. A verificar ataques maliciosos detectados .....	65
3.2.3. A adicionar processos a exceções .....	65
3.2.4. Detecção de exploits .....	65
3.2.5. Ativar ou desativar a deteção de exploits .....	66
3.3. Prevenção de ameaças on-line .....	66
3.3.1. Alertas do Bitdefender no navegador .....	68
<b>4. Como .....</b>	<b>69</b>
4.1. Instalação .....	69
4.1.1. Como instalo o Bitdefender num segundo dispositivo? ....	69
4.1.2. Como posso reinstalar o Bitdefender? .....	69
4.1.3. De onde é que posso transferir o meu produto Bitdefender? .....	70
4.1.4. Como posso atualizar o Bitdefender para a versão mais recente? .....	71
4.2. Bitdefender Central .....	72
4.2.1. Como faço para aceder o Bitdefender com outra conta? ...	72
4.2.2. Como desligar as mensagens de ajuda da Central Bitdefender? .....	73
4.2.3. Esqueci-me da palavra-passe que defini para a minha conta Bitdefender. Como é que a reponho? .....	73
4.2.4. Como posso gerir os inícios de sessão associados à minha conta do Bitdefender? .....	74
4.3. A analisar com BitDefender .....	74
4.3.1. Como posso analisar um ficheiro ou uma pasta? .....	74
4.3.2. Como posso analisar o seu sistema .....	75
4.3.3. Como programar uma verificação? .....	75
4.3.4. Como posso criar uma tarefa de análise personalizada? .	76
4.3.5. Como excluir uma pasta da análise? .....	78



4.3.6. O que fazer se o Bitdefender identificar um ficheiro limpo como infectado? .....	79
4.3.7. Como posso saber que ameaças o Bitdefender detetou? ..	80
4.4. Informações Úteis .....	80
4.4.1. Como posso testar a minha solução de segurança? .....	80
4.4.2. Como removo o Bitdefender? .....	81
4.4.3. Como desligo automaticamente o meu dispositivo após terminar a análise? .....	82
4.4.4. Como posso configurar o Bitdefender para utilizar uma ligação à internet com proxy? .....	83
4.4.5. Estou a utilizar uma versão de 32 ou 64 Bit do Windows? .....	85
4.4.6. Como posso mostrar objetos ocultos no Windows? .....	85
4.4.7. Como posso remover outras soluções de segurança? .....	86
4.4.8. Como posso reiniciar no Modo de Segurança? .....	87
<b>5. Solução de problemas .....</b>	<b>89</b>
5.1. Resolver incidências comuns .....	89
5.1.1. O meu sistema parece estar lento .....	89
5.1.2. A análise não inicia .....	91
5.1.3. Já não posso utilizar uma aplicação .....	93
5.1.4. O que fazer quando o Bitdefender bloqueia um site, domínio, endereço IP ou aplicação online que é seguro .....	94
5.1.5. Como atualizar o Bitdefender numa ligação à Internet lenta .....	95
5.1.6. Os serviços do Bitdefender não estão a responder .....	96
5.1.7. A remoção Bitdefender falhou .....	96
5.1.8. O meu sistema não reinicia após a instalação de Bitdefender .....	98
5.2. Remover ameaças do seu sistema .....	101
5.2.1. O que fazer quando o Bitdefender encontrar ameaças no seu dispositivo? .....	101
5.2.2. Como posso limpar uma ameaça num ficheiro? .....	103
5.2.3. Como posso limpar uma ameaça num ficheiro de e-mail? .....	104
5.2.4. O que fazer se suspeitar que um ficheiro é perigoso? .....	105
5.2.5. O que são os ficheiros protegidos por palavra-passe no relatório de análise? .....	106
5.2.6. O que são os itens ignorados no relatório de análise? .....	106
5.2.7. O que são os ficheiros muito comprimidos no relatório de análise? .....	106
5.2.8. Por que é que Bitdefender eliminou automaticamente um ficheiro infectado? .....	107



<b>6. Conseguindo ajuda .....</b>	<b>108</b>
6.1. Pedir Ajuda .....	108
6.2. Recursos Em Linha .....	108
6.2.1. Centro de Suporte da Bitdefender .....	108
6.2.2. A Comunidade de Especialistas da Bitdefender .....	109
6.2.3. Bitdefender Cyberpedia .....	109
6.3. Informações de Contato .....	110
6.3.1. Distribuidores locais .....	110
<b>Glossário .....</b>	<b>111</b>





## SOBRE ESTE GUIA

### Objetivo e público-alvo

Este guia destina-se a todos os usuários do Windows que escolheram Bitdefender Antivirus Free como uma solução de segurança para seus computadores. As informações apresentadas neste livro são adequadas não apenas para especialistas em computação, mas também acessíveis a todos que podem trabalhar com um PC com Windows.

Você descobrirá como configurar e usar Bitdefender Antivirus Free para se proteger contra ameaças e outros softwares mal-intencionados. Você aprenderá como tirar o melhor proveito do seu Bitdefender.

Desejamos-lhe uma palestra agradável e útil.

### Como usar este guia

Este guia está organizado em torno de vários tópicos principais:

[Começar \(página 14\)](#)

Comece a usar o Bitdefender Free e sua interface de usuário.

[Gerir a sua segurança \(página 44\)](#)

Aprenda a usar o Bitdefender Free para se proteger contra software malicioso.

[Como \(página 69\)](#)

Saiba mais sobre o Bitdefender Free.

[Conseguindo ajuda \(página 108\)](#)

Onde procurar e onde pedir ajuda se algo inesperado aparecer.

## Convenções utilizadas neste guia

### Convenções Tipográficas

São utilizados diversos estilos de texto neste manual para uma maior facilidade de leitura. O seu aspecto e significado são apresentados na tabela abaixo.



Aparência	Descrição
<code>sample syntax</code>	As amostras de sintaxe são impressas com <b>monospaced</b> personagens.
<a href="https://www.bitdefender.com">https://www.bitdefender.com</a>	A hiperligação URL aponta para uma localização externa em servidores http ou ftp.
<a href="mailto:documentation@bitdefender.com">documentation@bitdefender.com</a>	Endereços de email são inseridos no texto para contactar a solicitar mais informação.
<a href="#">Sobre este Guia (página 1)</a>	Esta é uma hiperligação interna que o leva para uma localização dentro do documento.
<code>filename</code>	Arquivos e diretórios são impressos usando <b>monospaced</b> Fonte.
<b>opção</b>	Todas as opções de produtos são impressas usando <b>audacioso</b> personagens.
<b>palavra-chave</b>	Palavras-chave ou frases importantes são destacadas usando <b>audacioso</b> personagens.

## Avisos

Os avisos estão em notas internas do texto, com marcação gráfica, que chamam a sua atenção para informações adicionais relacionadas ao parágrafo atual.



### Observação

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



### Importante

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



### Aviso

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

## Pedido de Comentários

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





Informe-nos enviando um e-mail para [documentation@bitdefender.com](mailto:documentation@bitdefender.com).  
Escreva todos os seus e-mails relacionados à documentação em inglês  
para que possamos processá-los com eficiência.



## 1. INSTALAÇÃO

### 1.1. A preparar a instalação

Antes de instalar o Bitdefender Antivirus Free, 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 \(página 4\)](#).
- 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.
- Desativar ou remover qualquer programa de firewall que possa estar em execução no dispositivo. Executar dois programas de firewall simultaneamente poderá afetar o seu funcionamento e causar grandes problemas no sistema. A Firewall do Windows será desativada durante a instalação.
- Recomenda-se que o seu 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 incluídos no pacote de instalação, o Bitdefender irá descarregá-las e instalá-las.

### 1.2. Requisitos do sistema

Só pode instalar o Bitdefender Antivirus Free 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.



## Observação

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 **Meu Computador** na área de trabalho, depois selecione **Propriedades** no menu.
- No **Windows 8**, a partir do ecrã Iniciar, localize **Computador** (por exemplo, pode começar a escrever "Computador" diretamente no ecrã Iniciar) e, em seguida, clique com o botão direito do rato 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**, escreva **Sistema** na caixa de pesquisa da barra de tarefas e clique no ícone correspondente. Procure na área de **Sistema** para encontrar informações sobre o seu tipo de sistema.

## 1.3. 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
- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 e superior



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

### 1.4.1. A instalar a partir da Central Bitdefender

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 Free é ativado.

Para transferir Bitdefender Antivirus Free a partir do Bitdefender Central:

1. Aceda à **Central da Bitdefender**.
2. Selecione o painel **Os meus dispositivos** e, em seguida, 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 proprietário do dispositivo. Se o dispositivo pertencer a outra pessoa, clique no botão correspondente.
- b. Clique em **ENVIAR LINK PARA A TRANSFERÊNCIA**.
- 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

Em primeiro lugar, o Bitdefender verifica o seu 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 Total Security é constantemente atualizado.



### Observação

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

Assim que a instalação estiver validada, o assistente de configuração irá aparecer. Siga os passos para instalar Bitdefender Antivirus Free.

## Passo 1 - Instalação do Bitdefender

Antes de concluir o processo de instalação, deve concordar com o Contrato de Subscrição. Leia o Acordo de Subscrição com calma, já que ele contém os termos e condições segundo os quais pode utilizar o Bitdefender Antivirus Free.

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 progresso

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**.



### Observação

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 **TERMINAR** para aceder à Bitdefender Antivirus Free interface.

## 1.4.2. 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

Em primeiro lugar, o Bitdefender verifica o seu 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 Total Security é constantemente atualizado.



### Observação

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

Assim que a instalação estiver validada, o assistente de configuração irá aparecer. Siga os passos para instalar Bitdefender Antivirus Free.



## Passo 1 - Instalação do Bitdefender

Antes de prosseguir com a instalação, você deve concordar com o Contrato de Assinatura. Reserve algum tempo para ler o Contrato de Assinatura, pois contém os termos e condições sob os quais você pode usar Bitdefender Antivirus Free.

Se você não concorda com estes termos, feche a janela. O processo de instalação será abandonado e você sairá do setup.

Duas tarefas adicionais podem ser executadas nesta etapa:

- Mantenha o **Enviar relatórios de produtos** opção habilitada. Ao permitir esta opção, os relatórios contendo informações sobre como você usa o produto são enviados para os servidores da Bitdefender. Essas informações são essenciais para melhorar o produto e podem nos ajudar a proporcionar uma experiência melhor no futuro. Observe que esses relatórios não contêm dados confidenciais, como seu nome ou endereço IP, e que não serão usados para fins comerciais.
- Selecione o idioma no qual deseja instalar o produto.

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

## Passo 2 - Instalação em processo

Aguarde a conclusão da instalação. Informações detalhadas sobre o progresso são exibidas.

## Passo 3 - Instalação concluída

Um resumo da instalação é exibido. Se alguma ameaça ativa foi detectada e removida durante a instalação, uma reinicialização do sistema pode ser necessária.

## Etapa 4 - Análise do dispositivo

Agora você será perguntado se deseja realizar uma análise do seu dispositivo, para garantir que ele seja seguro. Durante esta etapa, o Bitdefender verificará as áreas críticas do sistema. Clique **Iniciar análise do dispositivo** para iniciá-lo.

Você pode ocultar a interface de digitalização clicando em **Executar verificação em segundo plano**. Depois disso, escolha se deseja ser informado quando a verificação for concluída ou não.



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



## Observação

Como alternativa, se você não deseja realizar a verificação, basta clicar em **Pular**.

## Passo 5 - Conta Bitdefender

Após concluir a configuração inicial, a janela Bitdefender Account aparece. É necessária uma conta Bitdefender para ativar o produto e utilizar as suas ferramentas online. Para mais informação, dirija-se a [Bitdefender Central \(página 30\)](#).

Proceda consoante a sua situação.

### ○ Pretendo 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 caracteres, incluindo pelo menos um número ou símbolo, um carácter 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**.



## Observação

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 **Iniciar sessão**.
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-se da 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 deseja definir, depois introduza-a novamente. Clique em **GUARDAR**.



## Observação

Caso já tenha uma conta MyBitdefender, pode utilizá-la para entrar na sua conta Bitdefender. Caso se tenha esquecido da palavra-passe, deve ir primeiro a <https://my.bitdefender.com> para repô-la. Em seguida, utilize as credenciais atualizadas para entrar 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. Será 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.



## Observação

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



### Observação

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. Introduza o código de ativação no campo Eu tenho um código de ativação, depois clique em **CONTINUAR**.



### Observação

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. **Pretendo avaliar o Bitdefender**

Neste caso, pode utilizar o produto durante um período de 30 dias. Para iniciar o período de avaliação, selecione **Não tenho uma subscrição; quero experimentar o produto de forma gratuita** e, em seguida, clique em **CONTINUAR**.

## Passo 7 - Introdução

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

Clique **TERMINAR** para acessar o Bitdefender Antivirus Free interface.



## 2. COMEÇAR

### 2.1. Os básicos

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

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

Ligar-se a redes sem fios públicas de aeroportos, shoppings, cafés ou hotéis sem proteção pode ser perigoso para o seu dispositivo e para os seus dados. 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](#).

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

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

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](#).

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](#).

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 \(página 15\)](#).

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


Para utilizar as funcionalidades online do Bitdefender Antivirus Free, gerir as suas subscrições e os dispositivos, aceda à sua conta Bitdefender. Para mais informação, dirija-se a [Bitdefender Central \(página 30\)](#).

A secção [Como \(página 69\)](#) é onde encontrará as instruções passo a passo para executar as tarefas comuns. Se tiver problemas durante a utilização do Bitdefender, verifique a secção [Resolver incidências comuns \(página 89\)](#) para encontrar possíveis soluções para os problemas mais comuns.

## 2.1.1. Notificações

O Bitdefender mantém um registo detalhado dos eventos relativos à sua atividade no seu dispositivo. Sempre que algo relevante para a segurança do seu sistema ou dos seus dados ocorrer, uma nova mensagem será adicionada à área de notificações do Bitdefender, de forma semelhante a um novo e-mail que aparece 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 na **interface do Bitdefender**. Sempre que um evento crítico ocorrer, um contador poderá ser visto no ícone .

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



- Os eventos **críticos** indicam problemas críticos. Deve verificá-los imediatamente.
- O eventos de **Aviso** indicam incidências não críticas. Dev verificar e resolvê-los quando puder.
- Eventos de **Informação** indicam operações bem sucedidas.

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

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

## 2.1.2. 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 Bitdefender atribuem mais recursos do sistema às aplicações em execução ao modificar temporariamente as definições de proteção e ajustar 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 de 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 de Wi-Fi Público

Aplica definições do produto para beneficiar da proteção completa enquanto está ligado a uma rede sem fios insegura.

## Perfil de modo de bateria

Aplica definições de produto e coloca em pausa as atividades em segundo plano para economizar bateria.

## Configure a ativação automática de perfis

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

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](#).

## 2.1.3. 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. Escreva a palavra-passe nos dois campos e, em seguida, clique em **OK**. A palavra-passe deve 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 suporte do Bitdefender.

Para remover a proteção por palavra-passe:

1. Clique **Configurações** no menu de navegação do [Interface do Bitdefender](#).
2. Na janela **Geral**, desative a **Proteção por palavra-passe**.
3. Digite a palavra-passe e, em seguida, clique em **OK**.



### Observação

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.

## 2.1.4. 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 **Configurações** no menu de navegação do [Interface do Bitdefender](#).
2. Selecione o separador **Avançado**.
3. Desative os **Relatórios de produto**.

## 2.1.5. 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 **Configurações** no menu de navegação do [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.

## 2.2. Interface do Bitdefender

O Bitdefender Antivirus Free 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** exhibe 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 a área de definições, notificações e as **sessões do Bitdefender** para as definições detalhadas e as tarefas administrativas avançadas.

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

## 2.2.1. Ícone na área de notificação


Para gerir todo o produto mais rapidamente, pode utilizar o ícone do Bitdefender  na bandeja do sistema.



### Observação

O ícone do Bitdefender pode não estar sempre visível. Para fazer o ícone surgir de forma permanente:

#### ○ No **Windows 7, Windows 8 e Windows 8.1**

1. Clique na seta  no canto inferior direito do ecrã.
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. Percorra na página para baixo e clique no link **Selecionar quais ícones aparecem na barra de tarefas** na **Área de notificação**.
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.

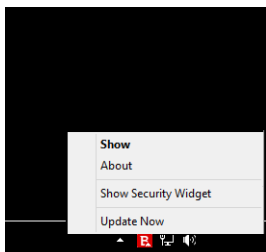
○ **Exibir** - abre a janela principal do Bitdefender.

○ **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** - inicia uma atualização imediata. Pode acompanhar o estado da atualização no painel Atualizações na **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 bandeja do sistema aparece sobre um fundo cinzento: . Isto acontece normalmente quando a subscrição expira. Também pode ocorrer quando os serviços Bitdefender não estão a responder ou quando outros erros afetam o funcionamento normal do Bitdefender.

## 2.2.2. 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 de controlo.** Aqui, pode reparar os problemas de segurança rapidamente, ver recomendações de acordo com as necessidades e uso do seu dispositivo, além de realizar ações rápidas e instalar o Bitdefender em outros dispositivos.
-  **Proteção.** Daqui, pode executar e configurar análises antivírus, aceder às definições do Firewall, recuperar dados encriptados por ransomware e configurar a proteção enquanto navega na internet.



-  **Privacidade.** Aqui, pode criar gestores de palavras-passe para as suas contas online, proteger o acesso à sua webcam contra espões, fazer pagamentos online num ambiente online, abrir a aplicação do VPN e proteger os seus filhos ao visualizar e restringir a sua atividade online.
-  **Funcionalidades.** Aqui, pode otimizar a velocidade do sistema e configurar a função Antifurto para os seus dispositivos.
-  **Notificações.** A partir daqui pode aceder às notificações geradas.
-  **Definições.** A partir daqui, é possível aceder às definições gerais.
-  **Suporte.** Aqui, sempre que precisar de assistência para resolver uma situação com o seu Bitdefender Antivirus Free, pode contactar o departamento de Suporte Técnico da Bitdefender.
-  **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.

## 2.2.3. 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 e a funcionar na velocidade ideal. Também pode instalar Bitdefender noutros dispositivos, uma vez que a sua subscrição tem entradas disponíveis suficientes.



## 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, um pop-up confirma 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.

## Autopilot

Para oferecer uma operação efetiva e maior proteção ao realizar diferentes atividades, o Autopilot da Bitdefender atuará como seu conselheiro pessoal de segurança. Dependendo da atividade que realizar, seja trabalhar, fazer pagamentos online, assistir a filmes ou jogar jogos, o Autopilot da Bitdefender fornecerá recomendações contextuais com base na sua 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.

### A desativar 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 **Configurações** no menu de navegação do **Interface do Bitdefender**.




2. Na janela **Geral**, desative as **Notificações de recomendações**.

## Ações rápidas

Utilizando as ações rápidas, pode executar com rapidez tarefas que considera importantes para manter o seu sistema protegido e a funcionar na melhor velocidade possível.

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:

- **Verificação rápida.** Realizar uma verificação rápida para detetar imediatamente as possíveis ameaças que podem estar presentes no seu dispositivo.
- **Verificação do sistema.** Execute uma verificação do sistema para garantir que o dispositivo esteja livre de ameaças.
- **Análise de vulnerabilidades.** Analise o seu dispositivo para identificar vulnerabilidades e garantir que todas as aplicações instaladas, juntamente com o sistema operativo, 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.
- **Abrir o Safepay.** Abra o Bitdefender Safepay™ para proteger os seus dados privados ao realizar transações online.
- **Abrir VPN.** Abra o Bitdefender VPN para adicionar uma camada de proteção enquanto estiver ligado à internet.
- **Destruidor de Ficheiros.** Abra o Destruidor de Ficheiros para remover todos os traços de dados sensíveis do seu dispositivo.
- **Abrir o Otimizador em um Clique.** Liberte espaço em disco, corrija erros de registo e proteja a sua privacidade ao apagar ficheiros que não são mais úteis com um único clique.

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 **ENVIAR LINK PARA TRANSFERÊNCIA**.
3. Siga os passos no ecrã para instalar o Bitdefender.




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

- ☐ Bitdefender Antivirus Free nos dispositivos Windows.
- ☐ Bitdefender Antivirus para Mac em dispositivos MacOS.
- ☐ Bitdefender Mobile Security em dispositivos Android.
- ☐ Bitdefender Mobile Security em dispositivos iOS.

## 2.2.4. 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 quiser aceder às funcionalidades de uma secção específica ou para começar a configurar o seu produto, clique nos ícones seguintes, localizados no menu de navegação na **interface do Bitdefender**:

- ☐  **Proteção**
- ☐  **Privacidade**
- ☐  **Funcionalidades**

## Proteção

Na secção Proteção, pode ajustar as suas definições avançadas de segurança, gerr amigos e spammers, ver e editar as definições da ligação de rede, configurar as funções da Prevenção Contra Ameaças Online, conferir e reparar potenciais vulnerabilidades do sistema e avaliar as redes sem fios às quais se liga.

As funcionalidades que pode gerir na secção Proteção são:

### ANTIVÍRUS



A proteção antivírus 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 \(página 44\)](#).

## **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 on-line \(página 66\)](#).

## **FIREWALL**

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

Para mais informações sobre configuração de firewall, consulte [Firewall](#).

## **DEFESA AVANÇADA CONTRA AMEAÇAS**

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 [Defesa Avançada contra Ameaças \(página 64\)](#).

## **ANTISPAM**

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

Para mais informações sobre a proteção antispam, consulte [Antispam](#).





## 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 espões.

Para mais informações sobre como configurar a proteção de vulnerabilidade, consulte [Vulnerabilidade](#).

## REMEDIÇÃO 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](#).

## Privacidade

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

As funcionalidades que pode gerir na secção Privacidade são:

### VPN

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

Para mais informações sobre esta funcionalidade, consulte [VPN](#).

## PROTEÇÃO DE VÍDEO E ÁUDIO



A Proteção de Vídeo e Áudio mantém a sua webcam fora de perigo ao bloquear o acesso de aplicações não confiáveis e notifica quando alguma aplicação tentar obter acesso ao seu microfone.

Para saber mais sobre como manter a sua webcam protegida contra acessos indesejados e como configurar o Bitdefender para o(a) notificar sobre a atividade do seu microfone, consulte [Proteção de Audio & Vídeo](#).

## 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™, aceda ao [Segurança Safepay para transações online](#).

## CONTROLO PARENTAL

O Controlo Parental da Bitdefender permite monitorizar o que os seus filhos fazem nos seus dispositivos. Em caso de conteúdo inadequado, pode decidir restringir o seu acesso à internet ou a aplicações específicos.

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

Para mais informações sobre a configuração do Controlo Parental, aceda a [Controle dos pais](#).

## 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](#).

## Utilitários

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

### Otimizar num único Clique

O Bitdefender Total Security oferece não só segurança, mas também ajuda a manter o desempenho do seu dispositivo em forma.



O nosso Otimizador em Um Clique irá ajudar a remover os ficheiros desnecessários do seu dispositivo num único e simples passo.

Para mais informações, dirija-se a [OneClick Optimizer](#).

## **Antifurto**

O Antirroubo da Bitdefender protege o seu dispositivo e os seus dados contra o roubo ou a perda. Caso algum destes eventos ocorra, ele permitirá que localize ou bloqueie remotamente o seu dispositivo. Também pode limpar todos os dados presentes no seu sistema.

O Antifurto da Bitdefender oferece as seguintes funções:

- ☐ Localização Remota
- ☐ Bloqueio Remoto
- ☐ Limpeza Remota
- ☐ Alerta Remoto

Para mais informações sobre como pode manter o seu sistema longe das mãos erradas, consulte [Device Anti-Theft](#).

## **Proteção de dados**

O Destruidor de Ficheiros da Bitdefender ajuda a eliminar dados de forma permanente ao removê-los fisicamente do seu disco rígido.

Para mais informações sobre ele, consulte [Proteção de dados](#).

## **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 obter mais informações sobre esse recurso, consulte [Perfis](#).

## **2.2.5. 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 **Configurações** no menu de navegação do [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.

## 2.3. Bitdefender Central

### 2.3.1. Sobre a Central Bitdefender

A Central Bitdefender é a plataforma onde tem acesso aos recursos e serviços online do produto e pode realizar remotamente tarefas importantes em dispositivos nos quais o Bitdefender estiver instalado. Você pode entrar na sua conta da Bitdefender a partir de qualquer computador ou telemóvel ligado à internet ao aceder ao <https://central.bitdefender.com>, ou diretamente da aplicação da Central Bitdefender em dispositivos Android e iOS.

Para instalar a aplicação da Central Bitdefender nos seus dispositivos:

- **Em Android** - procure por Bitdefender Central no Google Play e descarregue e instale a aplicação. Siga os passos necessários para completar a instalação.
- **Em 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 Bitdefender nos sistemas operativos Windows, macOS, iOS e Android. Os produtos disponíveis para transferência são:
  - A linha de produtos da Bitdefender para Windows
  - Bitdefender Antivirus for Mac
  - Bitdefender Mobile Security for 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.
- Proteja os dispositivos de rede e os seus dados contra roubo ou perda com o **Anti-Roubo**.
- Configurar as definições do **Parental Control** para as contas das suas crianças e monitorizar a sua atividade onde quer que eles estejam.

## 2.3.2. Aceda à Central Bitdefender

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

- A partir da interface principal do Bitdefender:
  1. Clique em **Minha Conta** no menu de navegação na **Interface do Bitdefender**.
  2. Clique em **Ir para a Central Bitdefender**.
  3. Inicie a sessão na sua conta Bitdefender com 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 a: <https://central.bitdefender.com>.
  3. Inicie sessão na sua conta com o seu endereço de e-mail e palavra-passe.
- No seu dispositivo Android ou iOS:
  1. Abra a aplicação da Central Bitdefender que instalou.



### Observação

Neste material incluímos as opções que pode encontrar na interface na web.

## 2.3.3. 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. Acesso [Bitdefender Central](#).
2. Clique no ícone  no lado superior direito do ecrã.
3. Clique em **Conta da Bitdefender** no menu suspenso.
4. Selecione o separador **Palavra-passe e segurança**.
5. Clique em **Autenticação de 2 fatores**.
6. Clique em **COMEÇAR**.

Selecione uma das seguintes opções:

- **Aplicação de autenticação** - utilize uma aplicação 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 computador, 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 o seu email e utilize o código que lhe foi enviado.
  - a. Clique em **UTILIZAR E-MAIL** para começar.
  - b. Verifique a sua conta de e-mail e introduza o código fornecido.
  - 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 **CONCLUÍDO**.

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.

## 2.3.4. 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. Acesso [Bitdefender Central](#).
2. Clique no  ícone no canto superior direito da tela.
3. Clique **Conta Bitdefender** no menu de slides.
4. Selecione os **Senha e segurança** aba.
5. Clique em **Dispositivos de confiança**.



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.

## 2.3.5. 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 ver o número dos dispositivos ligados juntamente com seu estado de proteção. Para corrigir problemas remotamente nos dispositivos detetados, clique em **Corrigir problemas**, e depois, clique em **VERIFICAR E RESOLVER OS 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 de 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.

## 2.3.6. As minhas subscrições

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

### Verificar subscrições disponíveis

Para verificar as suas subscrições disponíveis:





1. Acesso [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.



## Observação

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

## Ativar subscrição

É possível ativar uma subscrição durante o processo de instalação ao utilizar a sua conta Bitdefender. Juntamente com o processo de ativação, a validade da subscrição inicia a sua contagem decrescente.

Se tiver comprado um código de ativação de um dos nossos revendedores ou o tiver recebido como presente, pode adicionar a sua disponibilidade à sua subscrição do Bitdefender.

Para ativar uma subscrição com um código de ativação, siga os passos abaixo:

1. Acesso [Bitdefender Central](#).
2. Selecione os **Minhas assinaturas** painel.
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.

## Renovar subscrição

Caso tenha desativado a renovação automática da sua subscrição do Bitdefender, pode renová-la manualmente seguindo estas instruções:

1. Acesso [Bitdefender Central](#).
2. Selecione os **Minhas assinaturas** painel.
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.

## 2.3.7. Meus dispositivos

A secção **Os Meus Dispositivos** na sua conta Bitdefender permite-lhe instalar, gerir e realizar ações remotas no seu Bitdefender em qualquer dispositivo, desde que esteja ativado e ligado à Internet. Os cartões de dispositivos exibem o nome do dispositivo, o estado da proteção e se há algum risco de segurança afetando a proteção dos seus dispositivos.

## Adicione um novo dispositivo

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

1. Acesso [Bitdefender Central](#).
2. Selecione os **Meus dispositivos** painel e, em seguida, toque em **INSTALAR PROTEÇÃO**.
3. Escolha uma das duas opções disponíveis:

- ☐ **Proteger este dispositivo**

Selecione esta opção e, em seguida, selecione o proprietário do dispositivo. Se o dispositivo pertencer a outra pessoa, toque no botão correspondente.

- ☐ **Proteger outros dispositivos**

Selecione esta opção e, em seguida, selecione o proprietário do dispositivo. Se o dispositivo pertencer a outra pessoa, toque no botão correspondente.

Clique em **ENVIAR LINK PARA A TRANSFERÊNCIA**. Introduza um endereço de e-mail no campo correspondente, e clique em **ENVIAR E-MAIL**. Saiba que o link gerado para a transferência é válido apenas durante as próximas 24 horas. Se o link expirar, deve gerar um link novo ao seguir os mesmos passos.


No dispositivo em que deseja instalar seu produto Bitdefender, verifique a conta de e-mail que você digitou e toque no botão de download correspondente.




4. Aguarde pela conclusão da transferência, em seguida, execute o instalador:

## Personalize o seu dispositivo

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

1. Acesso [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 **Configurações**.
5. Introduza um nome novo no campo **Nome do dispositivo**, depois clique em **GUARDAR**.

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


1. Acesso [Bitdefender Central](#).
2. Selecione os **Meus dispositivos** painel.
3. Toque no cartão do dispositivo desejado e, em seguida, no  ícone no canto superior direito da tela.
4. Selecione **Perfil**.
5. Clique em **Adicionar proprietário** e, em seguida, preencha os respetivos campos. Personalize o perfil adicionando uma fotografia e selecionando a data de nascimento, além de um e-mail e número de telefone.
6. Clique em **ADICIONAR** para guardar o perfil.
7. Selecione o proprietário desejado na lista **Proprietário do dispositivo** e, em seguida, clique em **ATRIBUIR**.

## Ações remotas

Para atualizar o Bitdefender remotamente no dispositivo:

1. Acesso [Bitdefender Central](#).
2. Selecione os **Meus dispositivos** painel.



3. Toque no cartão do dispositivo desejado e, em seguida, no  ícone no canto superior direito da tela.

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 ver detalhes sobre o dispositivo selecionado, verifique 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 afetando seu dispositivo, amarelo, quando o dispositivo solicitar a sua atenção, ou vermelho, quando o dispositivo estiver em risco. Quando houver problemas a afetar o seu dispositivo, clique na seta suspensa na área de estado superior para saber mais detalhes. Aqui,
- **Proteção.** Nesta janela, pode executar uma Verificação do Sistema ou uma Verificação Rápida dos seus dispositivos remotamente. Clique no botão **VERIFICAR** para iniciar o processo. Também pode conferir quando a última verificação foi realizada no dispositivo e aceder um relatório da última verificação, contém as informações mais importantes.
- **Otimizador.** Aqui pode melhorar remotamente o desempenho de um dispositivo através da digitalização rápida, deteção e limpeza de ficheiros inúteis. Clique no botão **INICIAR** e, em seguida, selecione as áreas que deseja otimizar. Clique novamente no botão **INICIAR** para iniciar o processo de otimização. Clique em **Mais detalhes** para aceder a um relatório detalhado sobre as questões corrigidas.
- **Antifurto.** Em caso de extravio, furto ou perda, com a funcionalidade Antifurto, pode localizar o seu dispositivo e tomar ações remotas. Clique em **LOCALIZAR** para descobrir a localização do dispositivo. A última localização conhecida será exibida, com a hora e a data.
- **Vulnerabilidade.** Para verificar um dispositivo em pesquisa de qualquer vulnerabilidade, como atualizações do Windows ausentes, aplicações desatualizadas ou palavras-passe fracas, clique no botão **VERIFICAR** no separador Vulnerabilidade. Vulnerabilidades não podem ser corrigidas remotamente. Caso qualquer vulnerabilidade seja descoberta, é necessário executar uma verificação nova no dispositivo



e, em seguida, tomar as ações recomendadas. Clique em **Mais detalhes** para aceder a um relatório detalhado sobre os problemas encontrados.



## 2.3.8. Notificações

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

## 2.4. Manter o 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 .
- 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 .

### 2.4.1. Verificar se o Bitdefender está atualizado

Para conferir 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.

## 2.4.2. A efetuar uma atualização

Para realizar actualizações, é necessária uma ligação à Internet.

Para iniciar uma atualização, clique no ícone do Bitdefender  na **bandeja do sistema**, depois 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. Acesso [Bitdefender Central](#).
2. Selecione os **Meus dispositivos** painel.
3. Clique no cartão do dispositivo desejado e, em seguida, no  ícone no canto superior direito da tela.
4. Selecione **Atualizar**.

## 2.4.3. Ligar ou desligar a atualização automática

Para desativar a atualização automática:

1. Clique **Configurações** no menu de navegação do [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.



## Aviso

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

## 2.4.4. Ajuste das configurações da atualização

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

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

Para ajustar as definições de atualização:

1. Clique **Configurações** no menu de navegação do [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 atualização, 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**.

## 2.4.5. Atualizações contínuas

Para garantir que está a utilizar a versão mais recente, o Bitdefender verifica automaticamente a existência de produtos. Estas atualizações podem apresentar novas funcionalidades e melhorias, corrigir problemas de produto ou atualizar automaticamente para uma nova versão. Quando a nova versão de Bitdefender é fornecida por atualização, as definições personalizadas são guardadas e o procedimento de desinstalação e reinstalação é ignorado.

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



### Observação

As atualizações com as novas funcionalidades e melhorias serão proporcionadas apenas aos utilizadores que tenham o Bitdefender 2020 instalado.



## 3. GERIR A SUA SEGURANÇA

### 3.1. Proteção Antivírus

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

- **Análise no acesso** - previne que novas ameaças entrem no seu sistema. Por exemplo, o Bitdefender irá analisar um documento word à procura de ameaças conhecidas quando o abrir, e uma mensagem de email quando recebe uma.

A análise no acesso garante protecção 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 \(página 59\)](#).

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 excepções de análise \(página 61\)](#).

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 desinfetados são movidos para a quarentena de modo a conter a infeção. Para mais informação, dirija-se a [Gerir ficheiros da quarentena \(página 63\)](#).



Se o seu dispositivo estiver infetado com ameaças, consulte [Remover ameaças do seu sistema \(página 101\)](#). 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](#). 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.

## 3.1.1. Análise no acesso (protecção em tempo real)

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

### Ligar ou desligar a protecção em tempo real

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

1. Clique em **Protecção** no menu de navegação na **interface do Bitdefender**.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Avançado**, ative ou desative o **Bitdefender Shield**.
4. Se pretender desativar a protecção 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 protecção em tempo real durante 5, 15 ou 30 minutos, por uma hora, permanentemente ou até ao reinício do sistema. A protecção em tempo real será ativada automaticamente quando o tempo seleccionado expirar.



#### Aviso

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



## 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 **Proteção** no menu de navegação do [Interface do Bitdefender](#).
2. No **ANTIVÍRUS** painel, clique **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 as aplicações.** Pode definir o Bitdefender para verificar apenas as aplicações acedidas.
- **Analise aplicações potencialmente indesejadas.** Selecione esta opção para analisar aplicações indesejadas. Uma aplicação potencialmente indesejada (PUA) ou um programa potencialmente indesejado (PUP) é um software que normalmente vem com software freeware e irá mostrar pop-ups ou instalar uma barra de ferramentas no navegador predefinido. Alguns irão alterar a página inicial ou o motor de pesquisa e outros irão executar vários processos em segundo plano, deixando o seu PC lento, ou irão mostrar numerosos anúncios. Estes programas podem ser instalados sem o seu consentimento (também chamado adware) ou serão incluídos por predefinição no seu kit de instalação expresso (suportado por anúncios).
- **Verificar os scripts.** A função de Verificar Scripts permite que o Bitdefender verifique os scripts de PowerShell e documentos do Office que possam conter malware baseado em scripts.
- **Verificar os partilhas de rede.** Para aceder a uma rede remota com segurança no seu dispositivo, recomendamos que mantenha ativada a opção Verificar partilhas de rede.
- **Verificação da memória de processo.** Verifica atividades maliciosas na memória dos processos em execução.



- **Verificação da linha de comando.** Verifica a linha de comando das aplicações recém-iniciadas para evitar ataques sem ficheiros.
- **Verificar os ficheiros.** A verificação de ficheiros internos é um processo lento e com intensa exigência de recursos. Portanto, não é recomendada para uma proteção em tempo real. Pastas compactadas que contenham ficheiros infetados não constituem uma ameaça imediata à segurança do seu sistema. A ameaça só afetará o seu sistema se o ficheiro infetado for extraído e executado sem que a proteção em tempo real seja 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).
- **Verificar os setores de arranque.** Pode definir o Bitdefender para verificar os setores de arranque do seu disco rígido. Este setor do disco rígido contém o código necessário para começar o processo de arranque. Quando uma ameaça infecta o setor de arranque, a drive pode tornar-se inacessível e não conseguirá iniciar o sistema e aceder aos seus dados.
- **Verificar as apenas os ficheiros novos e modificados.** Ao verificar apenas os ficheiros novos e modificados, pode melhorar significativamente a resposta geral do sistema com um comprometimento mínimo da segurança.
- **Verificação de keyloggers.** Selecione esta opção para verificar o seu sistema à procura de aplicações keyloggers. Os keyloggers registam o que é introduzido no seu teclado e enviam relatórios pela internet a uma pessoa com más intenções (hacker). O hacker pode descobrir informações confidenciais a partir dos dados roubados, tais como números de contas bancárias e palavras-passe, e utilizá-las para benefício próprio.
- **Verificação do arranque antecipada.** Selecione a opção **Verificação do arranque antecipada** para verificar o seu sistema no arranque assim que todos os serviços essenciais tenham sido carregados. A missão desta funcionalidade é melhorar o tempo e a deteção de ameaças no arranque 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 **Proteção** no menu de navegação do [Interface do Bitdefender](#).
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Na janela **Avançado**, rode para baixo até ver a opção **Ações de ameaça**.
4. Configure as definições de análise como necessário.

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

## Tomar medidas adequadas

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

- **Ficheiros infetados.** Os ficheiros detetados como estando infetados correspondem a uma informação de ameaça na Base de Dados de Informações sobre Ameaças do Bitdefender. O Bitdefender irá tentar remover automaticamente o código malicioso do ficheiro infetado e reconstruir o ficheiro original. Esta operação é referida como desinfeção.

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 \(página 63\)](#).



### 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 detetados como sendo suspeitos pela análise heurística. Não é possível desinfetar ficheiros suspeitos porque não há uma rotina de desinfeção disponível. Irão ser colocados em quarentena para evitar uma potencial infeção.

Por predefinição, os ficheiros em quarentena são automaticamente enviados para o Bitdefender Labs para serem analisados pelos investigadores de ameaças do Bitdefender. Se a presença de uma ameaça for confirmada, é divulgada uma atualização de informações de ameaças para permitir a sua remoção.

- **Pastas 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 \(página 63\)](#).

## Negar o acesso

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

## Restaurar as predefinições

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

Para restaurar as definições da protecção em tempo real:

1. Clique **Proteção** no menu de navegação do [Interface do Bitdefender](#).
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Na janela **Avançado**, role para baixo até ver a opção **Restaurar configurações avançadas**. Selecione esta opção para retornar às configurações de fábrica do antivírus.

### 3.1.2. 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.

## Procurar ameaças num ficheiro ou pasta

Deve verificar os ficheiros e as pastas sempre que suspeitar que possam estar infetados. Clique com o botão direito do rato no ficheiro ou pasta que deseja verificar, aponte para o **Bitdefender** e selecione **Verificar com o Bitdefender**. O **Assistente de Verificação** aparecerá e irá guiá-lo através do processo de verificação. Ao final da verificação, será solicitado que escolha as ações a serem tomadas para os ficheiros detetados, se houver algum.

## 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 **Proteção** no menu de navegação da interface do Bitdefender.
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Na janela **Verificações**, clique no botão **Executar verificação** ao lado de **Verificação 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.





## 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.



### Observação

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 [Manter o Bitdefender atualizado \(página 40\)](#).
- 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 \(página 52\)](#).

Para realizar uma análise do sistema:

1. Clique **Proteção** no menu de navegação do [Interface do Bitdefender](#).
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Na janela **Verificações**, clique no botão **Executar verificação** ao lado de **Verificação do sistema**.
4. A primeira vez que executar uma Análise do Sistema, verá uma apresentação da função. Clique em **OK, entendi** para continuar.
5. Segue o [Assistente de verificação antivírus](#) para concluir a digitalização. O Bitdefender executará automaticamente as ações recomendadas nos arquivos detectados. Se houver ameaças não resolvidas, você será solicitado a escolher as ações a serem executadas.



## 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 **Proteção** no menu de navegação do [Interface do Bitdefender](#).
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Nas janelas de **Verificações**, clique em **+Criar verificação**.
4. No campo **Nome da tarefa**, introduza o nome da verificação, a seguir, selecione os locais que deseja verificar, e depois clique em **Próximo**.
5. Configure as seguintes opções gerais:
  - ☐ **Digitalizar apenas aplicativos**. Você pode configurar o Bitdefender para verificar apenas os aplicativos acessados.
  - ☐ **Prioridade da tarefa de verificação**. Pode escolher o impacto que um processo de verificação 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 de pós-verificação**. Escolha a ação que o Bitdefender deve tomar caso não sejam 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 encontrar informações sobre as análises listadas no final desta seção. Clique em **Próximo**.
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.

## Informações sobre as opções de digitalização

Você pode achar esta informação útil:

- ☐ Se não está familiarizado com alguns dos termos, procure-os no **glossário**. Pode também encontrar informação útil pesquisando a Internet.
- ☐ **Examine aplicativos potencialmente indesejados.** Selecione esta opção para procurar aplicativos indesejados. Um aplicativo potencialmente indesejado (PUA) ou programa potencialmente indesejado (PUP) é um software que geralmente vem junto com o software freeware e exibe pop-ups ou instala uma barra de ferramentas no navegador padrão. Alguns deles mudarão a página inicial ou



o mecanismo de pesquisa, outros executarão vários processos em segundo plano, tornando o PC mais lento ou exibirão vários anúncios. Esses programas podem ser instalados sem o seu consentimento (também chamados de adware) ou serão incluídos por padrão no kit de instalação expresso (suportado por anúncios).

- **Verificar os ficheiros.** Pastas compactadas que contenham ficheiros infectados não constituem uma ameaça imediata à segurança do seu sistema. A ameaça só afetará o seu sistema se o ficheiro infectado for extraído e executado sem que a proteção em tempo real seja ativada. Contudo, recomenda-se a utilização desta opção para detetar e remover qualquer ameaça potencial, mesmo que não seja uma ameaça imediata.

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



## Observação

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

- **Examine apenas arquivos novos e modificados.** Ao verificar apenas arquivos novos e modificados, você pode melhorar muito a capacidade de resposta geral do sistema com uma compensação mínima em segurança.
- **Verifique os setores de inicialização.** Você pode configurar o Bitdefender para verificar os setores de inicialização do seu disco rígido. Este setor do disco rígido contém o código de computador necessário para iniciar o processo de inicialização. Quando uma ameaça infecta o setor de inicialização, a unidade pode ficar inacessível e você pode não conseguir iniciar o sistema e acessar seus dados.
- **Analisar memória.** Selecione esta opção para analisar programas em execução na memória do seu sistema.
- **Verificar o registo.** Selecione esta opção para verificar as chaves de registo. O Registo do Windows é um banco de dados que armazena as configurações e opções para os componentes do sistema operacional Windows, bem como para as aplicações instaladas.
- **Verificar os cookies.** Selecione esta opção para verificar os cookies armazenados pelos navegadores do seu dispositivo.



- **Digitalizar keyloggers.** Selecione esta opção para escanear seu sistema em busca de aplicativos keylogger. Os keyloggers registram o que você digita no teclado e enviam relatórios pela internet para uma pessoa maliciosa (hacker). O hacker pode descobrir informações confidenciais dos dados roubados, como números de contas bancárias e senhas, e usá-los para obter benefícios pessoais.

## Assistente de Análise Antivírus

Sempre que iniciar uma verificação a pedido (por exemplo, clique com o botão direito do rato numa pasta, aponte para o Bitdefender e selecione **Verificar com o Bitdefender**), o Assistente de Verificação aparecerá. Siga o assistente para concluir o processo de verificação.



### Observação

Se o assistente de análise não surgir, a análise pode ser configurada para ser executada de forma silenciosa, em segundo plano. Procure o ícone de progresso de análise **B** na **bandeja do sistema**. Pode clicar neste ícone para abrir a janela de análise e para ver o progresso da análise.

## Passo 1 - Realizar Análise

BitDefender iniciará a análise dos objectos seleccionados. 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 colocar em pausar a verificação.** Pode parar a verificação sempre que quiser ao clicar em **PARAR**. Será direcionado ao último passo do assistente. Para parar temporariamente o processo de verificação, basta clicar em **PAUSA**. Terá que clicar em **RETOMAR** para retomar a verificação.

**Ficheiros protegidos por palavra-passe.** Quando um ficheiro protegido por palavra-passe é detetado, dependendo das definições de verificação, pode ser preciso fornecer a palavra-passe. Os ficheiros protegidos por palavra-passe não podem ser verificados, a menos que a mesma seja fornecida. As seguintes opções estão disponíveis:



- **Palavra-passe.** Se quiser que o Bitdefender verifique o ficheiro, selecione esta opção e escreva a palavra-passe. Se não souber a palavra-passe, escolha uma das outras opções.
- **Não peça uma palavra-passe e ignore este objeto na verificação.** Selecione esta opção para ignorar a verificação deste ficheiro.
- **Ignorar todos os itens protegidos por palavra -passe sem verificá-los.** Selecione esta opção se não quiser ser incomodado com ficheiros protegidos por palavra-passe. O Bitdefender não poderá verificá-los, mas um relatório será mantido no registo de verificação.

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.



### Observação

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 as medidas adequadas

O Bitdefender tomará as ações recomendadas dependendo do tipo de arquivo detectado:

- **Arquivos infectados.** Os arquivos detectados como infectados correspondem a uma informação sobre ameaças encontrada no Banco de Dados de Informações sobre Ameaças do Bitdefender. O Bitdefender tentará automaticamente remover o código malicioso do arquivo infectado e reconstruir o arquivo original. Esta operação é referida como desinfecção.



Os arquivos que não podem ser desinfetados são movidos para a quarentena para conter a infecção. Arquivos em quarentena não podem ser executados ou abertos; portanto, o risco de infecção desaparece. Para mais informações, consulte [Gerir ficheiros da quarentena \(página 63\)](#).



## Importante

Para determinados tipos de ameaças, a desinfecção não é possível porque o arquivo detectado é totalmente malicioso. Nesses casos, o arquivo infectado é excluído do disco.

- **Arquivos suspeitos.** Os arquivos são detectados como suspeitos pela análise heurística. Arquivos suspeitos não podem ser desinfetados porque nenhuma rotina de desinfecção está disponível. Eles serão transferidos para a quarentena para evitar uma possível infecção. Por padrão, os ficheiros em quarentena são automaticamente enviados ao Bitdefender Labs 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.
- **Arquivos contendo arquivos infectados.**
  - Os arquivos que contêm apenas arquivos infectados são excluídos automaticamente.
  - Se um arquivo contém arquivos infectados e limpos, o Bitdefender tentará excluir os arquivos infectados desde que possa reconstruir o arquivo com os arquivos limpos. Se a reconstrução do arquivo não for possível, você será informado de que nenhuma ação pode ser tomada para evitar a perda de arquivos limpos.

## Excluir

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 medidas



Nenhuma acção será levada a cabo sobre os ficheiros detectados. Após a análise terminar, pode abrir o relatório da análise para ver informação sobre 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-á 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 \(página 101\)](#).

## 3.1.3. 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 **Notificações** no menu de navegação do [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**.

## 3.1.4. 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.

## 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 progresso da verificação do Bitdefender  aparecerá na **bandeja do sistema**. Pode clicar neste ícone para abrir a janela de verificação e para ver o progresso da verificação.

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.



## Observação

Tenha em conta que nenhuma ação pode ser efetuada nos ficheiros que estiverem infetados ou suspeitos detetados em CDs / DVDs. Do mesmo modo, nenhuma ação pode ser tomada nos ficheiros infetados ou suspeitos detetados em unidades de rede mapeada se não tiver 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 \(página 101\)](#).

## Gerir análise de média removível

Para gerir a verificação automática de dispositivos multimédia amovíveis:

1. Clique **Proteção** no menu de navegação do [Interface do Bitdefender](#).
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Selecione a janela **Definições**.

As opções de análise estão pré-configuradas para obter os melhores resultados de deteção. Se forem detetados 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.



### 3.1.5. 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 exceções 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.



#### Observação

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 selecciona **Analisar com BitDefender**.

### Excluindo ficheiros e pastas da análise

Para excluir ficheiros e pastas específicas da análise:

1. Clique **Proteção** no menu de navegação do [Interface do Bitdefender](#).
2. No **ANTIVÍRUS** painel, clique **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, seleccioná-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.



## Exceto extensões de ficheiros de verificação

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 **Proteção** no menu de navegação do [Interface do Bitdefender](#).
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. No **Configurações** janela, clique **Gerenciar exceções**.
4. Clique **+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**.

## 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 **Proteção** no menu de navegação do [Interface do Bitdefender](#).
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Na janela de **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 um dado da lista, clique no botão  próximo a ele.



- 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**.

## 3.1.6. Gerir ficheiros da quarentena

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

Por padrão, os arquivos em quarentena são enviados automaticamente para o Bitdefender Labs para serem analisados pelos pesquisadores de ameaças da Bitdefender. Se a presença de uma ameaça for confirmada, uma atualização de informações é lançada para permitir a remoção da ameaça.

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 **Proteção** no menu de navegação do [Interface do Bitdefender](#).
2. No **ANTIVÍRUS** painel, clique **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**.

## 3.2. Defesa Avançada contra Ameaças

A Defesa Avançada contra as Ameaças do Bitdefender é uma tecnologia de deteção inovadora e proativa 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 ações 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.

### 3.2.1. Ativar ou desativar o Advanced Threat Defense

Para ativar ou desativar o Advanced Threat Defense:

1. Clique **Proteção** no menu de navegação do [Interface do Bitdefender](#).
2. No painel **DEFESA AVANÇADA CONTRA AMEAÇAS**, clique em **Abrir**.
3. Vá à janela **Definições** e clique no botão ao lado de **Defesa Avançada contra Ameaças do Bitdefender**.



#### **Observação**

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



## 3.2.2. 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 **Proteção** no menu de navegação do [Interface do Bitdefender](#).
2. No **DEFESA AVANÇADA DE AMEAÇA** painel, clique **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 desinfecção foi bem-sucedida, basta clicar neste.

## 3.2.3. 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 **Proteção** no menu de navegação do [Interface do Bitdefender](#).
2. No **DEFESA AVANÇADA DE AMEAÇA** painel, clique **Abrir**.
3. No **Configurações** janela, clique **Gerenciar exceções**.
4. Clique **+Adicionar uma exceção**.
5. Insira o caminho da pasta que deseja excluir da digitalização 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 **Salvar**.

## 3.2.4. 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.

## 3.2.5. Ativar ou desativar a detecção de exploits

Para ativar ou desativar a detecção de exploits:

- Clique **Proteção** no menu de navegação do [Interface do Bitdefender](#).
- No **DEFESA AVANÇADA DE AMEAÇA** painel, clique **Abrir**.
- Vá à janela de **Definições** e clique no botão ao lado de **Deteção de exploits** para ativar ou desativar a função.



### Observação

A opção de Deteção de exploits está ativa por predefinição.

## 3.3. Prevenção de ameaças on-line

A Prevenção contra Ameaças Online do Bitdefender garante uma navegação segura ao alertá-lo sobre as páginas da 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 **Proteção** no menu de navegação do [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 ícone ao lado de cada resultado:

 Não deve visitar esta página da web.

 Esta página web pode conter conteúdo perigoso. Tenha cuidado se decidir visitá-lo.

 Esta é uma página segura de visitar.

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 **Proteção** no menu de navegação do [Interface do Bitdefender](#).
  2. No **PREVENÇÃO DE AMEAÇAS ONLINE** painel, clique **Configurações**.
  3. Clique em **Gerir exceções**.
  4. Clique **+Adicionar uma exceção**.
  5. No campo correspondente, escreva o nome do site, do domínio ou do endereço IP que deseja adicionar às exceções.
  6. Clique no botão ao lado de **Prevenção de Ameaças Online**.
  7. Para remover uma entrada da lista, clique no botão  botão ao lado dele.
- Clique **Salvar** para salvar as alterações e fechar a janela.

### 3.3.1. Alertas do 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.



## 4. COMO

### 4.1. Instalação

#### 4.1.1. Como instalo 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**.  
Uma nova janela aparece em sua tela.
2. Clique **COMPARTILHAR LINK DE DOWNLOAD**.
3. Siga as instruções no ecrã para instalar o Bitdefender.

O novo dispositivo no qual instalou o produto Bitdefender aparece no painel do Bitdefender Central.

#### 4.1.2. Como posso reinstalar o 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.

Na eventualidade de uma das situações mencionadas ser o seu caso, siga estes passos:

- ☐ Em **windows 7**:
  1. Clique **Começar** e vai para **Todos os programas**.
  2. Localize Bitdefender Antivirus Free e selecione **Desinstalar**.
  3. Clique em **REINSTALAR** na janela que aparece.
  4. Precisa de reiniciar o dispositivo para concluir o processo.
- ☐ Em **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. Encontrar **Bitdefender Antivirus Free** e selecione **Desinstalar**.
  4. Clique **REINSTALAR** na janela que aparece.
  5. Você precisa reiniciar o dispositivo para concluir o processo.
- Em **Windows 10** e **Windows 11**:
1. Clique em **Iniciar** e, em seguida, clique em **Definições**.
  2. Clique no ícone **Sistema** na área de Definições e então selecione **Aplicações e funcionalidades**.
  3. Encontrar **Bitdefender Antivirus Free** e selecione **Desinstalar**.
  4. Clique em **Desinstalar** novamente para confirmar a sua escolha.
  5. Clique em **REINSTALAR**.
  6. Você precisa reiniciar o dispositivo para concluir o processo.



### Observação

Após 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.

## 4.1.3. De onde é que 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.



### Observação

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 a partir da Central Bitdefender:



1. Acesso [Bitdefender Central](#).
2. Selecione os **Meus dispositivos** painel e, em seguida, clique em **INSTALAR PROTEÇÃO**.
3. Escolha uma das duas opções disponíveis:
  - **Proteger este dispositivo**  
Selecione esta opção e, em seguida, selecione o proprietário do dispositivo. Se o dispositivo pertencer a outra pessoa, clique no botão correspondente.
  - **Proteger outros dispositivos**  
Selecione esta opção e, em seguida, selecione o proprietário do dispositivo. Se o dispositivo pertencer a outra pessoa, clique no botão correspondente.  
Clique **ENVIAR LINK DE DOWNLOAD**. Digite um endereço de e-mail no campo correspondente e clique em **ENVIAR EMAIL**. Observe que o link de download gerado é válido apenas pelas próximas 24 horas. Se o link expirar, você terá que gerar um novo seguindo os mesmos passos.  
No dispositivo em que deseja instalar seu produto Bitdefender, verifique a conta de e-mail que você digitou e clique no botão de download correspondente.
4. Execute o Bitdefender que transferiu.

## 4.1.4. Como posso atualizar o Bitdefender para a versão mais recente?

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 desejam atualizar gratuitamente da versão 2016 ou inferior para a versão mais recente do Bitdefender, devem remover a sua versão atual no Painel de Controlo, e depois transferir o ficheiro de instalação mais recente do site do Bitdefender no seguinte endereço: <https://www.bitdefender.com/Downloads/>. A ativação é possível apenas com uma subscrição válida

## 4.2. Bitdefender Central

### 4.2.1. Como faço para aceder o Bitdefender com outra conta?

Criou uma nova conta Bitdefender e deseja utilizá-la a partir de agora.

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. Digite o endereço de e-mail no campo correspondente e clique em **PRÓXIMO**.
4. Digite sua senha e clique em **ENTRAR**.



#### Observação

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 o Bitdefender para obter suporte, como descrito na secção [Pedir Ajuda \(página 108\)](#).



## 4.2.2. Como desligar as mensagens de ajuda da Central Bitdefender?

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. Acesso [Bitdefender Central](#).
2. Clique no ⓘ ícone no canto superior direito da tela.
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**.

## 4.2.3. 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:

○ De [Interface do Bitdefender](#):

1. Clique **Minha conta** no menu de navegação do [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**. Uma nova janela aparece.
4. Clique **Esqueceu sua senha?**.
5. Clique em **PRÓXIMO**.
6. Verifique sua conta de e-mail, digite o código de segurança que você recebeu e clique em **PRÓXIMO**. Alternativamente, você pode clicar **Alterar a senha** no e-mail que lhe enviamos.
7. Digite a nova senha que deseja definir e digite-a novamente. Clique **SALVAR**.

○ No seu navegador da Web:




1. Vá para: <https://central.bitdefender.com>.
2. Clique em **ENTRAR**.
3. Digite seu endereço de e-mail e clique em **PRÓXIMO**.
4. Clique **Esqueceu sua senha?**.
5. Clique **PRÓXIMO**.
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.

## 4.2.4. 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. Acesso [Bitdefender Central](#).
2. Clique no  ícone no canto superior direito da tela.
3. Clique em **Sessões** no menu deslizante.
4. Na área de **Sessões ativas**, selecione a opção **SAIR** próxima ao dispositivo em que deseja encerrar sessão.

## 4.3. A analisar com BitDefender

### 4.3.1. Como posso analisar um ficheiro ou uma pasta?

A forma mais fácil para verificar um ficheiro ou pasta é clicando com o botão direito no objeto que deseja verificar, apontar para o Bitdefender e selecionar no menu **Verificar com o Bitdefender**.

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.

## 4.3.2. Como posso analisar o seu sistema


Para realizar uma análise completa no sistema:

1. Clique **Proteção** no menu de navegação do [Interface do Bitdefender](#).
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Clique no botão **Executar verificação** ao lado de **Verificação 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 .

## 4.3.3. 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 **Proteção** no menu de navegação do [Interface do Bitdefender](#).
2. No **ANTIVÍRUS** painel, clique **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**.  
Também pode criar um tipo de verificação que atenda às suas necessidades clicando em **+Criar verificação** ao lado de **Gerir verificações**.



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:

- ☐ Na inicialização do sistema
- ☐ Diário
- ☐ Semanalmente
- ☐ Por mês

Se você escolher Diariamente, Mensalmente ou Semanalmente, arraste o controle deslizante ao longo da escala para definir o período de tempo desejado quando a verificação agendada deve começar.

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

## 4.3.4. 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 **ANTIVÍRUS** painel, clique **Abrir**.
2. Clique em **+Criar verificação** ao lado de **Gerir verificações**.
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 estas opções gerais:
  - ☐ **Verificar apenas aplicações**. Pode configurar o Bitdefender para verificar apenas aplicações acedidas.
  - ☐ **Verificar prioridade de tarefas**. Pode escolher o impacto que o processo de verificação tem no desempenho do seu sistema.
    - ☐ Auto - A prioridade do processo de verificação dependerá da atividade do sistema. Para garantir que o processo de verificação não afetará a atividade do sistema, o Bitdefender



decidirá se o processo de verificação deve ser executado com alta ou baixa prioridade.

- ☐ Alta - A prioridade do processo de verificação será alta. Ao escolher esta opção, você permitirá que outros programas sejam executados mais lentamente e diminuirá o tempo necessário para que o processo de verificação seja concluído.
  - ☐ Baixa - A prioridade do processo de verificação será baixa. Ao escolher esta opção, você permitirá que outros programas sejam executados mais rapidamente e aumentará o tempo necessário para a conclusão do processo de verificação.
  - ☐ **Medidas pós-verificação.** Escolha a ação que o Bitdefender deve realizar se não forem encontradas ameaças:
    - ☐ Mostrar janela de resumo
    - ☐ Dispositivo de desligamento
    - ☐ Fechar janela de digitalização
5. Se deseja configurar as opções de análise detalhadamente, clique em **Mostrar opções avançadas**.  
Clique **Próximo**.
6. Pode ativar a opção **Programar tarefa de análise** e, se quiser, escolha quando a análise personalizada que criou deve começar.
- ☐ Na inicialização do sistema
  - ☐ Diário
  - ☐ Por mês
  - ☐ Semanalmente
- Se você escolher Diariamente, Mensalmente ou Semanalmente, arraste o controle deslizante ao longo da escala para definir o período de tempo desejado quando a verificação agendada deve começar.
7. Clique **Salvar** para salvar as configurações e fechar a janela de configuração.
- Dependendo dos locais a serem verificados, a verificação pode demorar um pouco. Se forem encontradas ameaças durante o



processo de verificação, você será solicitado a escolher as ações a serem executadas nos arquivos detectados.

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

## 4.3.5. 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 **Proteção** no menu de navegação do [Interface do Bitdefender](#).
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Clique na aba **Definições**.
4. Clique em **Gerir exceções**.
5. Clique **+Adicionar uma exceção**.
6. Insira o caminho da pasta que deseja excluir da digitalização no campo correspondente.  
Como alternativa, você pode navegar até a pasta clicando no botão Procurar no lado direito da interface, selecioná-la e clicar em **OK**.
7. Ligue o interruptor ao lado do recurso de proteção que não deve verificar a pasta. Existem três opções:
  - ☐ antivírus
  - ☐ Prevenção de ameaças on-line
  - ☐ Defesa Avançada contra Ameaças



8. Clique **Salvar** para salvar as alterações e fechar a janela.

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

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

1. Desative a proteção antivírus em tempo real do Bitdefender:
  - a. Clique **Proteção** no menu de navegação do [Interface do Bitdefender](#).
  - b. No **ANTIVÍRUS** painel, clique **Abrir**.
  - c. Na janela **Avançado**, desative o **Bitdefender Shield**.  
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 ficheiros ocultos no Windows. Para saber mais sobre como fazer isto, aceda a [Como posso mostrar objetos ocultos no Windows? \(página 85\)](#).
3. Restaurar o ficheiro da área de Quarentena:
  - a. Clique **Proteção** no menu de navegação do [Interface do Bitdefender](#).
  - b. No **ANTIVÍRUS** painel, clique **Abrir**.
  - c. Vá para a janela **Definições** e clique em **Gerir a quarentena**.
  - d. Selecione o ficheiro e, em seguida, clique em **Restaurar**.
4. Adicione o ficheiro à Lista de exceções. Para saber mais sobre como fazer isso, aceda [Como excluir uma pasta da análise? \(página 78\)](#).
5. Ligue a proteção antivírus em tempo real do Bitdefender.
6. Entre em contacto com os nossos representantes do apoio para que possamos remover a deteção da atualização da informação de



ameaça. Para saber mais sobre como fazer isto, acesse a [Pedir Ajuda \(página 108\)](#).

## 4.3.7. 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.

Você pode abrir o log de verificação diretamente do assistente de verificação, uma vez que a verificação for concluída, clicando em **MOSTRAR LOG**.

Para verificar um log de verificação ou qualquer infecção detectada posteriormente:

1. Clique **Notificações** no menu de navegação do [Interface do Bitdefender](#).
2. No **Todos** guia, selecione a notificação sobre a verificação mais recente.  
É aqui que você pode encontrar todos os eventos de varredura de ameaças, incluindo ameaças detectadas por varredura no acesso, varreduras iniciadas pelo usuário e alterações de status para varreduras automáticas.
3. Na lista de notificações, você pode verificar quais verificações foram realizadas recentemente. Clique em uma notificação para ver os detalhes sobre ela.
4. Para abrir um relatório da análise, clique em **Ver Relatório**.

## 4.4. Informações Úteis

### 4.4.1. 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 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 \(página 108\)](#).

## 4.4.2. Como removo o Bitdefender?

Se deseja remover o seu Bitdefender Antivirus Free:

### ○ Em **windows 7**:

1. Clique **Começar**, Vá para **Painel de controle** e clique duas vezes **Programas e características**.
2. Encontrar **Bitdefender Antivirus Free** e seleccione **Desinstalar**.
3. Clique em **REMOVER** na janela que aparece.
4. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.

### ○ Em **Windows 8 e Windows 8.1**:

1. Na tela Iniciar do Windows, localize **Painel de controle** (por exemplo, você pode começar a digitar "Painel de controle" diretamente na tela Iniciar) e clicar em seu ícone.
2. Clique **Desinstalar um programa** ou **Programas e características**.



3. Encontrar **Bitdefender Antivirus Free** e selecione **Desinstalar**.
  4. Clique **REMOVER** na janela que aparece.
  5. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.
- Em **Windows 10** e **Windows 11**:
1. Clique em **Iniciar**, em seguida, clique em Definições.
  2. Clique no **Sistema** ícone na área Configurações e selecione **aplicativos**.
  3. Encontrar **Bitdefender Antivirus Free** e selecione **Desinstalar**.
  4. Clique **Desinstalar** novamente para confirmar sua escolha.
  5. Clique **REMOVER** na janela que aparece.
  6. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.



### Observação

Este procedimento de reinstalação irá eliminar permanentemente as definições personalizadas.

## 4.4.3. 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 **Proteção** no menu de navegação do [Interface do Bitdefender](#).





2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Na janela **Análises**, clique em "...", ao lado da Análise Rápida ou Análise do Sistema, e 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.  
Se você escolher Diariamente, Mensalmente ou Semanalmente, arraste o controle deslizante ao longo da escala para definir o período de tempo desejado quando a verificação agendada deve começar.
6. Clique **Salvar**.

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 ser iniciada.
4. Clique **Salvar**.

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

Se ainda houver ameaças não resolvidas, será solicitado que escolha as ações a tomar perante as mesmas. Para mais informação, dirija-se a [Assistente de Análise Antivírus \(página 55\)](#).

## 4.4.4. Como posso configurar o Bitdefender para utilizar uma ligação à internet com proxy?

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 **Configurações** no menu de navegação do [Interface do Bitdefender](#).
2. Selecione os **Avançado** aba.
3. Ative o **Servidor proxy**.
4. Clique em **Alteração 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 atual, extraídas do explorador por defeito. Se o servidor proxy requer um nome de utilizador e uma palavra-passe, deverá inseri-los nos campos correspondentes.



## Observação

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** - introduza a porta que o Bitdefender utiliza para estabelecer ligação ao servidor proxy.
- **Nome de usuário** - introduza um nome de utilizador reconhecido pelo proxy.
- **Palavra-passe** - introduza a palavra-passe válida do utilizador previamente especificado.

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.



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

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

○ Em **windows 7**:

1. Clique em **Iniciar**.
2. Localize **Computador** no menu **Iniciar**.
3. Clique com o botão direito do rato 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.

○ Em **Windows 10 e Windows 11**:

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.

### 4.4.6. 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**, vá para o **Painel de Controlo**.

No **Windows 8** e no **Windows 8.1**: No ecrã inicial do Windows, localize o **Painel de Controlo** (por exemplo, pode começar a introduzir "Painel de Controlo" diretamente no ecrã inicial) e depois clique no ícone.



2. Selecione **Opções de pasta**.
3. Acesse ao separador **Visualizar**.
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** e, em seguida, clique em **OK**.

Em **Windows 10** e **Windows 11**:

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 de ficheiros conhecidos**.
4. Desmarque **Ocultar arquivos protegidos do sistema operacional**.
5. Clique **Aplicar**, então clique **OK**.

## 4.4.7. 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 Free detecta 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:

### ○ Em **windows 7**:

1. Clique **Começar**, vá para **Painel de controle** e clique duas vezes **Programas e características**.
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 a conclusão do processo de desinstalação e reinicie o sistema.
- Em **Windows 8 e Windows 8.1**:
1. Na tela Iniciar do Windows, localize **Painel de controle** (por exemplo, você pode começar a digitar "Painel de controle" diretamente na tela Iniciar) e clicar em seu ícone.
  2. Clique **Desinstalar um programa** ou **Programas e características**.
  3. Aguarde alguns instantes até que a lista de softwares instalados seja exibida.
  4. Encontre o nome do programa que deseja remover e selecione **Desinstalar**.
  5. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.
- Em **Windows 10 e Windows 11**:
1. Clique **Começar** clique em Configurações.
  2. Clique no **Sistema** ícone na área Configurações e selecione **aplicativos**.
  3. Encontre o nome do programa que deseja remover e selecione **Desinstalar**.
  4. Clique **Desinstalar** novamente para confirmar sua escolha.
  5. Aguarde a 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.

## 4.4.8. 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:

○ Em **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 de Segurança** no menu de arranque ou **Modo de segurança 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 confirmar.
6. Para iniciar o Windows normalmente, basta reiniciar o sistema.

○ No **Windows 8, Windows 8.1, Windows 10 e Windows 11**:

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** e, em seguida, clique em **OK**.
3. Selecione o separador **Arranque**.
4. Na área **Opções de arranque** selecione a caixa **Arranque seguro**.
5. Clique em **Rede** e, em seguida, clique em **OK**.
6. Clique em **OK** na janela **Configuração do Sistema** que informa que o sistema tem de ser reiniciado para poder implementar as alterações que definiu.

O seu sistema será reiniciado no Modo Seguro com rede.

Para arrancar novamente no modo normal, reverta as definições executando novamente a **Operação do Sistema** e desmarcando a caixa de verificação **Arranque seguro**. Clique em **OK** e, em seguida, em **Reiniciar**. Aguarde até que as novas definições sejam aplicadas.



## 5. SOLUÇÃO DE PROBLEMAS

### 5.1. Resolver incidências comuns

Este capítulo apresenta alguns dos problemas que poderão surgir enquanto utiliza o BitDefender, e providencia possíveis soluções. A maioria destes problemas podem ser resolvidos através da configuração adequada das definições do produto.

- [O meu sistema parece estar lento \(página 89\)](#)
- [A análise não inicia \(página 91\)](#)
- [Já não posso utilizar uma aplicação \(página 93\)](#)
- [O que fazer quando o Bitdefender bloqueia um site, domínio, endereço IP ou aplicação online que é seguro \(página 94\)](#)
- [Como atualizar o Bitdefender numa ligação à Internet lenta \(página 95\)](#)
- [Os serviços do Bitdefender não estão a responder \(página 96\)](#)
- [O filtro Antispam não está a funcionar corretamente](#)
- [A remoção Bitdefender falhou \(página 96\)](#)
- [O meu sistema não reinicia após a instalação de Bitdefender \(página 98\)](#)

Se não conseguir encontrar o seu problema aqui, ou se as soluções apresentadas não resolvem o seu problema, pode contactar os representantes do suporte técnico da BitDefender como está representado no capítulo [Pedir Ajuda \(página 108\)](#).

#### 5.1.1. O meu sistema parece estar lento

Normalmente, após a instalação de um software de segurança, o sistema poderá abrandar ligeiramente, o que é, até um certo nível, normal.

Se notar um abrandamento significativo, este problema pode dever-se às seguintes razões:

- **O Bitdefender não é o único programa de segurança instalado 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? \(página 86\)](#).

○ **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 \(página 4\)](#).

○ **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

Se suspeitar que um programa ou uma aplicação é uma parte essencial do seu sistema operativo, não o remova e contacte o Serviço de Apoio ao Cliente da Bitdefender para obter assistência.

○ **O seu sistema pode estar infetado.**

A velocidade do seu sistema e do seu comportamento geral também podem ser afetados por ameaças. Spyware, malware, trojans e adware, todos afetam o desempenho do seu dispositivo. Certifique-se de verificar o seu sistema periodicamente, ao menos uma vez por semana. É recomendado utilizar a Verificação de Sistema da Bitdefender porque ela verifica todos os tipos de ameaça que colocam em risco a segurança do seu sistema.

Para iniciar a Verificação do Sistema:

1. Clique **Proteção** no menu de navegação do [Interface do Bitdefender](#).
2. No **ANTIVÍRUS** painel, clique **Abrir**.
3. Na janela **Análises**, clique em **Executar análise** ao lado de **Análise do sistema**.
4. Siga os passos do assistente.





## 5.1.2. A análise não inicia

Este tipo de problema pode ter duas causas principais:

- Uma instalação anterior do Bitdefender que não foi totalmente removida ou uma instalação do Bitdefender mal sucedida.

Neste caso, reinstale o Bitdefender:

- Em **windows 7**:

1. Clique **Começar**, Vá para **Painel de controle** e clique duas vezes **Programas e características**.
2. Encontrar **Bitdefender Antivirus Free** e selecione **Desinstalar**.
3. Clique **REINSTALAR** na janela que aparece.
4. Aguarde pela conclusão do processo de reinstalação e reinicie o sistema.

- Em **Windows 8 e Windows 8.1**:

1. Na tela Iniciar do Windows, localize **Painel de controle** (por exemplo, você pode começar a digitar "Painel de controle" diretamente na tela Iniciar) e clicar em seu ícone.
2. Clique **Desinstalar** um programa ou **Programas e características**.
3. Encontrar **Bitdefender Antivirus Free** e selecione **Desinstalar**.
4. Clique **REINSTALAR** na janela que aparece.
5. Aguarde a conclusão do processo de reinstalação e reinicie o sistema.

- Em **Windows 10 e Windows 11**:

1. Clique **Começar**, então clique **Configurações**.
2. Clique no **Sistema** ícone na área Configurações e selecione **Aplicativos instalados**.
3. Encontrar **Bitdefender Antivirus Free** e selecione **Desinstalar**.
4. Clique **Desinstalar** novamente para confirmar sua escolha.
5. Clique **REINSTALAR** na janela que aparece.



6. Aguarde a conclusão do processo de reinstalação e reinicie o sistema.



## Observação

Ao seguir este procedimento de reinstalação, as configurações personalizadas são salvas e disponibilizadas no novo produto instalado. Outras configurações podem ser alteradas de volta para sua configuração padrão.

### ○ 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? \(página 86\)](#).

2. Reinstale o Bitdefender:

#### ○ Em **windows 7**:

- a. Clique **Começar**, Vá para **Painel de controle** e clique duas vezes **Programas e características**.
- b. Encontrar **Bitdefender Antivirus Free** e selecione **Desinstalar**.
- c. Clique **REINSTALAR** na janela que aparece.
- d. Aguarde a conclusão do processo de reinstalação e reinicie o sistema.

#### ○ Em **Windows 8 e Windows 8.1**:

- a. Na tela Iniciar do Windows, localize **Painel de controle** (por exemplo, você pode começar a digitar "Painel de controle" diretamente na tela Iniciar) e clicar em seu ícone.
- b. Clique **Desinstalar** um programa ou **Programas e características**.
- c. Encontrar **Bitdefender Antivirus Free** e selecione **Desinstalar**.
- d. Clique **REINSTALAR** na janela que aparece.



- e. Aguarde a conclusão do processo de reinstalação e reinicie o sistema.
- Em **Windows 10** e **Windows 11**:
  - a. Clique **Começar**, então clique **Configurações**.
  - b. Clique no **Sistema** ícone na área Configurações e selecione **Aplicativos instalados**.
  - c. Encontrar **Bitdefender Antivirus Free** e selecione **Desinstalar**.
  - d. Clique **Desinstalar** novamente para confirmar sua escolha.
  - e. Clique em **REINSTALAR** na janela que aparece
  - f. Aguarde a conclusão do processo de reinstalação e reinicie o sistema.



### Observação

Ao seguir este procedimento de reinstalação, as configurações personalizadas são salvas e disponibilizadas no novo produto instalado. Outras configurações podem ser alteradas de volta para sua configuração padrão.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na secção [Pedir Ajuda \(página 108\)](#).

## 5.1.3. Já não posso utilizar uma aplicação

Este problema ocorre quando está a tentar utilizar um programa que estava a funcionar normalmente antes de instalar o Bitdefender.

Após instalar o Bitdefender pode deparar-se com uma das seguintes situações:

- Poderá receber uma mensagem do Bitdefender a informar que o programa está a tentar modificar o sistema.
- Pode receber uma mensagem de erro do programa que está a tentar utilizar.

Este tipo de situação ocorre quando o Advanced Threat Defense deteta erradamente algumas aplicações como maliciosas.

Advanced Threat Defense é uma funcionalidade do Bitdefender que monitoriza constantemente as aplicações executadas no seu sistema



e comunica o comportamento potencialmente malicioso. Como esta funcionalidade se baseia num sistema heurístico, pode haver casos em que as aplicações legítimas são comunicadas pelo Advanced Threat Defense.

Quando 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 **Proteção** no menu de navegação do [Interface do Bitdefender](#).
2. No **DEFESA AVANÇADA DE AMEAÇA** painel, clique **Abrir**.
3. No **Configurações** janela, clique **Gerenciar exceções**.
4. Clique **+Adicionar uma exceção**.
5. Introduza o caminho do executável que deseja adicionar à lista de exceção da verificação no campo correspondente.  
Como alternativa, você pode navegar até o executável clicando no botão de navegação no lado direito da interface, selecione-o e clique em **OK**.
6. Ligue o interruptor ao lado de **Defesa Avançada contra Ameaças**.
7. Clique **Salvar**.

Se esta informação não for útil, você pode entrar em contato com a Bitdefender para obter suporte conforme descrito na seção [Pedir Ajuda \(página 108\)](#).

## 5.1.4. O que fazer quando o Bitdefender bloqueia um site, domínio, endereço IP ou aplicação online que é seguro

O Bitdefender oferece uma experiência de navegação segura na web, ao filtrar todo o tráfego da web e ao bloquear qualquer conteúdo malicioso. No entanto, é possível que o Bitdefender considere um site, domínio, endereço IP ou uma aplicação online seguro como inseguro, o que poderá fazer com que a verificação de tráfego HTTP do Bitdefender o 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 **Proteção** no menu de navegação do [Interface do Bitdefender](#).
2. No **PREVENÇÃO DE AMEAÇAS ONLINE** painel, clique **Configurações**.
3. Clique **Gerenciar exceções**.
4. Clique **+Adicionar uma exceção**.
5. Digite no campo correspondente o nome do site, o nome do domínio ou o endereço IP que deseja adicionar às exceções.
6. Clique no botão ao lado de **Prevenção de ameaças on-line**.
7. Clique **Salvar** para salvar 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 for útil, você pode entrar em contato com a Bitdefender para obter suporte conforme descrito na seção [Pedir Ajuda \(página 108\)](#).

## 5.1.5. 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 **Configurações** no menu de navegação do [Interface do Bitdefender](#).
2. Selecione os **Atualizar** aba.
3. Desligar o botão **Atualização silenciosa**.
4. A próxima vez que uma atualização estiver disponível, será pedido para selecionar a atualização que deseja transferir. Selecionar apenas **Atualização das subscrições**.
5. O Bitdefender transfere e instala apenas a base de dados de informações de ameaças.



## 5.1.6. Os serviços do 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 do Bitdefender na **bandeja do sistema** está em cinzento e informa que os serviços do Bitdefender não estão a responder.
- A janela do BitDefender indica que os serviços do BitDefender não estão a responder.

O erro pode ter ocorrido devido a um dos seguintes 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? \(página 86\)](#).

Se o erro persistir, por favor contacte os nossos representantes do suporte conforme descrito na secção [Pedir Ajuda \(página 108\)](#).

## 5.1.7. A remoção 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:

○ Em **windows 7**:

1. Clique **Começar**, Vá para **Painel de controle** e clique duas vezes **Programas e características**.
2. Encontrar **Bitdefender Antivirus Free** e selecione **Desinstalar**.
3. Clique **REMOVER** na janela que aparece.
4. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.

○ Em **Windows 8 e Windows 8.1**:

1. Na tela Iniciar do Windows, localize **Painel de controle** (por exemplo, você pode começar a digitar "Painel de controle" diretamente na tela Iniciar) e clicar em seu ícone.
2. Clique **Desinstalar um programa** ou **Programas e características**.
3. Encontrar **Bitdefender Antivirus Free** e selecione **Desinstalar**.
4. Clique **REMOVER** na janela que aparece.
5. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.

○ Em **Windows 10 e Windows 11**:

1. Clique **Começar** clique em Configurações.
2. Clique no **Sistema** ícone na área Configurações e selecione **Aplicativos instalados**.
3. Encontrar **Bitdefender Antivirus Free** e selecione **Desinstalar**.
4. Clique **Desinstalar** novamente para confirmar sua escolha.
5. Clique **REMOVER** na janela que aparece.
6. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.



## 5.1.8. 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:

### ○ **Tinha o Bitdefender e não o removeu corretamente.**

Para resolver isto:

1. Reinicie o seu sistema e entre no Modo de Segurança. Para saber mais sobre como fazer isto, aceda a [Como posso reiniciar no Modo de Segurança? \(página 87\)](#).
2. Remova o Bitdefender do seu sistema:

#### ○ Em **windows 7**:

- a. Clique **Começar**, Vá para **Painel de controle** e clique duas vezes **Programas e características**.
- b. Encontrar **Bitdefender Antivirus Free** e seleccione **Desinstalar**.
- c. Clique **REMOVER** na janela que aparece.
- d. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.
- e. Reinicie o sistema no modo normal.

#### ○ Em **Windows 8 e Windows 8.1**:

- a. Na tela Iniciar do Windows, localize **Painel de controle** (por exemplo, você pode começar a digitar "Painel de controle" diretamente na tela Iniciar) e clicar em seu ícone.
- b. Clique **Desinstalar um programa** ou **Programas e características**.
- c. Encontrar **Bitdefender Antivirus Free** e seleccione **Desinstalar**.





- d. Clique **REMOVER** na janela que aparece.
- e. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.
- f. Reinicie seu sistema no modo normal.

○ Em **Windows 10** e **Windows 11**:

- a. Clique **Começar** clique em Configurações.
- b. Clique no **Sistema** ícone na área Configurações e selecione **Aplicativos instalados**.
- c. Encontrar **Bitdefender Antivirus Free** e selecione **Desinstalar**.
- d. Clique **Desinstalar** novamente para confirmar sua escolha.
- e. Clique **REMOVER** na janela que aparece.
- f. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.
- g. Reinicie seu 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 isso:

- 1. Reinicie seu sistema e entre no modo de segurança. Para saber como fazer isso, consulte [Como posso reiniciar no Modo de Segurança? \(página 87\)](#).
- 2. Remova as outras soluções de segurança do seu sistema:

○ Em **windows 7**:

- a. Clique **Começar**, Vá para **Painel de controle** e clique duas vezes **Programas e características**.
- b. Encontre o nome do programa que pretende remover e selecione **Remover**.
- c. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.



- Em **Windows 8 e Windows 8.1**:
  - a. Na tela Iniciar do Windows, localize **Painel de controle** (por exemplo, você pode começar a digitar "Painel de controle" diretamente na tela Iniciar) e clicar em seu ícone.
  - b. Clique **Desinstalar um programa** ou **Programas e características**.
  - c. Encontre o nome do programa que deseja remover e selecione **Remover**.
  - d. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.
- Em **Windows 10 e Windows 11**:
  - a. Clique **Começar** clique em Configurações.
  - b. Clique no **Sistema** ícone na área Configurações e selecione **Aplicativos instalados**.
  - c. Encontre o nome do programa que deseja remover e selecione **Desinstalar**.
  - d. Aguarde a conclusão do processo de desinstalação e reinicie o sistema.

Para desinstalar corretamente outro software, acesse o 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 isso:

1. Reinicie seu sistema e entre no modo de segurança. Para saber como fazer isso, consulte [Como posso reiniciar no Modo de Segurança? \(página 87\)](#).
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 \(página 108\)](#).

## 5.2. Remover ameaças do seu sistema

As ameaças podem afetar o seu sistema de várias formas e a atuação do Bitdefender depende do tipo de ataque da ameaça. Como as ameaças alteram frequentemente o modo de ação, é difícil estabelecer um padrão com base no comportamento e nas ações.

Há situações em que o Bitdefender não consegue remover automaticamente a infecção de ameaças do seu sistema. Nestes casos, a sua intervenção é necessária.

- [Ambiente de Resgate](#)
- [O que fazer quando o Bitdefender encontrar ameaças no seu dispositivo? \(página 101\)](#)
- [Como posso limpar uma ameaça num ficheiro? \(página 103\)](#)
- [Como posso limpar uma ameaça num ficheiro de e-mail? \(página 104\)](#)
- [O que fazer se suspeitar que um ficheiro é perigoso? \(página 105\)](#)
- [O que são os ficheiros protegidos por palavra-passe no relatório de análise? \(página 106\)](#)
- [O que são os itens ignorados no relatório de análise? \(página 106\)](#)
- [O que são os ficheiros muito comprimidos no relatório de análise? \(página 106\)](#)
- [Por que é que Bitdefender eliminou automaticamente um ficheiro infectado? \(página 107\)](#)

Se você não conseguir encontrar seu problema aqui, ou se as soluções apresentadas não resolverem, você pode entrar em contato com os representantes de suporte técnico da Bitdefender conforme apresentado no capítulo [Pedir Ajuda \(página 108\)](#).

### 5.2.1. O que fazer quando o Bitdefender encontrar 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 infectados.
- 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 infectados (Desinfetar, Eliminar, Mover para a Quarentena).



## Aviso

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 **Proteção** no menu de navegação do [Interface do Bitdefender](#).
  - b. No **ANTIVÍRUS** painel, clique **Abrir**.
  - c. No **Avançado** janela, desligue **Escudo Bitdefender**.
2. Exibir objetos ocultos no Windows. Para saber como fazer isso, consulte [Como posso mostrar objetos ocultos no Windows? \(página 85\)](#).
3. Procure a localização do ficheiro infectado (veja no relatório da análise) e elimine-o.
4. Ative a proteção antivírus em tempo real do Bitdefender.

### Caso o primeiro método para remover a infecção falhe:

1. Reinicie seu sistema e entre no modo de segurança. Para saber como fazer isso, consulte [Como posso reiniciar no Modo de Segurança? \(página 87\)](#).



2. Exibir objetos ocultos no Windows. Para saber como fazer isso, consulte [Como posso mostrar objetos ocultos no Windows? \(página 85\)](#).
3. Navegue até o local do arquivo infectado (verifique o log de verificação) e exclua-o.
4. Reinicie o seu sistema e inicie sessão no modo normal.

Se esta informação não for útil, você pode entrar em contato com a Bitdefender para obter suporte conforme descrito na seção [Pedir Ajuda \(página 108\)](#).

## 5.2.2. 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 **Proteção** no menu de navegação do [Interface do Bitdefender](#).
  - b. No **ANTIVÍRUS** painel, clique **Abrir**.
  - c. No **Avançado** janela, desligue **Escudo 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.



## Observação

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 for útil, você pode entrar em contato com a Bitdefender para obter suporte conforme descrito na seção [Pedir Ajuda \(página 108\)](#).

## 5.2.3. 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. Verifique o banco de dados de e-mail com o Bitdefender.
2. Desative a proteção antivírus em tempo real do Bitdefender:
  - a. Clique **Proteção** no menu de navegação do [Interface do Bitdefender](#).
  - b. No **ANTIVÍRUS** painel, clique **Abrir**.
  - c. No **Avançado** janela, desligue **Escudo 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 do Ficheiro, clique em Gestão de ficheiros de dados. Selecione as pastas pessoais (.pst) de ficheiros que pretende compactar e clique em Definições. Clique em Compactar agora.
  - No Microsoft Outlook 2010/2013/2016: No menu Ficheiro, clique em informações, depois em Definições da conta (adicione ou remova contas ou modifique as definições de ligação existentes). Depois clique em Ficheiros de dados, selecione as pastas pessoais (.pst) de ficheiros que pretende compactar e clique em Definições. Clique em Compactar agora.
6. Ative a proteção antivírus em tempo real do Bitdefender.

Se esta informação não for útil, você pode entrar em contato com a Bitdefender para obter suporte conforme descrito na seção [Pedir Ajuda \(página 108\)](#).

## 5.2.4. 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. Executar uma **Verificação do sistema** com o Bitdefender. Para saber mais sobre como fazer isto, aceda a [How do I scan my system?](#).
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 mais sobre como fazer isto, aceda a [Pedir Ajuda \(página 108\)](#).



## 5.2.5. 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 decodificados.

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.

## 5.2.6. 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.

## 5.2.7. 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 descriptação 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.





## 5.2.8. Por que é que Bitdefender eliminou automaticamente um ficheiro infectado?

Se for detetado um ficheiro infectado, o Bitdefender tentará automaticamente desinfecá-lo. Se a desinfecção falhar, o ficheiro é movido para a quarentena de modo a restringir a infecção.

Para determinados tipos de ameaças, a desinfecção não é possível porque o arquivo detectado é totalmente malicioso. Nesses casos, o arquivo infectado é excluído 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.



## 6. CONSEGUINDO AJUDA

### 6.1. Pedir Ajuda

O Bitdefender se empenha em oferecer aos seus clientes um nível incomparável de apoio preciso e rápido. Se tiver qualquer problema ou pergunta sobre o seu produto Bitdefender, pode utilizar vários recursos online para encontrar uma solução ou uma resposta. Ao mesmo tempo, pode entrar em contacto com a equipe de Atendimento ao Cliente da Bitdefender. Os nossos representantes de apoio responderão às suas perguntas em tempo hábil e oferecerão a assistência de que precisa.

### 6.2. Recursos Em Linha

Estão disponíveis vários recursos online para o ajudar a resolver problemas e a responder a questões relacionados com o Bitdefender.

- Centro de Suporte da Bitdefender:  
<https://www.bitdefender.pt/consumer/support/>
- A Comunidade de Especialistas da Bitdefender:  
<https://community.bitdefender.com/en/>
- Bitdefender Cyberpedia:  
<https://www.bitdefender.com/cyberpedia/>

Também pode utilizar o seu motor de busca favorito para saber mais sobre a segurança de computadores, os produtos Bitdefender e a empresa.

#### 6.2.1. Centro de Suporte da Bitdefender

A Bitdefender Support Center é um repositório de informação online acerca dos produtos BitDefender. Armazena, num formato de relatório facilmente acessível, os resultados das atividades de reparação de erros por parte da equipa técnica do suporte BitDefender e da equipa de desenvolvimento, isto juntamente com artigos gerais acerca de prevenção de ameaças, a administração de soluções BitDefender e explicações pormenorizadas e muitos outros artigos.

A Bitdefender Support Center encontra-se aberta ao público e pode ser utilizada gratuitamente. Esta abundância de informação é uma



outra forma de dar aos clientes BitDefender o conhecimento e o aprofundamento que eles necessitam. Todos os pedidos de informação ou relatórios de erro válidos originários de clientes BitDefender são incluídos na Bitdefender Support Center, como relatórios de reparação de erros, ou artigos informativos como suplementos aos ficheiros de ajuda dos produtos.

O Centro de Suporte Bitdefender está disponível a qualquer momento no seguinte endereço: <https://www.bitdefender.pt/consumer/support/>.

## 6.2.2. A Comunidade de Especialistas da Bitdefender

A Comunidade de Especialistas da Bitdefender é um ambiente onde os utilizadores, entusiastas e fãs da Bitdefender podem interagir, trocar ideias, apoiar-se mutuamente e partilhar os seus conhecimentos e soluções. É também um lugar de criação de ideias que fornece um feedback valioso para as nossas equipas de desenvolvimento. Os membros da comunidade são utilizadores experientes da Bitdefender que têm todo o prazer em ajudar outros colegas no seu tempo livre. Com a sua imensa contribuição e os seus esforços genuínos e voluntários, criámos uma base de conhecimento onde os utilizadores podem encontrar respostas e orientação, mas com um toque humano.

Aqui encontrará conversas significativas com pessoas que utilizam a Bitdefender nos seus dispositivos. A comunidade oferece uma verdadeira ligação com os nossos membros e faz com que sua voz seja ouvida. É um lugar onde é encorajado a participar sabendo que sua opinião e sua contribuição são respeitadas e bem recebidas. Ao ser um fornecedor valioso, esforçamo-nos para oferecer um nível inigualável de apoio rápido e preciso e desejamos aproximar os nossos utilizadores de nós. Projetamos a nossa comunidade com este propósito em mente.

Pode encontrar a nossa página da Comunidade de Especialistas aqui:

<https://community.bitdefender.com/en/>

## 6.2.3. Bitdefender Cyberpedia

A Bitdefender Cyberpedia tem toda a informação de que precisa sobre as últimas ameaças cibernéticas. Este é o lugar onde os especialistas da Bitdefender partilham dicas e truques sobre como se protegerem contra hackers, violações de dados, roubo de identidade e tentativas de personificação social.



A página da Bitdefender Cyberpedia pode ser encontrada aqui:

<https://www.bitdefender.com/cyberpedia/>.

## 6.3. Informações de Contato

Uma comunicação eficiente é a chave para um negócio de sucesso. Desde 2001 a BITDEFENDER estabeleceu uma reputação inquestionável por buscar constantemente uma melhor comunicação para superar as expectativas de nossos clientes e parceiros. Se você tiver alguma dúvida, não hesite em nos contatar diretamente através do nosso [Centro de Suporte da Bitdefender \(página 108\)](#).

<https://www.bitdefender.com/cyberpedia/>

### 6.3.1. 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 da 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.



## GLOSSÁRIO

### **Código de ativação**

É uma chave exclusiva que pode ser comprada no varejo e usada para ativar um produto ou serviço específico. Um código de ativação permite a ativação de uma assinatura válida por um determinado período de tempo e número de dispositivos e também pode ser usado para estender uma assinatura com a condição a ser gerada para o mesmo produto ou serviço.

### **ActiveX**

ActiveX é um modelo para escrever programas para que outros programas e o sistema operacional possam chamá-los. A tecnologia ActiveX é usada com o Microsoft Internet Explorer para criar páginas da Web interativas que se parecem e se comportam como programas de computador, em vez de páginas estáticas. Com o ActiveX, os usuários podem fazer ou responder perguntas, usar botões de pressão e interagir de outras maneiras com a página da web. Os controles ActiveX geralmente são escritos usando o Visual Basic. Active X é notável por uma completa falta de controles de segurança; especialistas em segurança de computadores desencorajam seu uso pela internet.

### **Ameaça persistente avançada**

Ameaça persistente avançada (APT) explora vulnerabilidades de sistemas para roubar informações importantes para entregá-las à fonte. Grandes grupos, como organizações, empresas ou governos, são alvo dessa ameaça. O objetivo de uma ameaça persistente avançada é permanecer indetectável por muito tempo, sendo capaz de monitorar e coletar informações importantes sem danificar as máquinas visadas. O método usado para injetar a ameaça na rede é por meio de um arquivo PDF ou documento do Office que pareça inofensivo para que todos os usuários possam executar os arquivos.

### **Adware**

O adware geralmente é combinado com um aplicativo host fornecido gratuitamente, desde que o usuário concorde em aceitar o adware. Como os aplicativos de adware geralmente são instalados depois que o usuário concorda com um contrato de licenciamento que declara a finalidade do aplicativo, nenhuma ofensa é cometida. No entanto, anúncios pop-up podem se tornar um aborrecimento e, em alguns casos, degradar o



desempenho do sistema. Além disso, as informações que alguns desses aplicativos coletam podem causar problemas de privacidade para usuários que não estavam totalmente cientes dos termos do contrato de licença.

## **Arquivo**

Um disco, cassete, ou diretório que contém ficheiros que foram armazenados.

Um arquivo que contém um ou mais arquivos em um formato compactado.

## **Porta dos fundos**

Uma brecha na segurança de um sistema deliberadamente deixada por designers ou mantenedores. A motivação para tais buracos nem sempre é sinistra; alguns sistemas operacionais, por exemplo, vêm com contas privilegiadas destinadas ao uso por técnicos de serviço de campo ou programadores de manutenção do fornecedor.

## **Setor de inicialização**

Um setor no início de cada disco que identifica a arquitetura do disco (tamanho do setor, tamanho do cluster e assim por diante). Para discos de inicialização, o setor de inicialização também contém um programa que carrega o sistema operacional.

## **Vírus de inicialização**

Uma ameaça que infecta o setor de inicialização de um disco fixo ou disquete. Uma tentativa de inicializar a partir de um disquete infectado com um vírus do setor de inicialização fará com que a ameaça se torne ativa na memória. Toda vez que você inicializar seu sistema a partir desse ponto, você terá a ameaça ativa na memória.

## **botnet**

O termo “botnet” é composto pelas palavras “robô” e “rede”. Botnets são dispositivos conectados à Internet infectados com ameaças e podem ser usados para enviar e-mails de spam, roubar dados, controlar remotamente dispositivos vulneráveis ou espalhar spyware, ransomware e outros tipos de ameaças. Seu objetivo é infectar o maior número possível de dispositivos conectados, como PCs, servidores, dispositivos móveis ou IoT pertencentes a grandes empresas ou indústrias.

## **Navegador**



Abreviação de navegador da web, um aplicativo de software usado para localizar e exibir páginas da web. Os navegadores populares incluem Microsoft Internet Explorer, Mozilla Firefox e Google Chrome. Estes são navegadores gráficos, o que significa que eles podem exibir gráficos, bem como texto. Além disso, a maioria dos navegadores modernos pode apresentar informações multimídia, incluindo som e vídeo, embora exijam plug-ins para alguns formatos.

## **Ataque de força bruta**

Ataque de adivinhação de senha usado para invadir um sistema de computador inserindo possíveis combinações de senha, geralmente começando com a senha mais fácil de adivinhar.

## **Linha de comando**

Em uma interface de linha de comando, o usuário digita comandos no espaço fornecido diretamente na tela usando a linguagem de comando.

## **Biscoitos**

Na indústria da Internet, os cookies são descritos como pequenos arquivos contendo informações sobre computadores individuais que podem ser analisados e usados por anunciantes para rastrear seus interesses e gostos online. Neste domínio, a tecnologia de cookies ainda está sendo desenvolvida e a intenção é direcionar os anúncios diretamente para o que você disse que são seus interesses. É uma faca de dois gumes para muitas pessoas porque, por um lado, é eficiente e pertinente, pois você só vê anúncios sobre o que está interessado. Por outro lado, envolve realmente "rastrear" e "seguir" onde você vai e o que você clicar. Compreensivelmente, há um debate sobre privacidade e muitas pessoas se sentem ofendidas com a noção de que são vistas como um "número SKU" (você sabe, o código de barras no verso dos pacotes que é escaneado na fila do caixa do supermercado). Embora esse ponto de vista possa ser extremo, em alguns casos é preciso.

## **Cyberbullying**

Quando colegas ou estranhos estão cometendo atos abusivos contra crianças com o propósito de machucá-las fisicamente. Para prejudicar emocionalmente, os agressores estão enviando mensagens maldosas ou fotos pouco lisonjeiras, fazendo com que suas vítimas se isolem dos outros ou se sintam frustradas.

## **Ataque de dicionário**



Ataques de adivinhação de senha usados para invadir um sistema de computador inserindo uma combinação de palavras comuns para gerar senhas em potencial. O mesmo método é usado para adivinhar as chaves decriptografia de mensagens ou documentos criptografados. Os ataques de dicionário são bem-sucedidos porque muitas pessoas tendem a escolher senhas curtas e simples que são fáceis de adivinhar.

## **Unidade de disco**

É uma máquina que lê e grava dados em um disco. Uma unidade de disco rígido lê e grava discos rígidos. Uma unidade de disquete acessa disquetes. As unidades de disco podem ser internas (alojadas em um computador) ou externas (alojadas em uma caixa separada que se conecta ao computador).

## **Download**

Copiar dados (geralmente um arquivo inteiro) de uma fonte principal para um dispositivo periférico. O termo é frequentemente usado para descrever o processo de copiar um arquivo de um serviço online para o próprio computador. O download também pode se referir à cópia de um arquivo de um servidor de arquivos de rede para um computador na rede.

## **E-mail**

Correio eletrônico. Um serviço que envia mensagens em computadores através de redes locais ou globais.

## **Eventos**

Uma ação ou ocorrência detectada por um programa. Os eventos podem ser ações do usuário, como clicar em um botão do mouse ou pressionar uma tecla, ou ocorrências do sistema, como falta de memória.

## **Exploits**

Uma forma de aproveitar diferentes bugs ou vulnerabilidades que estão presentes em um computador (software ou hardware). Assim, os hackers podem obter o controle de computadores ou redes.

## **Falso positivo**

Ocorre quando um mecanismo de varredura identifica um arquivo como infectado quando, na verdade, não está.

## **Extensão de nome de arquivo**

A parte de um nome de arquivo, após o ponto final, que indica o tipo de dados armazenados no arquivo. Muitos sistemas operacionais usam





extensões de nome de arquivo, por exemplo, Unix, VMS e MS-DOS. Eles geralmente têm de uma a três letras (alguns sistemas operacionais antigos e tristes não suportam mais do que três). Os exemplos incluem "c" para código-fonte C, "ps" para PostScript, "txt" para texto arbitrário.

## **Heurística**

Um método baseado em regras para identificar novas ameaças. Este método de verificação não depende de um banco de dados de informações de ameaças específico. A vantagem da verificação heurística é que ela não é enganada por uma nova variante de uma ameaça existente. No entanto, ocasionalmente pode relatar códigos suspeitos em programas normais, gerando o chamado "falso positivo".

## **Pote de mel**

Um sistema de computador isca criado para atrair hackers para estudar a maneira como eles agem e identificar os métodos heréticos que usam para coletar informações do sistema. Empresas e corporações estão mais interessadas em implementar e usar honeypots para melhorar seu estado geral de segurança.

## **IP**

Protocolo de Internet - Um protocolo roteável no conjunto de protocolos TCP/IP que é responsável pelo endereçamento IP, roteamento e fragmentação e remontagem de pacotes IP.

## **miniaplicativo Java**

Um programa Java projetado para ser executado apenas em uma página da Web. Para usar um applet em uma página da web, você deve especificar o nome do applet e o tamanho (comprimento e largura, em pixels) que o applet pode utilizar. Quando a página é acessada, o navegador baixa o applet de um servidor e o executa na máquina do usuário (o cliente). Os applets diferem dos aplicativos porque são regidos por um protocolo de segurança estrito.

Por exemplo, embora os applets sejam executados no cliente, eles não podem ler ou gravar dados na máquina do cliente. Além disso, os applets são ainda mais restritos para que possam apenas ler e gravar dados do mesmo domínio do qual são servidos.

## **Keylogger**

Um keylogger é um aplicativo que registra tudo o que você digita. Keyloggers não são maliciosos por natureza. Eles podem ser usados para



fins legítimos, como monitorar atividades de funcionários ou crianças. No entanto, eles estão sendo cada vez mais usados por cibercriminosos para fins maliciosos (por exemplo, para coletar dados privados, como credenciais de login e números de CPF).

## **Vírus de macro**

Um tipo de ameaça de computador codificada como uma macro incorporada a um documento. Muitos aplicativos, como Microsoft Word e Excel, oferecem suporte a poderosas linguagens de macro. Esses aplicativos permitem que você incorpore uma macro em um documento e execute a macro sempre que o documento for aberto.

## **cliente de e-mail**

Um cliente de e-mail é um aplicativo que permite enviar e receber e-mails.

## **Memória**

Áreas de armazenamento interno no computador. O termo memória identifica o armazenamento de dados que vem na forma de chips, e a palavra armazenamento é usada para memória que existe em fitas ou discos. Todo computador vem com uma certa quantidade de memória física, geralmente chamada de memória principal ou RAM.

## **Não heurístico**

Este método de verificação depende de um banco de dados de informações de ameaças específico. A vantagem da verificação não heurística é que ela não é enganada pelo que pode parecer uma ameaça e não gera alarmes falsos.

## **predadores online**

Indivíduos que procuram atrair menores ou adolescentes para conversas com o propósito de envolvê-los em atividades sexuais ilegais. As redes sociais são o local ideal onde crianças vulneráveis podem ser facilmente caçadas e induzidas a praticar atividades sexuais, online ou face a face.

## **Programas compactados**

Um arquivo em um formato de compactação. Muitos sistemas operacionais e aplicativos contêm comandos que permitem compactar um arquivo para que ele ocupe menos memória. Por exemplo, suponha que você tenha um arquivo de texto contendo dez caracteres de espaço consecutivos. Normalmente, isso exigiria dez bytes de armazenamento.



No entanto, um programa que compacta arquivos substituiria os caracteres de espaço por um caractere de série de espaço especial seguido pelo número de espaços sendo substituídos. Nesse caso, os dez espaços exigiriam apenas dois bytes. Esta é apenas uma técnica de empacotamento - existem muitas outras.

## **Caminho**

As direções exatas para um arquivo em um computador. Essas direções geralmente são descritas por meio do sistema de arquivamento hierárquico de cima para baixo.

A rota entre quaisquer dois pontos, como o canal de comunicação entre dois computadores.

## **Phishing**

O ato de enviar um e-mail a um usuário que afirma falsamente ser uma empresa legítima estabelecida na tentativa de enganar o usuário para que entregue informações privadas que serão usadas para roubo de identidade. O e-mail direciona o usuário a visitar um site onde é solicitado que ele atualize as informações pessoais, como senhas e números de cartão de crédito, previdência social e contas bancárias, que a organização legítima já possui. O site, no entanto, é falso e criado apenas para roubar as informações do usuário.

## **Fóton**

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.

## **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.

## **Porta**

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



Nas redes TCP/IP e UDP, um ponto de fim para uma ligação lógica. O número da porta identifica o tipo da porta. Por exemplo, a porta 80 é usada para o tráfego HTTP.

## **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.

## **Arquivo de relatório**

Um ficheiro que lista acções que tiveram ocorrência. O BitDefender um ficheiro de reporte que lista o caminho examinado, as pastas, o número de arquivos e ficheiros examinados, e quantos ficheiros suspeitos e infectados foram encontrados.

## **Rootkit**

Um rootkit é um pacote de ferramentas de software que proporcionam um nível de acesso de administrador a um sistema. O termo foi usado em primeiro lugar nos sistemas operativos UNIX e referia-se a ferramentas recompiladas que proporcionavam aos intrusos direitos de administração, permitindo-lhes ocultar a sua presença de forma a não serem vistos pelos administradores do sistema.

O papel principal dos rootkits é ocultar processos, ficheiros, logins e registos. Eles também podem interceptar dados dos terminais, ligações de rede ou periféricos, se eles incorporarem o software para tal.

Os rootkits não são maliciosos por natureza. Por exemplo, os sistemas e mesmo algumas aplicações ocultam ficheiros críticos usando rootkits. No entanto, 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 evitam ser detetados.

## **Script**



Outro termo para macro ou ficheiro de porção, uma escrita é uma lista de comandos que podem ser executados sem a interação do utilizador.

## **Spam**

Lixo de correio electrónico ou lixo de avisos de newsgroups. Geralmente atribuído a qualquer e-mail não solicitado.

## **Spyware**

Qualquer software que encobertamente reúne 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.

## **Itens de inicialização**

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.

## **Inscrição**



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.

## **Bandeja 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.

## **TCP/IP**

Transmission Control Protocol/Internet Protocol - Um conjunto de protocolos de uma rede de trabalho abrangentemente usados Internet que permite comunicações ao longo de redes de computadores interconectadas com várias arquitecturas de hardware e vários sistemas operativos. O TCP/IP inclui padrões de como os computadores comunicam e convenções para ligar redes e conduzir o tráfego.

## **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 a 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.

## **Atualização de informações sobre ameaças**

O padrão binário de uma ameaça é utilizado pela solução de segurança para detetá-la e eliminá-la.

## **Troiano**

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.

## **Atualizar**

Uma nova versão de um produto de software ou hardware concebida para substituir uma versão antiga do mesmo produto. Em adição, a instalação de rotina da atualização verifica se a versão anterior já está instalada no seu computador; se não estiver, não poderá instalar a atualização.

O Bitdefender tem a sua própria funcionalidade de atualização que lhe permite verificar atualizações manualmente, ou permitir atualizar o produto automaticamente.

## **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.

## **Worm**

Um programa que se propaga a si próprio ao longo de uma rede, reproduzindo-se à medida que avança. Não pode ligar-se sozinho a outros programas.