# Bitdefender®
# ANTIVIRUS FOR MAC

## GUIA DO UTILIZADOR

Mac

# Bitdefender Antivirus for Mac

**Guia do usuário**

Data de publicação 24/11/2022


## Notícia legal



Bitdefender

# Índice

# SOBRE ESTE GUIA

## Propósito e público-alvo

Este manual destina-se a todos os utilizadores Macintosh que escolheram Bitdefender Antivirus for Mac como uma solução de segurança para os seus computadores. As informações apresentadas neste livro são adequadas não só para pessoas que percebem de computador, mas também a qualquer pessoa que seja capaz de trabalhar com o sitema operativo Macintosh.

Vai descobrir como configurar e utilizar o Bitdefender Antivirus for Mac para se proteger contra ameaças e outros softwares maliciosos. Vai aprender como conseguir o melhor do seu Bitdefender.

Desejamos-lhe uma agradável e útil leitura.

## Como utilizar este guia

Este manual está organizado em diversos tópicos importantes:

Introdução (página 11)

Primeiros passos da Bitdefender Antivirus for Mac e a sua interface de utilizador.

Proteger contra software malicioso (página 15)

Aprenda como utilizar o Bitdefender Antivirus para Mac para se proteger contra software malicioso.

Configurar preferências (página 35)

Saiba mais sobre as preferências do Bitdefender Antivirus para Mac.

Conseguindo ajuda (página 53)

Onde procurar e onde pedir ajuda se algo inesperado acontecer.

## 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 |
|---|---|
| `sample syntax` | As amostras de sintaxe são impressas com `monospaced` personagens. |
| https://www.bitdefender.com | A hiperligação URL aponta para uma localização externa em servidores http ou ftp. |
| documentation@bitdefender.com | Endereços de email são inseridos no texto para contactar a solicitar mais informação. |
| Sobre este Guia (página 1) | Esta é uma hiperligação interna que o leva para uma localização dentro do documento. |
| `filename` | Arquivos e diretórios são impressos usando `monospaced` Fonte. |
| **opção** | Todas as opções de produtos são impressas usando **audacioso** personagens. |
| **palavra-chave** | Palavras-chave ou frases importantes são destacadas usando **audacioso** 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 critica 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. Escreva todos os seus e-mails relacionados à documentação em inglês para que possamos processá-los com eficiência.

# 1. O QUE É BITDEFENDER ANTIVIRUS FOR MAC

O Bitdefender Antivirus for Mac é um detetor antivírus poderoso, que pode detetar e remover todos os tipos de software malicioso ("ameaças"), incluindo:

- ransomware
- Adware
- vírus
- spyware
- Trojans
- keyloggers
- worms

Esta aplicação deteta e remove não só ameaças no Mac, mas também ameaças no Windows, prevenindo, assim, que envie ficheiros infetados para a sua família, amigos e colegas utilizando PC.

# 2. INSTALAÇÃO E REMOÇÃO

Este capítulo inclui os seguintes tópicos:



## 2.1. Requisitos do sistema

Pode instalar o Bitdefender Antivirus for Mac em computadores Macintosh com sistema operativo X Yosemite (10.10) ou versões mais recentes.

O seu Mac tem de ter um espaço mínimo de 1 GB disponível no disco rígido.

É necessária uma ligação à Internet para registar e atualizar Bitdefender Antivirus for Mac.

**Observação**
O anti-rastreador da Bitdefender e o VPN da Bitdefender apenas podem ser instalados em sistemas macOS 10.12 ou versões mais recentes.

**Como obter a versão do seu macOS e informações de hardware do seu Mac**
Clique no icon da Apple no canto superior esquerdo no ecrã e escolha Sobre **Este Mac**. Na janela que aparece pode ver a versão do seu sistema operativo e outras informações uteis. Clique em **Relatório do Sistema** para informações detalhadas sobre o hardware.

## 2.2. A instalar o Bitdefender Antivirus for Mac

A aplicação de Bitdefender Antivirus for Mac pode ser instalada a partir da sua conta Bitdefender da seguinte forma:

1. Inicie sessão como administrador.
2. Vá a: https://central.bitdefender.com.
3. Inicie a sessão na seu conta Bitdefender com o seu endereço de e-mail e palavra-passe.

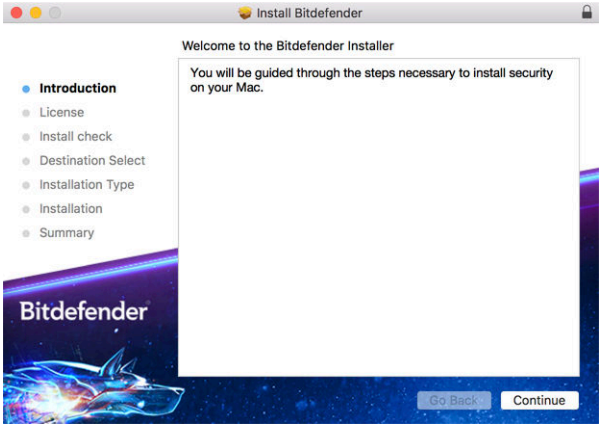
4. Selecione o painel **Os meus dispositivos** e, em seguida, clique em **INSTALAR PROTEÇÃO**.
5. Escolha uma das duas opções disponíveis:
   - **Proteger este dispositivo**
     a. Selecione esta opção e, em seguida, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique 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.
6. Execute o Bitdefender que transferiu.
7. Conclua os passos de instalação.

### 2.2.1. Processo de instalação

Para instalar o Bitdefender Antivirus for Mac:

1. Clique no ficheiro transferido. O instalador será iniciado e será orientado pelo processo de instalação.
2. Siga o assistente de instalação.

## Passo 1 - Janela de Boas-vindas




Clique em {1}Continuar{2}.

## Passo 2 - Ler o Acordo da Subscrição

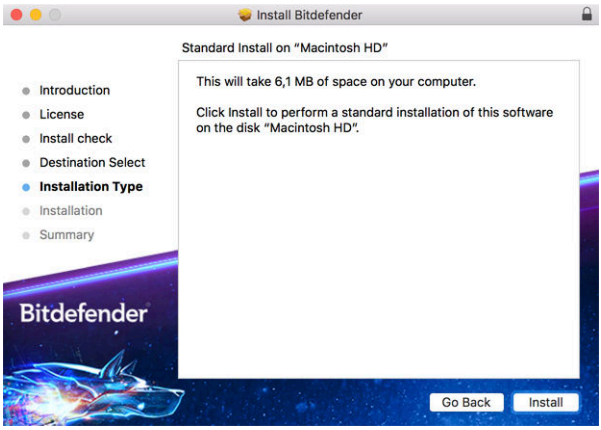

Antes de continuar com a instalação, tem de concordar com o Contrato de Subscrição. Leia o Contrato de Subscrição com calma pois contém os termos e condições que regem a utilização do Bitdefender Antivirus for Mac.

Nesta janela pode também selecionar o idioma em que quer instalar o produto.

Clique em **Continuar** e depois clique em **Aceitar**.

**Importante**
Caso não concorde com estes termos, clique em **Continuar** e depois em **Discordar** para cancelar a instalação e sair do instalador.

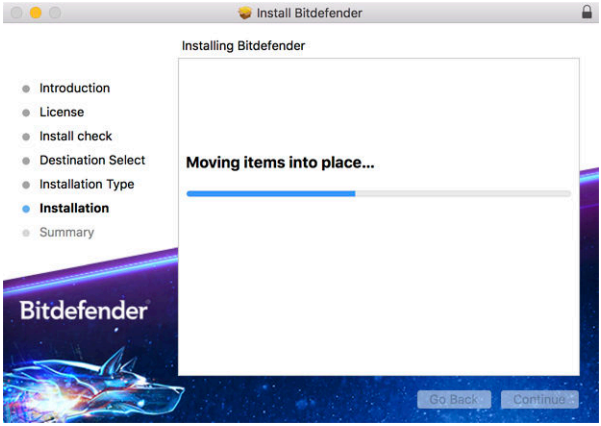
## Passo 3 - Iniciar instalação




O Bitdefender Antivirus para Mac será instalado no `Macintosh HD/Library/Bitdefender`. A localização de instalação não pode ser alterada.

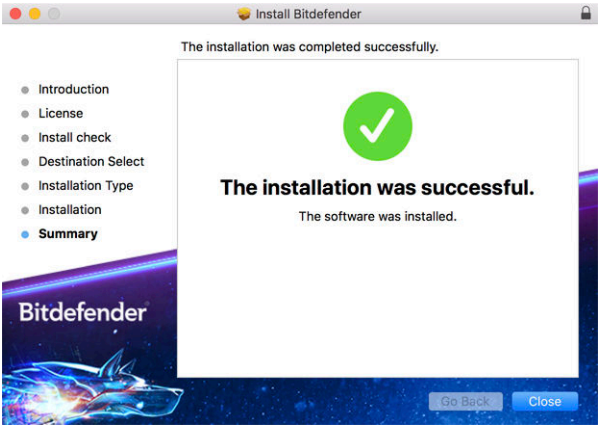
Clique em **Instalar** para iniciar a instalação.

## Passo 4 - Instalar o Bitdefender Antivirus para Mac



Aguarde a instalação concluir e clique em **Continuar**.

### Passo 5 - Terminar




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

O processo de instalação agora está concluído.

**Importante**

- Se estiver a instalar o Bitdefender Antivirus para Mac no macOS High Sierra 10.13.0 ou uma versão mais recente, a notificação da **Extensão do Sistema Bloqueada** aparece. Esta notificação informa que as extensões assinadas pela Bitdefender foram bloqueadas e devem ser ativadas manualmente. Clique em OK para continuar. Na janela Bitdefender Antivirus para Mac que aparece, clique no link **Segurança e Privacidade**. Clique em **Permitir** na parte inferior da janela, ou selecione Bitdefender SRL na lista e clique em **OK**.
- Se estiver a instalar o Bitdefender Antivirus para Mac no macOS Mojave 10.14 ou numa versão mais recente, uma nova janela será exibida, ao informar que deve **Conceder acesso total ao disco à Bitdefender** e **Permita que o Bitdefender carregue**. Siga as instruções no ecrã para configurar corretamente o produto.

## 2.3. Ao remover o Bitdefender Antivirus para Mac

Por ser uma aplicação complexa, o Bitdefender Antivirus for Mac não pode ser removido da forma convencional, ou seja, ao arrastar o ícone da aplicação da pasta **Aplicações** para a Reciclagem.

Para remover o Bitdefender Antivirus para Mac, siga os seguintes passos:

1. Abra uma janela **Finder** e aceda à pasta **Aplicações**.
2. Abra a pasta da Bitdefender em **Aplicações** e depois faça duplo clique em **Desinstalar o Bitdefender**.
3. Selecione a opção de desinstalar preferida.

   > **Observação**
   > Se estiver a tentar remover apenas a aplicação Bitdefender VPN selecione apenas **Desinstalar o VPN**.

4. Clique em **Desinstalar** e aguarde pela conclusão do processo.
5. Clique em **Fechar** para terminar.

   > **Importante**
   > Se houver um erro, pode contactar Atendimento ao Consumidor da Bitdefender como descrito em Pedir Ajuda (página 53).

# 3. INTRODUÇÃO

Este capítulo inclui os seguintes tópicos:



## 3.1. A abrir o Bitdefender Antivirus para Mac

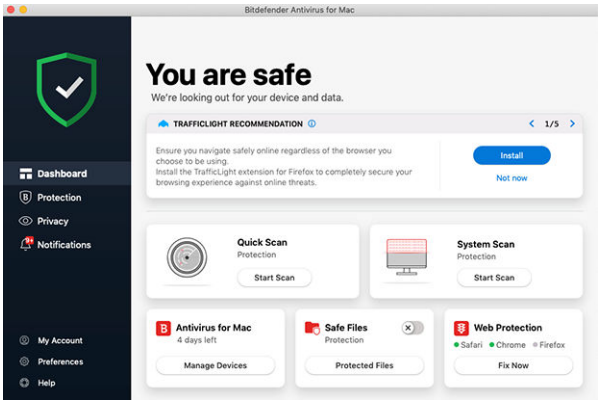
Tem diversas formas para abrir o Bitdefender Antivirus para Mac.

- Clique no ícone Bitdefender Antivirus para Mac no Painel de Iniciação.
- Clique no ícone na barra de menu e escolha **Abrir a interface de Antivirus**.
- Abra a janela de Pesquisa, vá a Aplicações e faça duplo clique no ícone **Bitdefender Antivirus para Mac**.

> **Importante**
> A primeira vez que abrir o Bitdefender Antivirus for Mac no macOS Mojave 10.14 ou superior, aparece uma recomendação de segurança. Esta recomendação aparece porque precisamos de permissões para fazer uma análise completa do seu sistema em busca de ameaças. Para dar permissões, precisa de ter iniciado sessão como administrador e seguir estes passos:
>
> 1. Clique na hiperligação **Preferências do Sistema**.
> 2. Clique no ícone e depois introduza as suas credenciais de administrador.
> 3. Uma nova janela aparece. Arraste o ficheiro **BDLDaemon** para a lista de aplicações permitidas.

## 3.2. Janela principal da aplicação

O Bitdefender Antivirus for Mac 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.

A barra de estado na parte superior da janela informa sobre o estado de segurança do sistema através de mensagens explícitas e cores sugestivas. Se o Bitdefender Antivirus para Mac não tiver avisos, a barra de estado estará a verde. Quando um problema de segurança for detetado, a barra de estado muda para vermelho. Para obter informações detalhadas sobre os problemas e como corrigi-los, consulte Reparar Incidência (página 26).

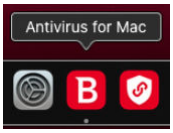
Para lhe oferecer uma operação eficaz e maior proteção durante a realização de diferentes atividades, o **Bitdefender Autopilot** atuará como o seu consultor de segurança pessoal. Dependendo da atividade que realiza, trabalha ou faz pagamentos online, o Bitdefender Autopilot apresentará recomendações contextuais com base na utilização e nas necessidades do seu dispositivo. Isto irá ajudá-lo a descobrir e a beneficiar das vantagens trazidas pelos recursos incluídos na aplicação do Bitdefender Antivirus para Mac.

No menu de navegação à esquerda, pode aceder às secções do Bitdefender para uma configuração detalhada e tarefas administrativas avançadas (Separadores de **Proteção** e **Privacidade**), notificações, a sua **Conta Bitdefender** e a área de **Preferências**. Além disto, pode entrar

em contato connosco (Separador **Ajuda**) para obter suporte caso tenha dúvidas ou ocorra algo inesperado.

## 3.3. Ícone da aplicação no Dock

O ícone do Bitdefender Antivirus para Mac pode ser notado no Dock assim que abrir a aplicação. O ícone no Dock fornece uma maneira fácil de verificar ficheiros e pastas quanto a ameaças. Basta arrastar e soltar o ficheiro ou pasta sobre o ícone do Dock e a verificação começará imediatamente.




## 3.4. Menu de navegação

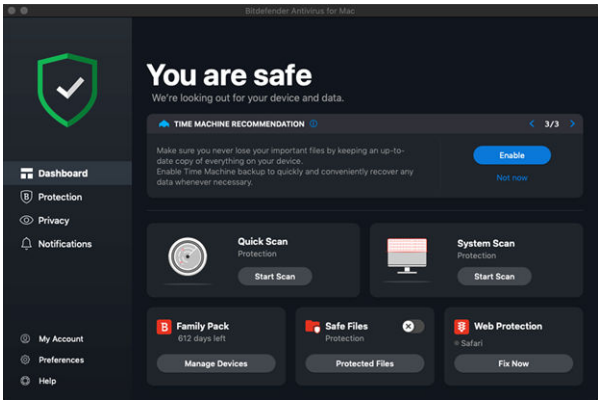
À esquerda, na interface da Bitdefender, encontra-se o menu de navegação, que lhe permite aceder rapidamente às funcionalidades da Bitdefender necessárias para utilizar o seu produto. Os separadores disponíveis nesta área são:

- **Painel de controlo**. A partir daqui, pode resolver rapidamente problemas de segurança, ver recomendações de acordo com os requisitos do seu sistema e padrões de utilização, realizar ações rápidas, e aceder à sua conta da Bitdefender para gerir os dispositivos que adicionou à sua subscrição da Bitdefender.
- **Proteção**. A partir daqui, pode executar análises de antivírus , adicione ficheiros à lista de exceções, proteger ficheiros e aplicações contra ataques de ransomware, proteger as suas cópias de segurança do Time Machine e configurar a proteção enquanto navega na Internet.
- **Privacidade**. A partir daqui, pode abrir a aplicação do Bitdefender VPN e instalar a extensão de Anti-rastreio no seu navegador de internet.
- **Notificações**. A partir daqui, pode ser detalhes sobre as ações tomadas relativamente aos ficheiros verificados.

- **A minha conta**. A partir daqui, pode consultar a conta e a subscrição Bitdefender pelas quais o seu dispositivo está a ser protegido, bem como mudar de conta se necessário.
- **Preferências**. A partir daqui, pode configurar as definições do Bitdefender.
- **Ajuda**. Aqui, pode entrar em contacto com o departamento de Assistência Técnica sempre que precisar de ajuda com o seu produto Bitdefender. Pode também enviar feedback para melhorar o produto.

## 3.5. Modo Escuro

Para proteger a vista de brilho e luzes durante a noite ou em locais pouco iluminados, o Bitdefender Antivirus for Mac possui um Modo Escuro para o Mojave 10.14 e daí em diante. As cores da interface foram optimizadas para que possa utilizar o seu Mac sem forçar a vista. A interface do Bitdefender Antivirus for Mac ajusta-se automaticamente consoante as definições do seu dispositivo.



# 4. PROTEGER CONTRA SOFTWARE MALICIOSO

Este capítulo inclui os seguintes tópicos:



## 4.1. Melhores Práticas

Para manter o seu sistema protegido contra ameaças e evitar infeções acidentais de outros sistemas, siga estas práticas:

- Mantenha o **Bitdefender Shield** ativado, de forma a permitir que os ficheiros do sistema sejam automaticamente verificados pelo Bitdefender Antivirus para Mac.
- Mantenha o seu Bitdefender Antivirus for Mac atualizado com as informações sobre as ameaças e atualizações de produto mais recentes.
- Verifique e corrija os problemas regularmente relatados pelo Bitdefender Antivirus para Mac. Para mais informações, consulte o Reparar Incidência (página 26).
- Verifique o registo detalhado de eventos relacionados à atividade do Bitdefender Antivirus para Mac no seu computador. Sempre que algo

relevante para a segurança do seu sistema ou dados ocorrer, uma mensagem nova é adicionada à área de Notificações do Bitdefender. Para mais detalhes, aceda a Notificações (página 27).

- É recomendável que também siga estas práticas:
  - Crie o hábito de verificar ficheiros que baixa de uma memória de armazenamento externa (como uma unidade USB ou CD), especialmente quando desconhecer a fonte.
  - Se tiver um ficheiro DMG, monte-o e analise o seu conteúdo (os ficheiros no volume/imagem montada).

  A forma mais fácil de verificar um ficheiro, uma pasta ou um volume é ao arrastar e largar sobre a janela Bitdefender Antivirus para Mac ou no ícone na Dock

Nenhuma outra configuração ou ação é necessária. No entanto, se pretender, é possível ajustar as definições e preferências da aplicação para melhor satisfazer as suas necessidades. Para mais informação, dirija-se a Configurar preferências (página 35).

## 4.2. Analisar o seu Mac

Além do recurso **Bitdefender Shield**, que monitoriza regularmente as aplicações instaladas, ao procurar ações semelhantes a ameaças e evita que novas ameaças entrem no seu sistema, pode verificar o seu Mac ou ficheiros específicos a qualquer momento que queira.

A maneira mais fácil de verificar um ficheiro, uma pasta ou um volume é arrastá-lo e soltá-lo sobre a janela do Bitdefender Antivirus para Mac ou ícone do Dock. O assistente de verificação irá aparecer e guiá-lo através do processo de verificação.

Também pode iniciar uma análise como se segue:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. Selecione o separador **Antivírus**.
3. Clique num dos três botões para iniciar a análise desejada.
   - **Análise Rápida** - procura por ameaças nos locais mais vulneráveis no seu sistema (por exemplo, as pastas que contêm os

documentos, transferências, transferências de e-mail e ficheiros temporários de cada utilizador).

- **Verificação do Sistema** - realize uma verificação completa por ameaças em todo o sistema. Todas as montagens ligadas também serão verificadas.

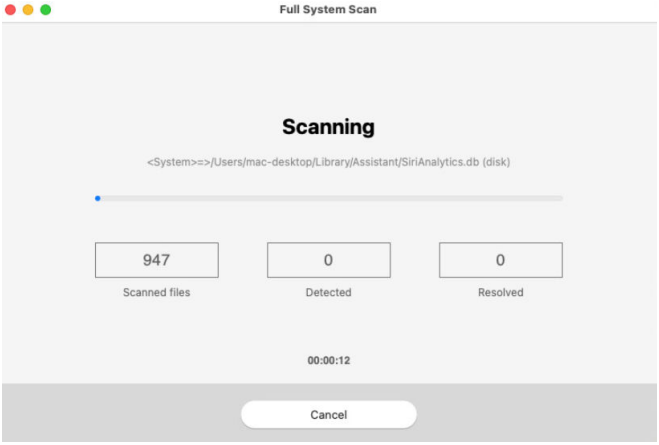
> **Observação**
> Dependendo do tamanho do seu disco rígido, analisar todo o sistema pode demorar (até uma hora ou mais). Para um desempenho melhor, é recomendável não executar esta tarefa ao executar outras tarefas intensivas (como edição de vídeo).
>
> Se preferir, pode optar por não analisar volumes montados específicos adicionando-os à lista **Exceções** na janela de Proteção.

- **Análise Personalizada** - ajuda a verificar ameaças em ficheiros, pastas ou volumes específicos.

Pode também iniciar uma Análise de Sistema ou Análise Rápida no painel de controlo.

## 4.3. Assistente de Análise

Sempre que iniciar uma verificação, o assistente de análise do Bitdefender Antivirus for Mac aparece.



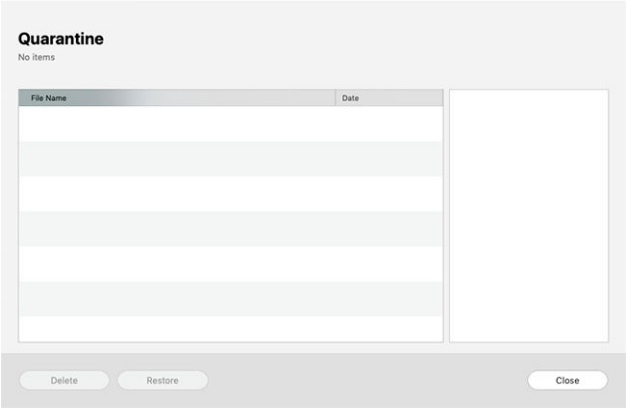
Informações em tempo real sobre as ameaças detetadas e resolvidas são apresentadas durante cada análise.

Espere que o Bitdefender Antivirus para Mac termine a verificação

> **Observação**
> O processo de verificação pode demorar algum tempo, dependendo da complexidade da mesma.

## 4.4. Quarentena

O Bitdefender Antivirus for Mac permite o isolamento de ficheiros infectados ou suspeitos numa área segura, chamada de quarentena. Quando uma ameaça se encontra na quarentena não pode provocar nenhum mal, porque não pode ser nem lida nem executada.




A secção de Quarentena mostra todos os ficheiros atualmente isolados na pasta de Quarentena.

Para eliminar um ficheiro da quarentena, selecione-o e clique em **Eliminar**. Se pretende restaurar um ficheiro da quarentena para a respetiva localização original, selecione-o e clique em **Restaurar**.

Para visualizar a lista de itens adicionados à quarentena:

1. Clique **Proteção** no menu de navegação na interface do Bitdefender.
2. Clique em **Abrir** no painel de **Quarentena**.

## 4.5. Bitdefender Shield (proteção em tempo real)

O Bitdefender fornece uma proteção contínua e em tempo real contra uma ampla variedade de ameaças ao verificar todos os ficheiros instalados, as suas versões atualizadas e ficheiros novos e modificados.

Para desativar a proteção em tempo real:

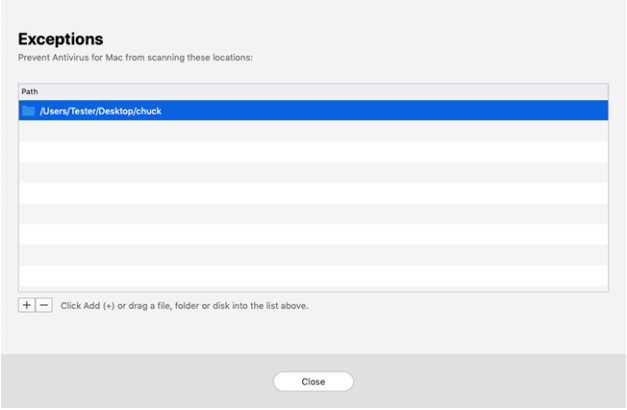
1. Clique em **Preferências** no menu de navegação da interface da Bitdefender.
2. Desligue o **Bitdefender Shield** na janela de **Proteção**.

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

## 4.6. Exceções de Análise

Se quiser, pode configurar o Bitdefender Antivirus for Mac para não analisar ficheiros, pastas ou até mesmo um volume inteiro específicos. Por exemplo, pode pretender eliminar da análise:

- Ficheiros que são erroneamente identificados como infetados (conhecidos como falsos positivos)
- Ficheiros que causam erros de análise
- Volumes de cópia de segurança



A lista de exceções contém os caminhos que foram excluídos da verificação.

Para aceder à lista de exceções:

1. Clique **Proteção** no menu de navegação na interface do Bitdefender.
2. Clique em **Abrir** no painel de **Exceções**.

Há duas formas de configurar uma exceção de análise:

- Arraste e largue um ficheiro, pasta ou volume sobre a lista de exceções.
- Clique no botão com o sinal mais (+), localizado sob a lista de exceções. De seguida, escolha o ficheiro, pasta ou volume a ser excluído da análise.

Para remover uma exceção de análise, selecione-a na lista e clique no botão com o sinal menos (-), localizado na lista de exceções.

## 4.7. Proteção da Internet

O Bitdefender Antivirus for Mac utiliza as extensões do TrafficLight para tornar a sua experiência de navegação na Web completamente segura. As extensões do TrafficLight intercetam, processam e filtram todo o tráfego na Web, bloqueando conteúdo malicioso.

As extensões funcionam e integram-se com os seguintes browsers: Mozilla Firefox, Google Chrome e Safari.

### 4.7.1. Ativar extensões do TrafficLight

Para ativar as extensões do TrafficLight:

1. Clique em **Resolver agora** no cartão de **Proteção da web** no Painel de Controlo.
2. É aberta a janela **Proteção na Web**.
   O navegador detetado que tem instalado no seu sistema aparecerá. Clique em **Obter extensão** para instalar a extensão do TrafficLight no seu navegador.
3. Vai ser redirecionado para:
   https://bitdefender.com/solutions/trafficlight.html
4. Selecione **Transferência Gratuita**.

5. Siga os passos para instalar a extensão do TrafficLight correspondente ao seu browser.

### 4.7.2. Gerir definições da extensões

Está disponível uma variedade de funcionalidades para o proteger de todas as formas de ameaças que pode encontrar enquanto navega na Internet. Para acedê-los, clique no ícone do TrafficLight próximo das definições do seu navegador e, em seguida, clique no botão ⚙ **Definições**:

- **Definições Bitdefender TrafficLight**
  - Proteção na Web - previne que aceda a sites utilizados para ataques de malware, phishing e fraude.
  - Analisador de Resultados de Pesquisa - proporciona alertas antecipados de websites de risco nos seus resultados de pesquisa.
- **Exceções**

  Se estiver no site que precisa de adicionar às exceções, clique em **Adicionar o site atual à lista**.

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

  Nenhum aviso será exibido caso ameaças estejam presentes nas páginas excluídas. É por esta razão que apenas as páginas em que confia totalmente devem ser adicionadas a esta lista.

### 4.7.3. Classificação de página e alertas

Dependendo de como o TrafficLight classifica a página que está a ver, é apresentado um dos seguintes ícones nessa área:

✅ Esta é uma página segura de visitar. Pode continuar o seu trabalho.

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

⛔ Deve abandonar esta página web imediatamente pois contém malware e outras ameaças.

No Safari, o fundo dos ícones do TrafficLight é preto.

## 4.8. Antitracker

Uma grande parte dos sites que utiliza monitorizadores para recolher informação sobre o seu comportamento para compartilhar com empresas

ou para mostrar publicidade direcionada para si. Devido a isso, os donos dos sites ganham dinheiro por proporcionar conteúdo de graça ou para continuarem a funcionar. Além de recolher informação, os monitorizadores podem desacelerar a sua navegação ou desperdiçar a sua banda larga.

Com a extensão Anti-rastreio Bitdefender ativada no seu navegador da web, evita que seja rastreado para que os seus dados permaneçam privados enquanto navega online e acelera o tempo que os sites precisam para carregar.

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

- Google Chrome
- Mozilla Firefox
- Safari

Os monitorizadores que detectamos estão divididos nas seguintes categorias:

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

### 4.8.1. A ativar o Anti-rastreio Bitdefender

Para ativar a extensão Anti-rastreio Bitdefender no seu navegador da web:

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
2. Selecione o separador **Anti-tracker**.

3. Clique **Permitir extensão** no browser em que pretende activar a extensão.

### 4.8.2. Interface do Antitracker

Quando a extensão Anti-rastreio Bitdefender é ativada, o ícone aparece ao lado da barra de pesquisa no seu navegador da web. Todas as vezes que visita um site, um contador pode ser observado no ícone, referente aos rastreadores detetados e bloqueados. Para ver mais detalhes sobre os rastreadores bloqueados, clique no ícone para abrir a interface. Além do número de rastreadores bloqueados, pode visualizar o tempo necessário para a página carregar e as categorias às quais pertencem os rastreadores detetados. Para ver a lista dos sites que estão a rastrear, clique na categoria desejada.

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

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

### 4.8.3. Desligar o Anti-rastreio Bitdefender

Para desligar o Anti-rastreio Bitdefender do seu navegador da internet:

1. Abra o seu navegador web.
2. Clique no ícone ao lado da barra de endereço no seu navegador da web.
3. Clique no ícone no canto superior direito.
4. Utilize o interruptor correspondente para o desativar.
   O ícone do Bitdefender fica cinzento.

### 4.8.4. Permitir a monitorização de um site

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

1. Abra seu navegador da web.

2. Clique no ícone ao lado da barra de pesquisa.
3. Clique no ícone no canto superior direito.
4. Se você estiver no site que deseja adicionar às exceções, clique em **Adicionar site atual à lista**.
   Se você deseja adicionar outro site, digite seu endereço no campo correspondente e clique em .

## 4.9. Safe Files

Ransomwares são softwares maliciosos que atacam sistemas vulneráveis bloqueando-os e exigindo dinheiro para permitir que o utilizador volte a ter controlo do seu sistema. Este software malicioso finge ser inteligente ao exibir mensagens falsas para assustar o utilizador, persuadindo-o a realizar o pagamento solicitado.

Utilizando a tecnologia mais recente, a Bitdefender assegura a integridade do sistema ao proteger as suas áreas essenciais contra ataques de ransomware sem ter impacto no sistema. Contudo, pode desejar proteger os seus ficheiros pessoais, como documentos, fotos ou filmes, contra o acesso de aplicações não fiáveis. Com o Safe Files da Bitdefender pode colocar os seus ficheiros pessoais sob proteção e configurar quais aplicações devem ou não ter permissão para fazer alterações nos ficheiros protegidos.

Para adicionar ficheiros ao ambiente protegido posteriormente:

1. Clique **Proteção** no menu de navegação na interface do Bitdefender.
2. Selecione o separador **Antiransomware**.
3. Clique em **Ficheiros protegidos** na área de ficheiros seguros.
4. Clique no botão com o sinal mais (+), localizado sob a lista de ficheiros protegidos. Em seguida, escolha o ficheiro, pasta ou volume a proteger no caso de ataques de ransomware que tentam aceder aos mesmos.

Para evitar o abrandamento do sistema, recomendamos que adicione no máximo 30 pastas ou guarde vários ficheiros numa única pasta.

Por predefinição, as pastas Imagens, Documentos, Ambiente de Trabalho e Transferências estão protegidas contra ataques de ameaças.

> **Observação**
> Pastas personalizadas apenas podem ser protegidas para os utilizadores atuais. Unidades externas, ficheiros do sistema e de aplicações não podem ser adicionados ao ambiente de proteção.

Será informador sempre que uma aplicação desconhecida com um comportamento incomum tente modificar os ficheiros adicionados. Clique em **Permitir** ou **Bloquear** para adicioná-la à lista **Gerir aplicações**.

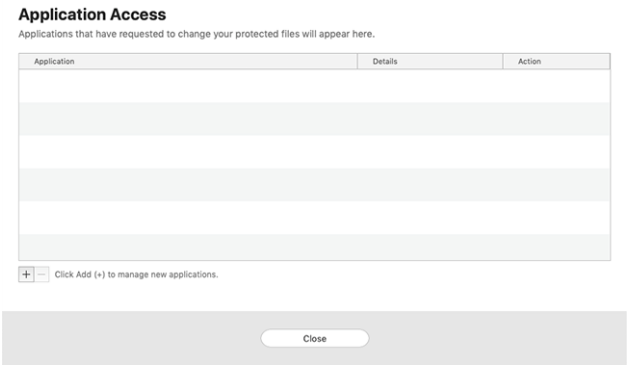
### 4.9.1. Acesso à aplicação

As aplicações que tentam mudar ou apagar ficheiros protegidos podem ser sinalizadas como potencialmente inseguras e adicionadas à lista de aplicações bloqueadas. Se uma aplicação como esta estiver bloqueada e não tiver a certeza se o respetivo comportamento é normal, pode autorizá-la ao seguir estes passos:

1. Clique **Proteção** no menu de navegação na interface do Bitdefender.
2. Selecione os **Anti-Ransomware** aba.
3. Clique em **Acesso à aplicação** na área de ficheiros seguros.
4. Altere o estado para Permitir, ao lado da aplicação bloqueada.

As aplicações definidas como Permitidas também podem ser definidas como Bloqueadas.

Utilize o método arraste&largar ou clique no sinal positivo (+) para adicionar mais aplicações à lista.



## 4.10. Time Machine Protection

A Proteção da Máquina do Tempo da Bitdefender funciona como uma camada de segurança adicional para a sua unidade de cópia de segurança, ao incluir todos os ficheiros nela armazenados, através do bloqueio do acesso de qualquer fonte externa. Caso os ficheiros da sua unidade da Máquina do Tempo sejam encriptados por ransomware, poderá recuperá-los sem pagar pelo resgate.

Caso precise de restaurar os itens de uma cópia de segurança da Máquina do Tempo, verifique a página de apoio da Apple para ver as instruções.

### 4.10.1. Ativar ou desativar a Proteção da Máquina do Tempo

Para ligar ou desligar desative a Proteção da Máquina do Tempo:

1. Clique em **Proteção** no menu de navegação da interface do **Bitdefender**.
2. Selecione os **Anti-Ransomware** aba.
3. Ative ou desative o botão de **Proteção Time Machine**.

## 4.11. Reparar Incidência

O Bitdefender Antivirus for Mac deteta automaticamente e informa-o sobre uma série de problemas que podem afetar a segurança do seu sistema e dados. Desta forma, pode reparar riscos de segurança facilmente e a tempo.

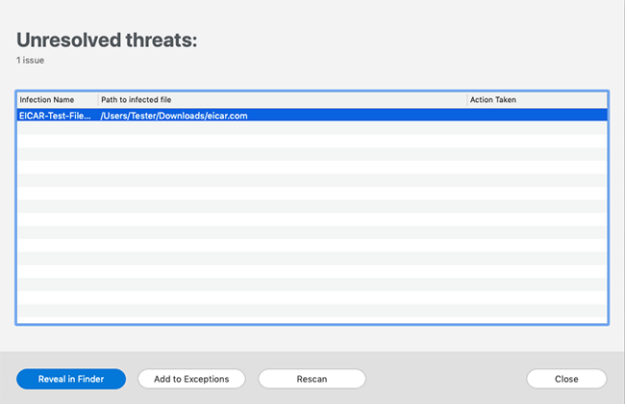
Reparar os problemas indicados pelo Bitdefender Antivirus for Mac é uma forma rápida e fácil de garantir a melhor proteção do seu sistema e dados.

Os problemas detetados incluem:

- A nova atualização de informações sobre ameaças não foi descarregada dos nossos servidores.
- Foram detectadas ameaças no seu sistema e o produto não pode desinfectá-las automaticamente.
- A proteção em tempo real está desativada.

Para verificar e reparar os problemas detetados:

1. Se o Bitdefender não tiver alertas, a barra de estado é verde. Quando um problema de segurança é detectado, a cor da barra de estado muda para vermelho.
2. Verifique a descrição para obter mais informações.
3. Quando um problema for detectado, clique no botão correspondente para realizar uma ação.




A lista de ameaças não resolvidas é atualizada após cada verificação de sistema, independentemente de se a verificação é feita de forma automática em segundo plano ou iniciada por si.

Pode escolher as seguintes ações para ameaças não resolvidas:

- **Eliminar manualmente**. Tome esta ação para remover as infeções manualmente.
- **Adicionar às Exceções**. Esta ação não está disponível para ameaças encontradas dentro dos ficheiros.

## 4.12. Notificações

A Bitdefender mantém um registo detalhado de eventos em relação à sua atividade no seu computador. Sempre que acontece algo relevante para a segurança do seu sistema ou dados, é adicionada uma nova mensagem à área de Notificações da Bitdefender, de forma semelhante a um novo e-mail a aparecer na sua caixa de entrada.

As notificações são uma ferramenta importante na monitorização e gestão da proteção do seu Bitdefender. Por exemplo, pode verificar

com facilidade se a atualização foi realizada com sucesso, se foram encontradas ameaças ou vulnerabilidades no seu computador, etc. Adicionalmente, pode realizar outras ações, se necessário, ou alterar ações tomadas pelo Bitdefender.

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

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.

## 4.13. Atualizações

Novas ameaças são encontradas e identificadas todos os dias. É por isto que é muito importante manter Bitdefender Antivirus for Mac atualizado com as atualizações de informação mais recentes.

As atualizações de informações sobre ameaças são executadas imediatamente, ou seja, os ficheiros que precisam de ser atualizados são substituídos progressivamente. Deste modo, a atualização não afetará o funcionamento do produto e, ao mesmo tempo, qualquer vulnerabilidade será eliminada.

- Se o Bitdefender Antivirus for Mac estiver atualizado, pode detetar as ameaças mais recentes descobertas e limpar os ficheiros infetados.

- Se o Bitdefender Antivirus para Mac não estiver atualizado, não será capaz de detetar e remover as ameaças mais recentes descobertas pelo Bitdefender Labs.

### 4.13.1. Solicitar uma Atualização

Pode solicitar uma atualização manualmente sempre que quiser.

É necessária uma ligação à Internet ativa para verificar atualizações disponíveis e transferi-las.

Para solicitar uma atualização manualmente:

1. Clique no botão **Ações** na barra de menu.
2. Escolha **Atualizar base de dados de informações sobre ameaças**.

Em alternativa, pode solicitar uma atualização manualmente ao premir CMD + U.

Pode ver o progresso de atualização e ficheiros transferidos.

### 4.13.2. A obter atualizações através de um servidor proxy

O Bitdefender Antivirus for Mac só pode ser atualizado através de servidores proxy que não requerem autenticação. Não precisa de modificar quaisquer definições do programa.

Caso se ligue à Internet através de um servidor proxy que requer autenticação, é necessário mudar para uma ligação direta regularmente para obter atualizações de informações sobre as ameaças.

### 4.13.3. Atualizar para uma nova versão

Ocasionalmente, lançamos atualizações do produto para adicionar novas funcionalidades e melhorias ou reparar problemas. Estas atualizações podem exigem um reinício do sistema para iniciar a instalação de ficheiros novos. Por predefinição, se uma atualização requer a reinicialização do sistema, o Bitdefender Antivirus for Mac continuará a trabalhar com os ficheiros anteriores até reiniciar o sistema. Neste caso, o processo de atualização não interferirá com o trabalho do utilizador.

Quando uma atualização do produto é concluída, uma janela pop-up irá informar para reiniciar o sistema. Se perder a notificação, pode clicar em **Reiniciar para atualizar** na barra de menus ou reiniciar o sistema manualmente.

### 4.13.4. Descobrir informação sobre o Bitdefender Antivirus para Mac

Para mais informações sobre a versão do Bitdefender Antivirus for Mac que tem instalada, aceda à janela **Informações**. Na mesma janela, pode obter acesso e visualizar as licenças de código aberto do Contrato de Subscrição e a Política de Privacidade.

Para aceder à janela Sobre:

1. Abra o Bitdefender Antivirus para Mac.
2. Clique em Bitdefender Antivirus para Mac na barra de menu e selecione **Sobre o Antivirus para Mac**.

# 5. VPN

Este capítulo inclui os seguintes tópicos:



## 5.1. Sobre a VPN

Com o Bitdefender VPN , pode manter os seus dados privados sempre que se ligar a redes sem fios não seguras em aeroportos, shoppings, cafés ou hotéis. Assim, poderá evitar situações inoportunas, como roubo de dados pessoais ou tentativas de tornar o endereço de IP do seu dispositivo acessível a hackers.

A aplicação VPN pode ser instalada a partir do seu produto Bitdefender e utilizada todas as vezes que quiser adicionar uma camada extra de proteção à sua ligação. A VPN serve como um túnel entre o seu dispositivo e a rede a que se liga para proteger a sua ligação, ao encriptar os dados utilizados com uma encriptação de nível bancário e ao ocultar o seu endereço IP onde quer que esteja. O seu tráfego é redirecionado por meio de um servidor separado; tornando assim o seu dispositivo quase impossível de ser identificado por meio de uma infinidade de outros dispositivos que estão a utilizar os nossos serviços. Além disso, enquanto estiver ligado à internet via Bitdefender VPN, pode aceder ao conteúdo que normalmente é restrito em áreas específicas.

> **Observação**
> Alguns países censuram a Internet e, portanto, a utilização de VPN nos seus territórios foi banido por lei. Para evitar consequências legais, pode ser apresentada uma mensagem de aviso ao tentar utilizar a aplicação do VPN pela primeira vez. Ao continuar a utilizar a funcionalidade, confirma que está ciente dos regulamentos aplicáveis e dos riscos aos quais pode estar exposto.

## 5.2. A abrir a VPN

Há três formas de abrir a aplicação Bitdefender VPN:

- Clique em **Privacidade** no menu de navegação da interface da **Bitdefender**.
  Clique em **Abrir** no cartão Bitdefender VPN.
- Clique no ícone da barra de menu.
- Aceda à pasta Aplicações, abra a pasta Bitdefender e clique duas vezes no ícone Bitdefender VPN.

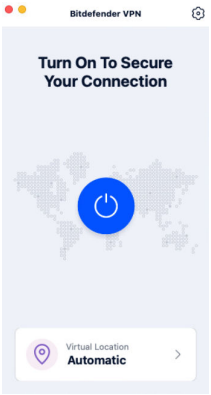
Na primeira vez que abrir a aplicação, ser-lhe-á solicitada permissão para que a Bitdefender possa adicionar configurações. Ao permitir que a Bitdefender adicione configurações, está a concordar que a atividade da rede do seu dispositivo poderá ser filtrada ou monitorizada ao utilizar a aplicação de VPN.

> **Observação**
> A aplicação Bitdefender VPN só pode ser instalado no macOS Sierra (10.12.6), macOS High Sierra (10.13.6), ou macOS Mojave (10.14) ou versões posteriores do sistema operativo.

## 5.3. Interface

A interface do VPN exibe o estado da aplicação, conectado ou desconectado. O local do servidor para utilizadores com a versão gratuita é determinado automaticamente pelo Bitdefender para o servidor mais adequado, enquanto os utilizadores Premium têm a possibilidade de alterar o local do servidor ao qual desejam se ligar selecionando-o na lista Localizações virtuais. Para detalhes sobre as subscrições de VPN, aceda a Subscrições (página 34).

Para ligar ou desligar, basta clicar no estado exibido no topo do ecrã. A barra de menu fica preta quando a VPN está conectada e branca quando a VPN está desconectada.




Enquanto estiver ligado, o tempo decorrido é mostrado na parte inferior da interface. Para aceder a mais opções, clique no ícone ⚙ no canto superior direito:

- **A minha conta** - detalhes sobre a sua conta Bitdefender e a subscrição do VPN são exibidos. Clique em **Trocar de conta** se deseja iniciar sessão com outra conta.
- **Definições** - dependendo das suas necessidades, pode personalizar o comportamento do seu produto:
  - **Geral**
    - Notificações - Exiba as notificações de produtos.
    - Executar no arranque - Automaticamente executar o Bitdefender VPN no início da sessão.
    - Relatórios de produto - Submeta relatórios de produto anónimos para nos ajudar a melhorar a experiencia e a capacidade de proteção.
  - **Avançado**
    - Interruptor de corte da Internet - Suspende temporariamente todo o tráfego da internet caso a ligação à VPN caia acidentalmente.
    - Bloqueador de anúncios e Anti-rastreio - Bloqueie anúncios e rastreadores para desfrutar de uma web mais limpa e rápida.
    - Split tunneling - Os sites selecionados irão contornar o VPN e aceder à internet diretamente.

> **Observação**
> Clique em **Gerir** e depois em **Adicionar o website** para adicionar páginas da web a esta lista.

- Ligar automaticamente - Ligar o VPN automaticamente quando:
  - A ligar a uma rede Wi-Fi pública ou insegura.
  - Uma aplicação de partilha de ficheiros ponto-a-ponto foi iniciada.

- **Apoio** - é redirecionado para a nossa plataforma do Centro de Apoio onde poderá ler um artigo útil sobre como utilizar o Bitdefender VPN.
- **Sobre** - são exibidas informações sobre a versão instalada.
- **Sair** - sair da aplicação.

## 5.4. Subscrições

O Bitdefender VPN oferece gratuitamente 200 MB de franquia por dispositivo para proteger a sua ligação sempre que precisar, além de o ligar automaticamente ao melhor local de servidor.

Para obter tráfego ilimitado e acesso irrestrito a conteúdos no mundo inteiro escolhendo um local da sua preferência, atualize para a versão Premium.

Pode atualizar para a versão Bitdefender Premium VPN em qualquer momento, ao clicar no botão **Atualizar** disponível na interface do produto.

A subscrição do Bitdefender Premium VPN é independente da subscrição do Bitdefender Antivirus para Mac, o que significa que poderá utilizá-la enquanto estiver disponível, independentemente do estado da subscrição de segurança. Caso a subscrição do Bitdefender Premium VPN expire, mas a do Bitdefender Antivirus para Mac ainda estiver ativa, será revertido para o plano gratuito.

O Bitdefender VPN é um produto multiplataforma, disponível nos produtos Bitdefender compatíveis com Windows, MacOS, Android e iOS. Quando atualizar para o plano premium, poderá utilizar a sua subscrição em todos os seus produtos, desde que inicie a sessão com a mesma conta da Bitdefender.

# 6. CONFIGURAR PREFERÊNCIAS

Este capítulo inclui os seguintes tópicos:



## 6.1. Aceder às preferências

Para abrir a janela de Preferências do Bitdefender Antivirus para Mac:

- Faça qualquer uma das seguintes:
  - Clique **Preferências** no menu de navegação na interface do Bitdefender.
  - Clique em Bitdefender Antivirus para Mac na barra de menu e selecione **Preferências**.

## 6.2. Preferências de proteção

As preferências de proteção permitem que configure a abordagem geral de análise. Pode configurar as ações para ficheiros infectados e suspeitos detetados e outras definições gerais.

- **Bitdefender Shield.** A Bitdefender Shield oferece proteção em tempo real contra uma ampla gama de ameaças, verificando todas as aplicações instaladas, suas versões atualizadas e ficheiros novos e modificados. Não recomendamos que desative a Bitdefender Shield, mas se for necessário, faça-o pelo menor tempo possível. Se a Bitdefender Shield for desativada, não estará protegido contra ameaças.
- **Apenas Analise ficheiros novos e alterados.** Selecione esta caixa de seleção para configurar o Bitdefender Antivirus para Mac para analisar apenas ficheiros que não foram verificados antes ou que foram modificados desde a última análise.

Pode optar por não aplicar esta configuração para a verificação personalizada por meio de arrastar e soltar ao desmarcar a caixa de seleção correspondente.

- **Não analise conteúdo em cópias de segurança.** Selecione esta caixa para eliminar ficheiros de cópia de segurança da análise. Se os ficheiros infetados forem restaurados posteriormente, o Bitdefender Antivirus para Mac irá detetá-los automaticamente e tomará a ação apropriada.

## 6.3. Preferências avançadas

Pode escolher uma ação coletiva para todos os problemas e itens suspeitos encontrados durante o processo de análise.

**Ação para itens infetados**

- **Tente desinfetar ou mover para quarentena** - Se forem detetados ficheiros infetados, a Bitdefender tentará desinfetá-los (eliminar o código malicioso) ou colocá-los em quarentena.
- **Não fazer nada** - Nada será realizada qualquer ação em relação aos ficheiros detetados.

**Ação para itens suspeitos**

- **Mover os ficheiros para quarentena** - Se forem detetados ficheiros suspeitos, a Bitdefender irá colocá-los em quarentena.
- **Não faça nada** - Nenhuma ação será tomada nos arquivos detectados.

## 6.4. 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 **Preferências** no menu de navegação na interface do Bitdefender.
2. Selecione o separador **Outros**.
3. Ative ou desative o botão **As minhas ofertas**.

**Observação**
A opção **As minhas ofertas** aparece ativada como definição padrão.

# 7. SOBRE A CENTRAL BITDEFENDER

A Bitdefender Central é a plataforma virtual onde tem acesso às funções e serviços online do produto, e pode realizar remotamente tarefas importantes nos dispositivos em que a Bitdefender estiver instalada. Pode aceder à sua conta Bitdefender de qualquer computador ou dispositivo móvel ligado à internet, acedendo https://central.bitdefender.com, ou diretamente pela aplicação da Bitdefender Central 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:
  - Antivírus Bitdefender para Mac
  - A linha de produtos da Bitdefender para Windows
  - 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.

## 7.1. 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:

- Na interface principal do Bitdefender Antivirus para Mac:

1. Clique na hiperligação **Ir para a sua conta** na parte inferior direita do ecrã.

- Do seu navegador Web:
  1. Abrir um navegador em qualquer dispositivo com acesso à internet.
  2. Vá para: https://central.bitdefender.com.
  3. Inicie sessão na sua conta com o seu endereço de e-mail e palavra-passe.
- No seu dispositivo Android ou iOS:
  1. Abra a aplicação da Central Bitdefender que tem instalado.

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

## 7.2. Autenticação de dois fatores

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

### 7.2.1. Ativar autenticação de dois fatores

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

Para ativar a autenticação de dois fatores:

1. Aceda à **Central da Bitdefender**.
2. Clique no ícone no lado superior direito do ecrã.
3. Clique em **Conta da Bitdefender** no menu deslizante.
4. Selecione o separador **Palavra-passe e segurança**.

5. Clique em **INICIAR**.
   Selecione uma das seguintes opções:

   - **Aplicação de autenticação** - utilize uma apliação de autenticação para gerar um código sempre que quiser aceder à sua conta Bitdefender.
     Caso queira utilizar a aplicação de autenticação, mas não tem a certeza de qual escolher, aparecerá uma lista com as aplicações de autenticação recomendadas.

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

     b. Para uniciar sessão num dispositivo Android ou iOS, utilize o seu dispositivo para digitalizar o código QR.
     Para iniciar sessão utilizando um portátil ou um 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**.

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.

## 7.3. 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.

## 7.4. 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.

### 7.4.1. 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 for Mac 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:

### 7.4.2. 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**.

### 7.4.3. 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.

## 7.5. 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 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.

## 7.6. As minhas subscrições

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

### 7.6.1. 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).

### 7.6.2. 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.

### 7.6.3. 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.

## 7.7. 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.

# 8. PERGUNTAS FREQUENTES

**Como posso experimentar o Bitdefender Antivirus for Mac antes de realizar a subscrição?**

É um novo cliente Bitdefender e gostaria de experimentar o nosso produto antes de o comprar. O período de avaliação é de 30 dias e pode continuar a utilizar o produto instalado apenas se comprar uma subscrição Bitdefender. Para avaliar o Bitdefender Antivirus for Mac, precisa de:

1. Criar uma conta Bitdefender seguindo os seguintes passos:
   a. Vá para: https://central.bitdefender.com.
   b. Digite as informações solicitadas nos campos correspondentes. Os dados que nos fornecer serão mantidos confidenciais.
   c. 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.
   d. Clique em **CRIAR CONTA**.

2. Tranfira o Bitdefender Antivirus for Mac seguindo as instruções abaixo:
   a. Selecione os **Meus dispositivos** painel e, em seguida, clique em **INSTALAR PROTEÇÃO**.
   b. Escolha uma das duas opções disponíveis:
      - **Proteger este dispositivo**
        i. Selecione esta opção e, em seguida, selecione o proprietário do dispositivo. Se o dispositivo pertencer a outra pessoa, clique no botão correspondente.
        ii. Salve o arquivo de instalação.
      - **Proteger outros dispositivos**
        i. Selecione esta opção e, em seguida, selecione o proprietário do dispositivo. Se o dispositivo pertencer a outra pessoa, clique no botão correspondente.
        ii. Clique **ENVIAR LINK DE DOWNLOAD**.

iii. 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.

iv. 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.

c. Execute o produto Bitdefender que você baixou.

**Tenho um código de ativação. Como adiciono a sua validade à minha subscrição?**

Se você comprou um código de ativação de um de nossos revendedores ou o recebeu de presente, pode adicionar sua disponibilidade à sua assinatura do Bitdefender.

Para ativar uma assinatura usando um código de ativação, siga estas etapas:

1. Acesso Bitdefender Central.
2. Selecione os **Minhas assinaturas** painel.
3. Clique no **CÓDIGO DE ATIVAÇÃO** botão e digite o código no campo correspondente.
4. Clique **ATIVAR** continuar.

A extensão agora é visível na sua conta da Bitdefender, e no seu produto Bitdefender Antivirus para Mac instalado, na parte inferior direita do ecrã.

**O registo de análise indica que ainda há itens não resolvidos. Como os removo?**

Os itens não resolvidos no registo de análise podem ser:

- ficheiros de acesso restrito (xar, rar, etc.)
  **Solução:** Utilize a opção {3}Revelar no Finder{4} para encontrar o ficheiro e apagá-lo manualmente. Certifique-se de esvaziar a Lixeira.
- caixas de correio de acesso restrito (Thunderbird, etc.)
  **Solução:** utilize a aplicação para remover a entrada que contém o ficheiro infetado.

- O conteúdo nas cópias
  **Solução:** Ative a opção **Não verificar o conteúdo nas cópias de segurança** nas Preferências de Proteção ou **Adicione a Exceções** os os ficheiros detetados.
  Se os ficheiros infetados forem restaurados posteriormente, o Bitdefender Antivirus for Mac os detetará automaticamente e tomará a ação necessária.

> **Observação**
> Ficheiros de acesso restrito significam que o Bitdefender Antivirus for Mac só os pode abrir, mas não pode modificá-los.

**Onde posso ver detalhes sobre a atividade do produto?**

O Bitdefender mantém um registo de todas as ações importantes, mudanças de estado e outras mensagens críticas relacionadas com a sua atividade. Para aceder a essas informações, clique em **Notificações** no menu de navegação na interface da Bitdefender.

**Posso atualizar o Bitdefender Antivirus for Mac através de um servidor proxy?**

O Bitdefender Antivirus for Mac pode atualizar apenas através de servidores proxy que não requerem autenticação. Você não precisa definir nenhuma configuração do programa.

Se você se conectar à Internet por meio de um servidor proxy que exija autenticação, deverá alternar para uma conexão direta à Internet regularmente para obter atualizações de informações sobre ameaças.

**Como faço para remover o Bitdefender Antivirus para Mac?**

Para remover o Bitdefender Antivirus for Mac, siga estes passos:

1. Abra uma janela **Finder** e aceda à pasta Aplicações.
2. Abra a pasta da Bitdefender e depois clique duas vezes em Desinstalador Bitdefender.
3. Clique **Desinstalar** e aguarde a conclusão do processo.
4. Clique **Fechar** terminar.

**Importante**
Se houver um erro, você pode entrar em contato com o Atendimento ao Cliente da Bitdefender conforme descrito em Pedir Ajuda (página 53).

**Como removo as extensões do TrafficLight do meu browser?**

- Para remover as extensões do TrafficLight do Mozilla Firefox, siga estes passos:
  1. Vá para **Ferramentas** e selecione **Add-ons**.
  2. Selecione **Extensões** na coluna da esquerda.
  3. Selecione a extensão e clique em **Remover**.
  4. Reinicie o browser para concluir o processo de remoção.
- Para remover as extensões do TrafficLight do Google Chrome, siga estes passos:
  1. Na parte superior direita, clique em **Mais** ⋮.
  2. Vá para **Mais ferramentas** e selecione **Extensões**.
  3. Clique no ícone **Remover** 🗑 ao lado da extensão que deseja remover.
  4. Clique em **Desinstalar** para confirmar o processo de remoção.
- Para remover o Bitdefender TrafficLight do Safari, siga estes passos:
  1. Vá para **Preferências** ou pressione **Command-Comma(,)**.
  2. Selecione as **Extensões**.
     Será exibida a lista das extensões instaladas.
  3. Selecione a extensão do Bitdefender TrafficLight, e depois clique em **Desinstalar**.
  4. Clique outra vez em **Desinstalar** para confirmar a desinstalação.

**Quando devo utilizar o Bitdefender VPN?**

Tem de ter cuidado quando aceder, transferir ou enviar conteúdos na internet. Para garantir que fica em segurança enquanto navega na Web, recomendamos que utilize o Bitdefender VPN quando:

- quiser ligar-se a redes sem fios públicas

- quiser aceder a conteúdos que normalmente são restritos em áreas específicas, não importa se estiver em casa ou fora
- quiser manter os seus dados pessoais privados (nomes de utilizador, palavras-passe, informações de cartão de crédito, etc.)
- desejar esconder o seu endereço IP

**O Bitdefender VPN terá um impacto negativo na bateria do meu dispositivo?**

O Bitdefender VPN foi concebido para proteger os seus dados pessoais, esconder o seu endereço IP enquanto estiver ligado a redes sem fios não seguras e aceder a conteúdo restrito em certos países. Para evitar um consumo desnecessário de bateria do seu dispositivo, recomendamos que use o VPN apenas quando precisar, e que o desconecte quando estiver offline.

**Por que estou a deparar-me com lentidão na Internet enquanto uso o Bitdefender VPN?**

O Bitdefender VPN foi concebido para suavizar a sua experiência enquanto navega na Internet. No entanto, a lentidão pode ser causada pela sua conectividade com a internet ou pela distância do servidor ao qual está ligado. Nesse caso, se não for uma necessidade ligar a um servidor distante com respeito à sua localização (por exemplo, dos EUA ou China), recomendamos que permita ao Bitdefender VPN ligá-lo automaticamente ao servidor mais próximo, ou encontrar um servidor próximo da sua localização atual.

# 9. CONSEGUINDO AJUDA

## 9.1. 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.

## 9.2. 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.

### 9.2.1. 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/.

### 9.2.2. 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/

### 9.2.3. 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/.

## 9.3. 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 53).

https://www.bitdefender.pt/consumer/support/

### 9.3.1. Distribuidores locais

Os distribuidores locais BitDefender estão preparados para responder a quaiquer 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 de descriptografia 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 ocurrência. 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 evitarem 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 reune informação do utilizador através da ligação à Internet do utilizador sem o seu conhecimento, normalmente para propósitos de publicidade. As aplicações de spyware são tipicamente adicionadas como um elemento oculto de programas freeware ou shareware que podem ser download a partir da Internet; no entanto salientamos que a maioria das aplicações freeware ou shareware não possuem spyware. Uma vez instalado, o spyware monitoriza a actividade do utilizador na Internet e transmite essa informação em background para alguém. O spyware pode também ser capaz de obter endereços de e-mail e até mesmo palavras-passe e números de cartão de crédito.

O spyware é similar a uma ameaça Cavalo de Troia em que os utilizadores o instalam sem saberem, enquanto estão a instalar outra coisa qualquer. Uma forma comum de ser uma vítima de spyware é fazer download de determinado ficheiro peer-to-peer de produtos de swapping que se encontram actualmente disponíveis.

Para além destas questões de ética e privacidade, o spyware priva o utilizador de recursos de memória e também de largura de banda pois para enviar informação do utilizador para a fonte do spyware usa a ligação à Internet do utilizador. Por causa do spyware utilizar memória e recursos do sistema, as aplicações que estão a funcionar em background podem causar crashes no sistema ou uma grande instabilidade geral.

**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 londo de redes de computadores interconectadas com várias arquitecturas de hardware e vários sistemas operaticos. O TCP/IP ínclui padrões de como os computadores comunicam e convenções para ligar redes e conduzir o tráfego.

**Ameaça**

Um programa ou um pedaço de código que é carregado no seu computador sem o seu conhecimento e executa-se contra a sua vontade. A maioria das ameaças também se pode replicar. Todas as ameaças de computador são criadas pelo homem. Uma simples ameaça pode copiar-se várias vezes e é relativamente fácil de produzir. Mesmo uma simples ameaça é perigosa porque pode rapidamente utilizar toda memória disponível e fazer o sistema parar. O tipo de ameaça mais perigoso é aquele que é capaz de se transmitir através de uma rede ou contornando sistemas de segurança.

**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.