

# Bitdefender® **TOTAL SECURITY 2017**



**GUIA DO USUÁRIO**



## Bitdefender Total Security 2017 Guia do Usuário

Data de Publicação 05/12/2017

Copyright© 2017 Bitdefender

### Aviso Legal

Todos os direitos reservados. Nenhuma parte deste livro pode ser reproduzida ou transmitida em qualquer forma e mídia, eletrônica ou mecânica, incluindo fotocópia, gravação ou qualquer armazenamento e recuperação de informações, sem a permissão por escrito de um representante autorizado Bitdefender. Poderá ser possível a inclusão de breve citações em revisões apenas com a menção da fonte citada. O conteúdo não pode ser modificado em qualquer modo.

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

Este livro contém links para Websites de terceiros que não estão sob controle da Bitdefender, e a Bitdefender não é responsável pelo conteúdo de qualquer site acessado por link. Caso você acesse alguma página web de terceiros mencionados neste guia, será por sua conta e risco. A Bitdefender fornece esses links apenas para facilitar, e a inclusão do link não implica que a Bitdefender endosse ou aceite qualquer responsabilidade pelo conteúdo deste sites de terceiros.

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



## Índice

Sobre este guia .....	vi
1. Objetivo e público-alvo .....	vi
2. Como usar este guia .....	vi

## Total Security para PC ..... 1

1. Instalação .....	2
1.1. Preparando a instalação .....	2
1.2. Requisitos de Sistema .....	2
1.3. Instalando seu produto Bitdefender .....	4
1.3.1. Instalar da Bitdefender Central .....	4
2. Introdução .....	12
2.1. O básico .....	12
2.2. Interface Bitdefender .....	20
2.3. Bitdefender Central .....	36
2.4. Mantendo o seu Bitdefender atualizado .....	43
3. Como .....	48
3.1. Instalação .....	48
3.2. Assinaturas .....	55
3.3. Bitdefender Central .....	56
3.4. A analisar com Bitdefender .....	59
3.5. Consultor Parental .....	64
3.6. Privacidade .....	70
3.7. Ferramentas de Otimização .....	74
3.8. Informações Úteis .....	75
4. Gerenciar a sua segurança .....	84
4.1. Proteção Antivírus .....	84
4.2. Antispam .....	109
4.3. Proteção da Internet .....	118
4.4. Proteção de Dados .....	120
4.5. Criptografia de Arquivos .....	121
4.6. Vulnerabilidade .....	126
4.7. Firewall .....	133
4.8. Proteção contra Ransomware .....	141
4.9. Segurança Safepay para transações online .....	144
4.10. Proteção do Gerenciador de Senhas para suas credenciais .....	149
4.11. Consultor Parental .....	156
4.12. Dispositivo Anti-Roubo .....	167
4.13. USB Immunizer .....	170
5. Otimização do sistema .....	171
5.1. Ferramentas .....	171
5.2. Perfis .....	175
6. Resolução de Problemas .....	183
6.1. Resolvendo incidências comuns .....	183



6.2. Remover malware do seu sistema .....	207
<b>Antivirus for Mac .....</b>	<b>216</b>
<b>7. Instalação e Remoção .....</b>	<b>217</b>
7.1. Requisitos de Sistema .....	217
7.2. Instalando o Bitdefender Antivirus for Mac .....	217
7.2.1. Instalar da Bitdefender Central .....	217
7.2.2. Instalar a partir do CD/DVD .....	218
7.2.3. Processo de instalação .....	220
7.3. Removendo o Bitdefender Antivirus for Mac .....	224
<b>8. Introdução .....</b>	<b>225</b>
8.1. Sobre o Bitdefender Antivirus for Mac .....	225
8.2. Abrindo o Bitdefender Antivirus for Mac .....	225
8.3. Janela principal do aplicativo .....	225
8.4. Ícone do aplicativo no Dock .....	227
<b>9. Protegendo contra softwares maliciosos .....</b>	<b>228</b>
9.1. Melhores Práticas .....	228
9.2. Verificando seu Mac .....	229
9.3. Ligando ou desligando o Autopilot .....	230
9.4. Proteção da Máquina do Tempo .....	230
9.5. Assistente de Análise .....	232
9.6. Reparando Incidências .....	232
9.7. Proteção da Internet .....	262
9.8. ATUALIZAÇÕES .....	235
9.8.1. Solicitando uma Atualização .....	236
9.8.2. Obtendo atualizações via servidor proxy .....	236
9.8.3. Atualizar para uma nova versão .....	236
<b>10. Configurando Preferências .....</b>	<b>237</b>
10.1. Acessando as preferências .....	237
10.2. Info da conta .....	237
10.3. Preferências de proteção .....	237
10.4. Exclusões de Análise .....	239
10.5. Histórico .....	240
10.6. Quarentena .....	241
<b>11. Bitdefender Central .....</b>	<b>243</b>
11.1. Sobre Bitdefender Central .....	243
11.2. Acessando a Bitdefender Central .....	277
11.3. Minhas assinaturas .....	279
11.3.1. Ativar assinatura .....	244
11.3.2. Comprar assinatura .....	244
11.4. Meus dispositivos .....	277
11.4.1. Personalize seu dispositivo .....	245
11.4.2. Ações remotas .....	246
<b>12. Perguntas Mais Frequentes .....</b>	<b>247</b>



<b>Mobile Security para Android</b> .....	<b>251</b>
13. Recursos de Proteção .....	252
14. Introdução .....	253
15. Verificador de Malware .....	257
16. Consultor de Privacidade .....	260
17. Segurança na Web .....	262
18. Recursos Anti-Roubo .....	264
19. Bloqueio de Aplicativo .....	270
20. Relatórios .....	275
21. WearON .....	276
22. Bitdefender Central .....	277
23. Perguntas Mais Frequentes .....	281
<b>Contate-nos</b> .....	<b>286</b>
24. Solicite Ajuda .....	287
25. Recursos online .....	288
25.1. Centro de Suporte Bitdefender .....	288
25.2. Fórum de Suporte Bitdefender .....	288
25.3. Portal HOTforSecurity .....	289
26. Informação sobre contato .....	290
26.1. Endereços da Rede .....	290
26.2. Distribuidores locais .....	290
26.3. Escritórios Bitdefender .....	290
Glossário .....	293



## Sobre este guia

### 1. Objetivo e público-alvo

Sua assinatura Bitdefender Total Security 2017 pode proteger até 10 PCs, Macs, e smartphones e tablets Android diferentes. O gerenciamento dos dispositivos protegidos pode ser feito por meio de uma conta Bitdefender, que deve estar vinculada a uma assinatura ativa.

Este guia auxilia na configuração e uso dos produtos incluídos no sua assinatura : Bitdefender Total Security, Bitdefender Antivirus for Mac e Bitdefender Mobile Security & Antivirus.

Você pode aprender a configurar o Bitdefender em diferentes dispositivos para mantê-los protegidos contra todo tipo de ameaça.

### 2. Como usar este guia

Este guia foi elaborado para os três produtos incluídos no Bitdefender Total Security 2017:

- “Total Security para PC” (p. 1)

Aprenda a usar o produto nos seus PCs e laptops com Windows.

- “Antivirus for Mac” (p. 216)

Aprenda a usar o produto nos seus Macs.

- “Mobile Security para Android” (p. 251)

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

- “Contate-nos” (p. 286)

Veja onde procurar por ajuda caso algo inesperado apareça.



# **TOTAL SECURITY PARA PC**



## 1. INSTALAÇÃO

### 1.1. Preparando a instalação

Antes de instalar o Bitdefender Total Security, complete estes preparativos para assegurar que a instalação irá ocorrer normalmente:

- Assegure-se que o computador onde deseja instalar o Bitdefender tenha os requisitos mínimos de sistema. Caso o computador não atenda aos requisitos mínimos de sistema, o Bitdefender não será instalado ou caso instalado, não irá trabalhar de forma apropriada e irá causar lentidão e instabilidade. Para uma lista completa de requisitos de sistema, por favor consulte "*Requisitos de Sistema*" (p. 2).
- Efetue logon no computador utilizando uma conta de Administrador.
- Remova qualquer outro software similar do seu computador. Se algum for detectado durante o processo de instalação da Bitdefender, você será notificado para desinstalá-lo. Rodar dois programas de segurança simultaneamente pode afetar seu funcionamento e causar maiores problemas ao sistema. O Windows Defender será desativado durante a instalação.
- Desabilitar ou remover qualquer programa de firewall que possa estar rodando neste computador. Rodar dois programas de firewall simultaneamente pode afetar a operação deles e causar maiores problemas ao sistema. A Firewall do Windows será desativada durante a instalação.
- Recomenda-se que o seu computador esteja conectado à Internet durante a instalação, mesmo quando realizar a instalação a partir de um CD/DVD. Se estiverem disponíveis versões dos arquivos de aplicativos mais recentes do que as incluídas no pacote de instalação, o Bitdefender irá fazer o download e instalá-las.

### 1.2. Requisitos de Sistema

Você pode instalar o Bitdefender Total Security apenas nos computadores com os seguintes sistemas operacionais:

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





## ● Windows 10

Antes da instalação, certifique-se de que o seu computador cumpre os requisitos mínimos do sistema.



### Nota

Para saber qual é o sistema operacional Windows do seu computador e informações de hardware:

- No **Windows 7**, clique com o botão direito em **Meu Computador** na área de trabalho, depois selecione **Propriedades** no menu.
- No **Windows 8**, na tela inicial, localize **Computador** (por exemplo, você pode começar digitando "Computador" diretamente na tela inicial) e depois clique com o botão direito no seu ícone. No **Windows 8.1**, localize **Este PC**.

Selecione **Propriedades** no menu inferior. Veja a área do **Sistema** para encontrar mais informações sobre seu sistema.

- No **Windows 10**, digite **Sistema** na caixa de busca da barra de tarefas e clique no seu ícone. Veja a área do **Sistema** para encontrar mais informações sobre seu sistema.

## Requisitos mínimos do sistema

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

## Requisitos de sistema recomendados

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

## Requisitos de Software

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

- Internet Explorer 10 ou superior
- Mozilla Firefox 30 ou superior
- Google Chrome 34 ou superior



- Skype 6.3 ou superior
- Microsoft Outlook 2007 / 2010 / 2013
- Mozilla Thunderbird 14 ou superior

## 1.3. Instalando seu produto Bitdefender

Você pode instalar o Bitdefender com o disco de instalação, ou usar o instalador da internet baixado no seu computador na [Bitdefender Central](#).

Se sua aquisição cobre mais de um computador, repita o processo de instalação e ative seu produto com a mesma conta em cada computador. A conta a ser usada deve ser a mesma que contém sua assinatura ativa do Bitdefender.

### 1.3.1. Instalar da Bitdefender Central

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

Para baixar o Bitdefender Total Security na Bitdefender Central:

1. Acesse [Bitdefender Central](#).
2. Selecione o painel **Meus Dispositivos**.
3. Na janela **MEUS DISPOSITIVOS**, clique em **INSTALAR Bitdefender**.
4. Escolha uma das duas opções disponíveis:

- **DOWNLOAD**

Clique no botão e salve o arquivo de instalação.

- **Em outro dispositivo**

Selecione **Windows** para fazer download do seu produto Bitdefender e, em seguida, clique em **CONTINUAR**. Digite um endereço de e-mail no campo correspondente e clique em **ENVIAR**.

5. Espere o download ser concluído, depois execute o instalador:

### Validando a instalação

O Bitdefender primeiro verificará seu sistema para validar a instalação.



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

Se for detectado um programa antivírus incompatível ou uma versão antiga do Bitdefender, será avisado para removê-la do seu sistema. Por favor siga as instruções para remover o software do seu sistema, evitando assim que ocorram problemas mais tarde. Pode ser preciso reiniciar o seu computador para concluir a remoção dos programas antivírus detectados.

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



## Nota

Fazer download dos arquivos de instalação pode demorar muito tempo, especialmente se a conexão à Internet for lenta.

Quando a instalação for validada, o assistente de instalação aparecerá. Siga estes passos para instalar o Bitdefender Total Security:

## Passo 1 – instalação do Bitdefender

A tela de instalação do Bitdefender permite que você escolha que tipo de instalação deseja fazer.

Para uma instalação totalmente livre de dificuldades, basta clicar no botão **INSTALAR**. O Bitdefender será instalado no local padrão com as definições normais e você irá diretamente para a **Etapa 3** do assistente.

Se deseja configurar a instalação, clique em **INSTALAÇÃO PERSONALIZADA**.

Três tarefas adicionais podem ser realizadas neste passo:

- Leia o Acordo de Licença de Usuário antes de iniciar a instalação. O Acordo de Licença contém os termos e condições sob os quais você pode usar o Bitdefender Total Security.

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

- Mantenha a opção **Enviar relatórios anônimos** ativada. Ao permitir esta opção, os relatórios que contêm informação sobre como você usa o produto são enviados para os servidores Bitdefender. Esta informação é essencial para melhorar o produto e pode ajudar-nos a oferecer-lhe uma experiência melhor no futuro. Note que estes relatórios não contêm dados



confidenciais, tais como seu nome ou endereço de IP e que também não serão usados para fins comerciais.

- Selecione o idioma em que deseja instalar o produto.

## Passo 2 - Personalizar definições da instalação



### Nota

Este passo apenas aparece caso tenha optado por personalizar a instalação durante o passo anterior.

As seguintes opções estão disponíveis:

#### **Caminho da Instalação**

Por padrão, o Bitdefender Total Security será instalado em C:\Arquivos de Programa\Bitdefender\Bitdefender 2017. Caso queira mudar o destino da instalação, clique em **MUDAR** e selecione a pasta na qual deseja que o Bitdefender seja instalado.

#### **Configurar Definições de Proxy**

O Bitdefender Total Security requer acesso à Internet para a ativação do produto, download de atualizações de segurança e de produto, componentes de detecção na nuvem, etc. Se você usa uma conexão proxy em vez de uma conexão direta com a internet, ative a opção correspondente e ajuste as configurações de proxy.

As definições podem ser importadas do navegador padrão ou você pode introduzi-las manualmente.

#### **Verificar o computador durante a instalação**

Desabilite essa opção se não deseja que o sistema seja verificado durante a instalação do produto Bitdefender.

Clique em **INSTALAR** para confirmar suas preferências e iniciar a instalação. Se mudar de ideia, clique no botão **VOLTAR**.

## Passo 3 - Evolução da instalação

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

As áreas críticas do seu sistema são analisadas em busca de vírus, as últimas versões dos arquivos do aplicativo são baixadas e instaladas, e os serviços do Bitdefender são iniciados. Este passo pode demorar alguns minutos.



## Passo 4 - Instalação terminada

Seu produto Bitdefender foi instalado com sucesso.

É apresentado um resumo da instalação. Se tiver sido detectado malware ativo e removido durante a instalação, pode ser necessário reiniciar o sistema. Clique em **COMEÇAR A USAR O Bitdefender** para continuar.

## Passo 5 - Introdução

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

Clique em **FINALIZAR** para acessar a interface do Bitdefender Total Security.

## Instale a partir do disco de instalação.

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

Uma tela de instalação deve ser exibida em alguns instantes. Siga as instruções para iniciar a instalação.

Se a tela de instalação não aparecer, use o Windows Explorer para procurar no diretório da raiz do disco e clique duas vezes no arquivo autorun.exe.

Se a velocidade da sua internet é baixa, ou seu sistema não está conectado à internet, clique no botão **Instalar do CD/DVD**. Nesse caso, o produto Bitdefender disponível no disco será instalado e uma versão mais nova será baixada dos servidores do Bitdefender por meio de atualizações do produto.

## Validando a instalação

O Bitdefender primeiro verificará seu sistema para validar a instalação.

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

Se for detectado um programa antivírus incompatível ou uma versão antiga do Bitdefender, será avisado para removê-la do seu sistema. Por favor siga as instruções para remover o software do seu sistema, evitando assim que ocorram problemas mais tarde. Pode ser preciso reiniciar o seu computador para concluir a remoção dos programas antivírus detectados.



## Nota

Fazer download dos arquivos de instalação pode demorar muito tempo, especialmente se a conexão à Internet for lenta.

Quando a instalação for validada, o assistente de instalação aparecerá. Siga estes passos para instalar o Bitdefender Total Security:

## Passo 1 – instalação do Bitdefender

A tela de instalação do Bitdefender permite que você escolha que tipo de instalação deseja fazer.

Para uma instalação totalmente livre de dificuldades, basta clicar no botão **INSTALAR**. O Bitdefender será instalado no local padrão com as definições normais e você irá diretamente para a **Etapa 3** do assistente.

Se deseja configurar a instalação, clique em **INSTALAÇÃO PERSONALIZADA**.

Três tarefas adicionais podem ser realizadas neste passo:

- Leia o Acordo de Licença de Usuário antes de iniciar a instalação. O Acordo de Licença contém os termos e condições sob os quais você pode usar o Bitdefender Total Security.

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

- Mantenha a opção **Enviar relatórios anônimos** ativada. Ao permitir esta opção, os relatórios que contêm informação sobre como você usa o produto são enviados para os servidores Bitdefender. Esta informação é essencial para melhorar o produto e pode ajudar-nos a oferecer-lhe uma experiência melhor no futuro. Observe que esses relatórios contêm dados não confidenciais, como seu nome ou endereço de IP, e que eles não serão usados para fins comerciais.

- Selecione o idioma em que deseja instalar o produto.

## Passo 2 - Personalizar definições da instalação



## Nota

Este passo apenas aparece caso tenha optado por personalizar a instalação durante o passo anterior.

As seguintes opções estão disponíveis:



## Caminho da Instalação

Por padrão, o Bitdefender Total Security será instalado em C:\Arquivos de Programa\Bitdefender\Bitdefender 2017\. Caso queira mudar o destino da instalação, clique em **MUDAR** e selecione a pasta na qual deseja que o Bitdefender seja instalado.

## Configurar Definições de Proxy

O Bitdefender Total Security requer acesso à Internet para a ativação do produto, download de atualizações de segurança e de produto, componentes de detecção na nuvem, etc. Se você usa uma conexão proxy em vez de uma conexão direta com a internet, ative a opção correspondente e ajuste as configurações de proxy.

As definições podem ser importadas do navegador padrão ou você pode introduzi-las manualmente.

## Verificar o computador durante a instalação

Desabilite essa opção se não deseja que o sistema seja verificado durante a instalação do produto Bitdefender.

Clique em **INSTALAR** para confirmar suas preferências e iniciar a instalação. Se mudar de ideia, clique no botão **VOLTAR**.

## Passo 3 - Evolução da instalação

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

As áreas essenciais do seu sistema são verificadas em busca de vírus e os serviços Bitdefender são iniciados. Este passo pode demorar alguns minutos.

## Passo 4 - Instalação terminada

É apresentado um resumo da instalação. Se tiver sido detectado malware ativo e removido durante a instalação, pode ser necessário reiniciar o sistema. Clique em **COMEÇAR A USAR O Bitdefender** para continuar.

## Passo 5 - conta Bitdefender

Após concluir a configuração inicial, a janela da conta Bitdefender aparece. Uma conta Bitdefender é necessária para ativar o produto e usar suas ferramentas online. Para mais informações, por favor consulte "*Bitdefender Central*" (p. 36).

Proceda de acordo com sua situação.



## Quero criar uma conta Bitdefender

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

Os dados que nos fornecer serão mantidos confidenciais.

A senha deve possuir no mínimo 8 caracteres e incluir um número.

Leia os Termos de Serviço da Bitdefender antes de continuar.



### Nota

Uma vez a conta criada, você pode usar o endereço de e-mail fornecido e a senha para fazer o login na sua conta em <https://central.bitdefender.com>.

## Já tenho uma conta Bitdefender

Clique em **Entrar** e depois digite o endereço de e-mail e a senha da sua conta Bitdefender.

Clique em **ENTRAR** para continuar.

Se você esqueceu a senha da sua conta, ou simplesmente deseja criar uma nova, clique no link **Esqueci minha senha**. Digite seu endereço de e-mail e depois clique no botão **ESQUECI A SENHA**. Confira seu e-mail e siga as instruções fornecidas para definir uma nova senha para a sua conta Bitdefender.



### Nota

Caso você já tenha uma conta MyBitdefender, pode usá-la para entrar na sua conta Bitdefender. Se você esqueceu sua senha, precisa ir primeiro em <https://my.bitdefender.com> para redefini-la. Depois, use as credenciais atualizadas para entrar na sua conta Bitdefender.

## Quero executar o login usando minha conta do Microsoft, Facebook ou Google.

Para entrar com sua conta Microsoft, Facebook ou Google:

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





## Nota

O Bitdefender não tem acesso a qualquer informação confidencial como a senha da conta que você usa para efetuar o log in, ou a informações pessoais de seus amigos e contatos.

## Etapa 6 - Ative o seu produto



## Nota

Este passo aparece se você escolheu criar uma nova conta Bitdefender durante o passo anterior, ou se você entrou usando uma conta com uma assinatura vencida.

É necessário possuir uma conexão à Internet para completar o ativação do seu produto.

Proceda conforme sua situação:

### ● Tenho um código de ativação

Neste caso, ative o produto seguindo estas etapas:

1. Digite o código de ativação no campo **Eu tenho um código de ativação** e depois clique em **CONTINUAR**.



## Nota

Você pode encontrar seu código de ativação:

- na etiqueta do CD/DVD.
- No cartão de registro do produto.
- no e-mail da sua compra on-line.

### 2. Desejo avaliar o Bitdefender

Neste caso, pode utilizar o produto durante 15 dias. Para iniciar o período de avaliação, selecione **Eu não tenho uma assinatura, quero avaliar o produto sem custos** e depois clique em **CONTINUAR**.

## Passo 7 - Introdução

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

Clique em **FINALIZAR** para acessar a interface do Bitdefender Total Security.



## 2. INTRODUÇÃO

### 2.1. O básico

Assim que instalar o Bitdefender Total Security, o seu computador fica protegido contra todos os tipos de malware (tais como vírus, spyware e cavalos de tróia) e ameaças da Internet (tais como hackers, phishing e spam).

O aplicativo usa a tecnologia Photon para melhorar a velocidade e o desempenho do processo de análise do antimalware. Ele funciona através da aprendizagem dos padrões de uso de seus aplicativos de sistema para saber o que e quando analisar, minimizando o impacto no desempenho do sistema.

Você pode ativar o **“Automático”** (p. 16) para aproveitar uma segurança completamente silenciosa sem que precise ajustar qualquer configuração. No entanto, poderá querer usufruir das definições do Bitdefender para otimizar e melhorar a sua proteção.

Sempre que seu dispositivo estiver conectado a uma rede sem fio insegura, o Bitdefender identifica e reforça a proteção para salvaguardá-lo de potenciais bisbilhoteiros e espiões. Para instruções sobre como manter seus dados pessoais seguros, por favor, acesse o **“Consultor de Segurança Wi-Fi”** (p. 130).

Enquanto você trabalha, joga ou assiste filmes, Bitdefender pode lhe oferecer uma experiência de usuário contínua, adiando as tarefas de manutenção, eliminando as interrupções e ajustando os efeitos visuais do sistema. Você pode se beneficiar de tudo isso, ativando e configurando os **“Perfis”** (p. 175).

Bitdefender tomará por si a maioria das decisões relacionadas com segurança e raramente surgirão alertas pop-up. Detalhes sobre ações tomadas e informações sobre a operação de programas estão disponíveis na janela de Notificações. Para mais informações, por favor consulte **“Notificações”** (p. 15).

De vez em quando, deve abrir o Bitdefender e corrigir as incidências existentes. Você pode ter que configurar componentes específicos do Bitdefender ou tomar ações preventivas para proteger seu computador e seus dados.



Para usar as ferramentas online do Bitdefender Total Security e gerenciar suas assinaturas e dispositivos, acesse sua conta Bitdefender. Para mais informações, por favor consulte "*Bitdefender Central*" (p. 36).

A seção "*Como*" (p. 48) é onde você irá encontrar instruções passo-a-passo sobre como realizar as tarefas mais comuns. Caso haja incidências durante o uso do Bitdefender, consulte a "*Resolvendo incidências comuns*" (p. 183) seção de possíveis soluções para os problemas mais comuns.

## Abrindo a janela do Bitdefender

Para acessar a interface principal do Bitdefender Total Security, siga os passos abaixo:

### ● No Windows 7:

1. Clique **Iniciar** e acesse **Todos os Programas**.
2. Clique em **Bitdefender 2017**.
3. Clique em **Bitdefender Total Security** ou, mais rápido, clique duas vezes no ícone do Bitdefender **B** na barra de sistema.

### ● No Windows 8 e Windows 8.1:

Localize o Bitdefender Total Security na tela inicial do Windows (por exemplo, você pode começar digitando "Bitdefender" diretamente na tela inicial) e depois clique no seu ícone. De forma alternativa, abra o aplicativo da área de trabalho, dê um clique duplo no ícone Bitdefender **B** na bandeja do sistema.

### ● No Windows 10:

Digite "Bitdefender" na caixa de busca da barra de tarefas, depois clique no seu ícone. Ou então clique duas vezes no ícone do Bitdefender **B** na área de notificação.

Para mais informações sobre a janela e ícone do Bitdefender na bandeja do sistema, por favor consulte "*Interface Bitdefender*" (p. 20).

## Corrigindo os problemas

O Bitdefender utiliza um sistema de rastreamento de problemas para detectar e lhe informar sobre os problemas que podem afetar a segurança do seu computador e dados. Por padrão, ele monitora apenas uma série de problemas considerados de suma importância. De qualquer forma você pode





configurá-lo conforme suas necessidades, escolhendo sobre quais problemas específicos você deseja ser notificado.

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

- **Questões críticas** - impedem que o Bitdefender proteja você contra malware ou represente um grande risco à segurança.
- **Incidências menores (não críticas)** - podem afetar a sua proteção num futuro próximo.

O ícone Bitdefender na **bandeja do sistema** indica incidências pendentes alterando a sua cor conforme indicado a seguir:

 Questões críticas estão afetando a segurança do seu sistema. Requerem sua atenção imediata e devem ser corrigidos assim que possível.

 Incidências não críticas estão afetando a segurança do seu sistema. Deve verificá-las e repará-las quando tiver oportunidade.

Também, se você mover o cursor do mouse sobre o ícone, um pop-up irá confirmar a existência de problemas pendentes.

Quando você abre a **interface do Bitdefender**, a área de status de segurança na barra de ferramentas superior indicará a natureza dos problemas que afetam seu sistema.

## Assistente de problemas de segurança

Para reparar problemas, siga o assistente de **Problemas de Segurança**.

1. Para abrir o assistente, faça qualquer um dos seguintes:

- Clique com o botão direito do mouse no ícone do Bitdefender na **bandeja do sistema** e selecione **Ver problemas de segurança**.
- Abra a **interface do Bitdefender** e depois clique em qualquer lugar da área de status de segurança na barra de ferramentas superior.

2. Você pode verificar as incidências que afetam a segurança do seu computador e dos dados. Todas ocorrências atuais estão selecionadas para serem corrigidas.

Se não quiser resolver uma incidência específica de imediato, limpe a caixa correspondente. Será solicitado que você especifique por quanto tempo pretende adiar a correção do problema. Escolha a opção desejada



no menu e clique em **OK**. Para deixar de monitorar a categoria de problema respectiva, escolha **Permanentemente**.

O status de incidências será alterado para **Adiado** e nenhuma ação será tomada para corrigir o problema.

3. Para reparar todas as incidências selecionadas, clique em **Reparar**. Algumas ocorrências são corrigidas imediatamente. Para outras, um assistente ajudará a corrigir

As questões que este assistente ajuda você a corrigir podem ser agrupadas em cinco categorias principais:


- **Configurações de segurança desativadas.** Tais problemas são corrigidos imediatamente, ao permitir as respectivas definições de segurança.
- **Tarefas preventivas de segurança que você precisa executar.** Ao fixar tais problemas, um assistente ajuda-o a concluir com êxito a tarefa.

## Configure o alerta de status

O Bitdefender informa quando são detectadas incidências no funcionamento dos seguintes componentes do programa:

- Antimalware
- Firewall
- Atualizar
- Segurança do Navegador

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

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



## Notificações

O Bitdefender mantém um registro detalhado dos eventos relacionados com a sua atividade no seu computador. Sempre que algo relevante para a



segurança do seu sistema ou dados acontecer, uma nova mensagem é adicionada à área de notificações do Bitdefender, de forma similar a um novo e-mail que entra na sua caixa de entrada.

As notificações são uma ferramenta importante no monitoramento e gerenciamento da proteção do seu Bitdefender. Por exemplo, você pode verificar com facilidade se a atualização foi realizada com sucesso, se algum malware ou vulnerabilidades foram encontrados no seu computador, etc. Adicionalmente, pode tomar outras ações se necessário ou alterar ações tomadas pelo Bitdefender.

Para acessar o Registro das notificações, clique no ícone  na barra lateral esquerda da **interface do Bitdefender**. Sempre que um evento ocorrer, um contador poderá ser visto no ícone .

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

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

Clique em cada aba para ver mais detalhes sobre os eventos gerados. Detalhes breves são exibidos 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. Podem ser fornecidas opções para tomar outras medidas, caso seja necessário.

Para ajudá-lo a gerenciar com facilidade os eventos registrados, a janela de notificações oferece opções para apagar ou marcar como lidos todos os eventos naquela seção.

## Automático

Para todos os usuários que desejam nada mais da sua solução de segurança do que serem protegidos sem serem incomodados, a Bitdefender Total Security foi concebida com um modo Autopilot.


No Autopilot, o Bitdefender aplica uma configuração de segurança otimizada e toma todas as decisões relacionadas à segurança por você. Isto significa que não verá pop-ups nem alertas e não terá de configurar quaisquer definições.



No modo Autopilot, o Bitdefender repara automaticamente incidências críticas, ativa e gerencia discretamente:

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

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

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



## Importante

Enquanto o Autopilot estiver ligado, em caso de modificação de alguma das definições, este será desligado.

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

## Perfis

Algumas atividades do computador, como jogos on-line ou apresentações de vídeo, requerem maior capacidade de resposta, alta performance e nenhuma interrupção do sistema. Quando seu laptop esta operando funcionando com a bateria, o melhor é que operações desnecessárias, que consomem energia, sejam adiadas até que o laptop esteja ligado a uma rede de energia.

Os Perfis do Bitdefender atribuem mais recursos do sistema para os aplicativos em execução, modificando temporariamente as configurações de proteção e ajustando a configuração do sistema. Conseqüentemente, o impacto do sistema na sua atividade é minimizado.

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

### Perfil de Trabalho

Otimiza a sua eficiência de trabalho ao identificar e ajustar as configurações de produto e de sistema.



## Perfil de Filme

Melhora os efeitos visuais e elimina as interrupções ao assistir filmes.

## Perfil de Jogo

Melhora efeitos visuais e elimina as interrupções ao jogar.

## Perfil Wi-Fi Público

Aplica configurações do produto para você se beneficiar da proteção completa enquanto está conectado a uma rede não segura.


## Perfil Modo de Bateria

Aplica configurações do produto e pausa atividades em segundo plano para economizar bateria.

## Configure a ativação automática de perfis

Para uma experiência intuitiva, você pode configurar o Bitdefender para gerenciar o seu perfil de trabalho. Neste modo, o Bitdefender detecta automaticamente a sua atividade e realiza e aplica configurações de otimização do produto.

Para permitir que o Bitdefender ative perfis:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Selecione a aba **PERFIS**.
3. Use o botão correspondente para habilitar a opção **Ativar perfis automaticamente**.


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

Para obter mais informações sobre Perfis, consulte "*Perfis*" (p. 175)

## Configurações de proteção da senha do Bitdefender

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

Para configurar a proteção por senha para os ajustes do Bitdefender:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Selecione a aba **GERAL**.






3. Ative a Proteção por senha clicando no botão correspondente.
4. Insira a senha nos dois campos, depois clique em **OK**. A senha deve conter no mínimo 8 caracteres.

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

## **Importante**

Memorize a sua senha ou guarde-a em um local seguro. Se esquecer a senha, terá de reinstalar o programa ou contactar o apoio do Bitdefender.

Para remover a proteção por senha:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Selecione a aba **GERAL**.
3. Desative a proteção por senha clicando no botão correspondente. Insira a senha, depois clique em **OK**.


## **Nota**

Para alterar a senha para o seu produto, clique no link **Alterar Senha**. Insira a sua senha, depois clique em **OK**. Na janela que aparecer, insira a nova senha que você deseja usar para restringir o acesso às configurações do Bitdefender.

## Relatórios de utilização anônimos

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

Caso você deseje parar de enviar Relatórios anônimos:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Selecione a aba **AVANÇADO**.
3. Clique no botão correspondente para desabilitar os **Relatórios de uso anônimos**.




## Ofertas especiais e notificações de produto

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

Além disso, as notificações do produto podem aparecer quando forem aplicadas mudanças no produto.

Para ativar ou desativar notificações de ofertas especiais e de produtos:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Selecione a aba **GERAL**.
3. Ative ou desative ofertas especiais e notificações de produto clicando no botão correspondente.

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

## 2.2. Interface Bitdefender

Bitdefender Total Security vai de encontro às necessidades tanto de iniciantes como de pessoas mais técnicas. Sua interface gráfica do usuário foi projetada para qualquer categoria de usuário.

Para conhecer a interface do Bitdefender, um assistente de introdução contendo detalhes sobre como interagir com o produto e como configurá-lo é exibido no lado superior esquerdo. Selecione **PRÓXIMO** para continuar sendo guiado, ou **Pular guia** para fechar o assistente.

Para ver o status do produto e realizar tarefas essenciais, o Bitdefender **ícone na bandeja do sistema** está disponível a qualquer momento.

A **janela principal** permite que você gerencie o comportamento do produto usando o **Autopilot**, realize tarefas comuns, e lhe dá acesso a informações importantes do produto. Na barra lateral esquerda, você pode acessar a sua **conta Bitdefender** e **as seções do Bitdefender** para configurações detalhadas e tarefas administrativas avançadas.

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



## Ícone da bandeja do sistema


Para gerenciar todo o produto mais rapidamente, você pode usar o ícone do Bitdefender **B** na área de notificação.



### Nota

Pode ser que o ícone do Bitdefender não esteja visível o tempo todo. Para fazer o ícone aparecer permanentemente:

#### ● No **Windows 7, Windows 8 e Windows 8.1**:

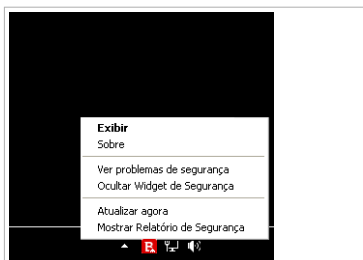
1. Clique na seta  no canto inferior direito da tela.
2. Clique **Personalizar...** para abrir a janela de ícones da Área de Notificação.
3. Selecione a opção **Mostrar ícones e notificações** para o ícone do **Agente do Bitdefender Agent**.

#### ● No **Windows 10**:

1. Clique com o botão direito na barra de tarefas e selecione **Propriedades**.
2. Clique em **Personalizar** na janela da barra de tarefas.
3. Clique no link de **Selecione quais ícones aparecem na barra de ferramentas** na janela de **Notificações e ações**.
4. Ative o botão ao lado do **Agente do Bitdefender**.

Se clicar duas vezes neste ícone, o Bitdefender irá abrir. Além disso, clicando com o botão direito do mouse no menu contextual, permitirá você gerenciar o produto Bitdefender mais rapidamente.

- **Exibir** - abre a janela principal do Bitdefender.
- **Sobre** - abre uma janela onde pode ver informação sobre o Bitdefender e onde procurar ajuda caso algo de inesperado lhe apareça.
- **Ver problemas de segurança** - ajuda-o a remover as vulnerabilidades de segurança. Se a opção não está disponível, não há problemas a serem corrigidos. Para informação detalhada, por favor consulte em **“Corrigindo os problemas”** (p. 13).







Ícone da área de notificação



- **Ocultar / Exibir Dispositivo Segurança** - ativa / desativa **Dispositivo Segurança**.
- **Atualizar agora** - realiza uma atualização imediata. Você pode acompanhar o status de atualizações no painel de Atualizações na **janela do Bitdefender**.
- **Mostrar Relatório de Segurança** - abre uma janela onde você pode visualizar o status semanal e recomendações para seu sistema. Você pode seguir as recomendações para melhorar a segurança do seu sistema.

O ícone da área de notificação do Bitdefender lhe informa quando problemas afetam seu computador ou como o produto é operado, ao mostrar um símbolo especial, como segue:

-  Problemas críticos estão afetando a segurança do seu sistema. Eles exigem atenção imediata e devem ser reparados o mais breve possível.
-  Incidências não críticas estão afetando a segurança do seu sistema. Deve verificá-las e repará-las quando tiver oportunidade.
-  O **Autopilot** Bitdefender está ativado.

Se o Bitdefender não estiver funcionando, o ícone da bandeja do sistema aparece sobre um fundo cinza: . Isso geralmente ocorre quando a assinatura expira. Isso pode ocorrer também quando os serviços do Bitdefender não estão respondendo ou quando outros erros afetam a operação normal do Bitdefender.

## Janela Principal

A tela principal do Bitdefender permite que você realize tarefas comuns, resolva problemas de segurança rapidamente, visualize informações sobre a operação do produto e acesse os painéis para alterar as configurações do produto. Tudo se encontra a apenas uns cliques de distância.

A janela é organizada em quatro áreas principais:

### Área de Estado

Aqui é onde você pode conferir o status de segurança do seu computador, executar uma atualização e configurar o **Autopilot**.

### Barra lateral esquerda

Este menu permite que você acesse e gerencie sua **conta Bitdefender** junto de outros recursos online do seu produto, ou que mude entre as três principais seções do produto. Neste menu você também pode



acessar as áreas **Notificações**, **Relatório de Segurança** semanal, Configurações gerais e **Ajuda e Suporte**.

## Botões de ação e acesso à área de módulos

Aqui você pode executar diferentes tarefas para manter seu sistema protegido e funcionando na melhor velocidade possível. Você também pode acessar os módulos do Bitdefender para configurar o produto por conta própria.

## Barra inferior

É onde você pode instalar facilmente o Bitdefender em outros dispositivos, desde que sua assinatura tenha disponibilidade.

## Área de Estado

A área de status contém os seguintes elementos:

- **Status de Segurança** no lado esquerdo da área, informa-se se há qualquer problema afetando a segurança do seu computador e o ajuda a repará-los.

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

- **A área está colorida de verde.** Não existem incidências para resolver. Seu computador e dados estão protegidos.
- **A área está colorida de amarelo.** Incidências não críticas estão afetando a segurança do seu sistema. Deve verificá-las e repará-las quando tiver oportunidade.
- **A área está colorida de vermelho.** Questões críticas estão afetando a segurança do seu sistema. Você deve resolver os problemas detectados imediatamente.

Ao clicar em qualquer lugar na área de status de segurança, você poderá cessar um assistente que irá ajudar a facilmente remover quaisquer ameaças de seu computador. Para informação detalhada, por favor consulte em **“Corrigindo os problemas”** (p. 13).

- O **Autopilot** permite que você tenha a melhor proteção e aproveite uma segurança completamente discreta. Para informação detalhada, por favor consulte em **“Automático”** (p. 16).
- **Atualizar agora** permite que você execute a atualização de um produto sempre que quiser para garantir que você tenha as assinaturas de malware










mais recentes. Para informação detalhada, por favor consulte em "*Mantendo o seu Bitdefender atualizado*" (p. 43).

- **Perfil Ativo** exibe o perfil atualmente ativo no seu produto Bitdefender. Para informação detalhada, por favor consulte em "*Perfis*" (p. 175).

## Barra lateral esquerda

Ícones sugestivos estão disponíveis no lado esquerdo da barra lateral, dando acesso à conta Bitdefender, a seções do produto, relatório de atividades, notificações, configurações gerais e suporte.

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

-  **Proteção.** Os botões de ação **Verificação Rápida** e **Verificação de Vulnerabilidades** ficam visíveis no canto inferior esquerdo na interface do Bitdefender. Além disso, informações sobre aplicações bloqueadas, ameaças detectadas e ataques ficam visíveis. Clique no link **VER MÓDULOS** para acessar a área de configuração.
-  **Privacidade.** Os botões de ação **Safepay** e **Consultor Parental** ficam visíveis no canto inferior esquerdo da interface do Bitdefender. Além disso, informações sobre carteiras e cofres de arquivos detectados são exibidas. Clique no link **VER MÓDULOS** para acessar a área de configuração.
-  **Ferramentas.** Os botões de ação **Otimizador em um clique** e **Otimizador de Inicialização** ficam visíveis no canto inferior esquerdo da interface do Bitdefender. Além disso, informações sobre o espaço otimizado são exibidas e a função **Limpeza de Disco** pode ser executada para liberar mais espaço para dados novos ao excluir arquivos e pastas grandes que você não usa mais. Além disso, a função Antifurto pode ser acessada.
-  **Atividade.** Aqui, você pode ver a atividade do produto nos últimos 30 dias e acessar o relatório de segurança que é gerado a cada sete dias.
-  **Notificações.** É possível acessar daqui as notificações geradas.
-  **Conta.** Detalhes sobre a conta Bitdefender e assinatura em uso estão disponíveis. Acesse sua conta Bitdefender para verificar suas assinaturas e realizar tarefas de segurança nos dispositivos que você controla.
-  **Configurações.** É possível acessar daqui as configurações gerais.



- **? Suporte.** Aqui é possível entrar em contato com o departamento de Suporte Técnico da Bitdefender sempre que precisar de assistência para resolver um problema com seu Bitdefender Total Security.

## Botões de ação e acesso à área de módulos

Você pode realizar tarefas importantes rapidamente usando os botões de ação. Os botões de ação se tornam visíveis no canto inferior esquerdo da interface do Bitdefender quando uma das três opções é selecionada: **Proteção**, **Privacidade** ou **Ferramentas** na barra lateral esquerda.

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

- **Quick Scan.** Execute uma verificação rápida para garantir que o computador esteja livre de malware.
- **Analisar Vulnerabilidade.** Verifique seu computador para identificar vulnerabilidades e assegurar que todos os aplicativos instalados, além do sistema operacional, estejam atualizados e funcionando corretamente.
- **Safepay.** Abra o Bitdefender Safepay™ para proteger seus dados privados ao realizar transações online.
- **Consultor Parental.** Acesse o Consultor Parental do Bitdefender para ficar informado sobre as atividades dos seus filhos.
- **Otimizador de Um Clique.** Libere espaço no disco, corrija erros de registro e proteja a sua privacidade, apagando arquivos que já não são mais úteis com um simples clique de botão.
- **Otimizador de Inicialização.** Diminua o tempo de inicialização do seu sistema impedindo a execução de aplicativos desnecessários durante a inicialização.

## Barra inferior

Para começar a proteger dispositivos adicionais:

1. Clique no link **INSTALAR EM OUTRO DISPOSITIVO**.

Você será redirecionado à página da conta Bitdefender. Assegure-se de acessar a conta com suas creden

2. Na janela que aparecer, selecione o sistema operacional desejado e clique em **CONTINUAR**.



3. Digite o endereço de e-mail para o qual devemos enviar o link de instalação da plataforma escolhida.

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

- Bitdefender Total Security em dispositivos Windows.
- Bitdefender Antivirus for Mac em dispositivos OS X.
- O Bitdefender Mobile Security ou Consultor Parental Bitdefender em dispositivos Android.

## As seções do Bitdefender

O Bitdefender vem com três seções diferentes divididas em módulos úteis para ajudá-lo a permanecer protegido enquanto trabalha, navega na internet ou deseja fazer pagamentos online, melhorar a velocidade do seu sistema e muito mais.

Sempre que você desejar acessar os módulos para uma seção específica ou para começar a configurar seu produto, clique nos seguintes ícones localizados na barra lateral da **interface do Bitdefender**:

-  **Proteção**
-  **Privacidade**
-  **Ferramentas**

## Proteção

Na seção de proteção você pode configurar seu nível de segurança, gerenciar amigos e spammers, ver e editar as configurações da conexão de rede, configurar as funções de proteção na web e contra ransomware, conferir e reparar potenciais vulnerabilidades do sistema e avaliar as conexões sem fio às quais se conecta.

Os módulos que você pode gerenciar na seção de proteção são:

### ANTIVIRUS

A proteção antivírus é a base da sua segurança. O Bitdefender protege em tempo real e a pedido contra todos os tipos de malware, tais como vírus, trojans, spyware, adware, etc.

Do módulo Antivírus, você pode acessar facilmente as seguintes tarefas de análise:





- Análise Rápida
- Análise do Sistema
- Gerenciar Verificações
- Modo de Recuperação

Para mais informações sobre tarefas de análise e como configurar a proteção antivírus, por favor consulte "*Proteção Antivírus*" (p. 84).

## PROTEÇÃO DA WEB

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

Para mais informações sobre como configurar o Bitdefender para proteger a sua atividade na rede, consulte "*Proteção da Internet*" (p. 118).

## VULNERABILIDADE

O módulo Vulnerabilidade o ajuda a manter seu sistema operacional e os aplicativos que usa regularmente atualizados, e a identificar as redes sem fio inseguras às quais se conecta.

Clique em **Verificação de Vulnerabilidades** no módulo de Vulnerabilidade para começar a identificar atualizações essenciais do Windows, atualizações de aplicativos, senhas fracas pertencentes a contas do Windows e redes sem fio não seguras.

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

Para mais informações sobre como configurar a proteção de vulnerabilidade, consulte "*Vulnerabilidade*" (p. 126).

## FIREWALL

A firewall protege você enquanto está conectado às redes e à Internet, através da filtragem de todas as tentativas de conexão.

Para mais informações sobre configuração de firewall, consulte "*Firewall*" (p. 133).

## ANTISPAM

O módulo antispam do Bitdefender assegura que a sua Caixa de Entrada permaneça livre de e-mails indesejados através da filtragem do tráfego de e-mail POP3.



Para mais informações sobre a proteção antispam, consulte "*Antispam*" (p. 109).

## PROTEÇÃO CONTRA RANSOMWARE

O módulo de Proteção contra Ransomwares protege seus arquivos pessoais contra ataques de chantagistas.

Para mais informações sobre como configurar a Proteção contra Ransomwares para proteger seu sistema contra ataques de ransomware, acesse "*Proteção contra Ransomware*" (p. 141).

## Privacidade

Na seção de privacidade, você pode criptografar seus dados privados, proteger suas transações online, manter sua navegação segura e proteger seus filhos ao restringir sua atividade online.

Os módulos que você pode gerenciar na seção de Privacidade são:

### PROTEÇÃO DE DADOS

O módulo de Proteção de dados permite que você apague arquivos permanentemente.

Clique em **Destruidor de Arquivos** na seção de Proteção de dados para iniciar um assistente que permitirá que você elimine arquivos completamente do seu sistema.

Para mais informações sobre como configurar a Proteção de Dados, consulte "*Proteção de Dados*" (p. 120).

### CARTEIRA

O Gerenciador de Senhas do Bitdefender o ajuda a lembrar as suas senhas, protege sua privacidade e fornece uma navegação segura.

No módulo Gerenciador de Senhas você pode realizar as seguintes tarefas:

- **Abrir Carteira** - abre a base de dados existente da Carteira.
- **Bloquear carteira** - bloqueia as informações existentes na Carteira.
- **Exportar Carteira** - permite que você salve a base de dados atual para um local no seu sistema.
- **Criar nova Carteira** - inicia um assistente que permite que você crie uma nova base de dados da Carteira.
- **Deletar** - permite que você delete o banco de dados da Carteira.



- **Configurações** - aqui é possível modificar o nome do seu banco de dados da Carteira e configurar para sincronizar as informações existentes com todos os seus dispositivos, ou não.

Para mais informações sobre a configuração do Gerenciador de Senhas, acesse "*Proteção do Gerenciador de Senhas para suas credenciais*" (p. 149).

## SAFEPAY

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

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

Para mais informações sobre o Bitdefender Safepay™, consulte "*Segurança Safepay para transações online*" (p. 144).

## Consultor Parental

O Consultor Parental do Bitdefender permite que você monitore o que seu filho está fazendo no computador. Caso haja conteúdo inapropriado, você pode decidir restringir o seu acesso à Internet ou a aplicativos específicos.

Clique em **Configurar** no módulo do Consultor Parental para começar a configurar os dispositivos dos seus filhos e monitorar sua atividade de onde você estiver.

Para mais informações sobre a configuração do Consultor Parental, acesse "*Consultor Parental*" (p. 156).

## ENCRIPTAÇÃO

Crie drives lógicos criptografados e protegidos por senha (ou cofres) no seu computador, onde você pode armazenar de forma segura seus documentos confidenciais e sensíveis.

Para mais informações sobre como criar partições de disco criptografadas e protegidas por senhas (ou cofres) no seu computador, consulte "*Criptografia de Arquivos*" (p. 121).

## Ferramentas

Ne seção Ferramentas, você pode melhorar a velocidade do sistema e gerenciar seus dispositivos.



## Otimização

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

No módulo de Otimização, você pode acessar uma variedade de ferramentas úteis:

- Otimizador de Um Clique
- Otimizador de Inicialização
- Limpeza de Disco

Para mais informações sobre o desempenho das ferramentas de otimização, por favor consulte "*Ferramentas*" (p. 171).

## Anti-Roubo

O Antifurto do Bitdefender protege o seu computador e os seus dados contra roubo ou perda. No caso de um evento como esse, isso permite que você localize remotamente ou bloqueie o seu computador. Você também pode apagar todos os dados presentes em seu sistema.

O Antifurto do Bitdefender oferece os seguintes recursos:

- Localização Remota
- Bloqueio Remoto
- Apagamento Remoto
- Alerta Remoto

Para mais informações sobre como você pode manter seu sistema longe de mãos erradas, consulte "*Dispositivo Anti-Roubo*" (p. 167).

## Dispositivo Segurança

**Dispositivo Segurança** é a forma rápida e fácil de controlar o Bitdefender Total Security. Adicionar este dispositivo pequeno e não intrusivo à sua área de trabalho permite ver informações críticas e realizar tarefas importantes a qualquer instante:

- abrir a janela principal do Bitdefender.
- monitorar a atividade de análise em tempo-real.
- monitorar o status de segurança do seu sistema e reparar qualquer incidência existente.
- ver quando uma atualização está em andamento.



- visualizar notificações e acessar os mais recentes eventos relatados pelo Bitdefender.
- analisar arquivos ou pastas ao arrastar e soltar um ou vários itens sobre o dispositivo.



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



Questões críticas estão afetando a segurança do seu sistema.

Requerem sua atenção imediata e devem ser corrigidos assim que possível. Clique no ícone de status para começar a reparar as incidências reportadas.



Incidências não críticas estão afetando a segurança do seu sistema. Deve verificá-las e repará-las quando tiver oportunidade. Clique no ícone de status para começar a reparar as incidências reportadas.




Seu sistema está protegido



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

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

**O lado inferior** do dispositivo exibe o contador de eventos não lidos (o número de eventos importantes reportados pelo Bitdefender, caso haja algum). Clique no contador de eventos, por exemplo  para um evento não lido, para abrir a janela de notificações. Para mais informações, por favor consulte em **“Notificações”** (p. 15).



## Analizando arquivos e pastas

Pode usar o Dispositivo de Segurança para analisar rapidamente arquivos e pastas. Arraste qualquer arquivo ou pasta que deseje analisar e solte sobre o **Dispositivo Segurança**.

O **Assistente do analisador Antivírus** aparecerá e irá lhe guiar através do processo de análise. As opções de análise estão pré-configuradas para obter os melhores resultados de detecção e não podem ser alteradas. Caso sejam detectados arquivos infectados, o Bitdefender irá tentar desinfecá-los (remover o código de malware). Se a desinfecção falhar, o assistente do Analisador Antivírus irá permitir que você especifique outras ações a serem tomadas para os arquivos infectados.

## Ocultar/exibir Dispositivo de Segurança


Quando não desejar mais visualizar o dispositivo, clique em .

Para restaurar o Dispositivo Segurança, use um dos seguintes métodos:

● Para a bandeja do sistema:

1. Clique com o botão direito no ícone do Bitdefender na **área de notificação**.
2. Clique em **Exibir Dispositivo Segurança** no menu contextual que aparece.

● A partir da interface do Bitdefender:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Selecione a aba **GERAL**.
3. Ligar **Exibir Dispositivo Segurança** clicando no botão correspondente.

O Widget de Segurança do Bitdefender é desativado por configuração padrão.

## Atividade

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

Além disso, você pode acessar o painel de **atividade** da Bitdefender Central clicando no link correspondente.



O Relatório de Segurança, que dá um status semanal para o seu produto e várias dicas para melhorar a proteção do sistema, pode ser acessado também clicando no link correspondente. Essas dicas são importantes para gerenciar a proteção geral e você poderá facilmente identificar as ações que pode tomar para seu sistema.

O relatório é gerado uma vez por semana e resume as informações relevantes sobre as atividades do seu produto, de forma que você possa entender com facilidade quais eventos ocorreram durante esse período.

A informação oferecida pelo Relatório de Segurança está dividida em três categorias:

- **Área de Proteção** - veja informações relacionadas à proteção do seu sistema.

- **Arquivos analisados**

- Permite visualizar os arquivos analisados pelo Bitdefender durante a semana. Você pode ver detalhes como o número de arquivos analisados e o número de arquivos limpos pelo Bitdefender.

- Para mais informações sobre a proteção antivírus, por favor consulte *"Proteção Antivírus"* (p. 84).

- **Páginas de Web analisadas**

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

- Para mais informações sobre a Proteção da Internet, consulte *"Proteção da Internet"* (p. 118).

- **Vulnerabilidades**

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

- Para mais informações sobre a Análise de Vulnerabilidade, por favor consulte a seção *"Vulnerabilidade"* (p. 126).

- **Linha do Tempo de Eventos**

- Permite que você tenha uma visão geral de todos os processos e problemas reparados pelo Bitdefender durante a semana. Os eventos são separados por dias.



Para mais informações sobre um registro detalhado de eventos relativos à atividade em seu computador, consulte **“Notificações”** (p. 15).

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

- **Arquivos no Cofre**

Permite visualizar quantos arquivos estão protegidos contra acesso indesejado.

Para obter maiores informações sobre como criar drives lógicos (ou cofres) protegidos por senha e criptografados em seu computador, favor consultar **“Criptografia de Arquivos”** (p. 121).

- **Área Otimização** - veja informações relacionadas ao espaço liberado, aplicações otimizadas e quanto da bateria do computador você economizou usando o perfil Modo de Bateria.

- **Espaço limpo**

Permite que você veja quanto espaço foi liberado durante o processo de otimização do sistema. O Bitdefender utiliza a Otimização para ajudar a aumentar a velocidade do seu sistema.

Para mais informações sobre a Otimização, acesse **“Ferramentas”** (p. 171).

- **Bateria economizada**

Permite que você veja quanto da bateria foi economizado enquanto o sistema era executado no perfil Modo de Bateria.

Para mais informações sobre o perfil Modo de Bateria, por favor, acesse **“Perfil Modo de Bateria”** (p. 180).

- **Aplicativos otimizados**

Permite que você veja o número de aplicativos utilizados nos Perfis.

Para mais informações sobre Perfis, consulte **“Perfis”** (p. 175).

## Verificando o Relatório de Segurança

O Relatório de Segurança utiliza um sistema rastreador de problemas para detectar e informá-lo sobre os eventos que podem afetar a segurança do seu computador e dados. As incidências detectadas incluem definições de proteção importantes que estão desligadas e outras condições que podem representar um risco à segurança. Ao utilizar o relatório, você pode configurar






componentes específicos do Bitdefender ou tomar ações preventivas para proteger o seu computador e dados privados.

Para conferir o Relatório de Segurança:

1. Acessar o relatório:

- Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.  
Clique no link **Relatório de Segurança** localizado no canto inferior direito da janela Relatório de Atividade.
- Clique com o botão direito do mouse no ícone do Bitdefender na bandeja do sistema e selecione **Mostrar Relatório de Segurança**.
- Após a conclusão de um relatório, você receberá uma notificação pop-up. Clique em **Mostrar** para acessar o relatório de atividade.  
Será aberta uma webpage no navegador onde você poderá visualizar o relatório gerado.

2. Observe a parte superior da janela para visualizar o status geral de segurança.


3. Veja as recomendações na parte inferior da página.

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

- **A área está verde.** Não existem problemas a corrigir. Seu computador e dados estão protegidos.
- **A área tem cor laranja** Há problemas não críticos afetando a segurança do seu sistema. Deve verificá-las e repará-las quando tiver oportunidade.
- **A área está vermelha.** A segurança do seu sistema está sendo afetada por problemas críticos. Você deve resolver os problemas detectados imediatamente.

## Ativar ou desativar a notificação de Relatório de Segurança

Para ligar ou desligar as notificações do Relatório de Segurança:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Selecione a aba **GERAL**.



3. Clique no botão correspondente para ativar ou desativar a notificação de Relatório de Segurança.

A notificação do Relatório de Segurança está ativada por padrão.

## 2.3. Bitdefender Central

Bitdefender Central é a plataforma virtual onde você tem acesso às funções e serviços online do produto, e pode realizar remotamente tarefas importantes nos dispositivos em que o Bitdefender estiver instalado. Você pode acessar sua conta Bitdefender de qualquer computador ou dispositivo móvel conectado à Internet visitando <https://central.bitdefender.com>. Assim que fizer login, você pode começar a fazer o seguinte:

- Fazer download e instalar o Bitdefender nos sistemas operacionais Windows, OS X e Android. Os produtos disponíveis para download são:
  - Bitdefender Total Security
  - O Antivírus Bitdefender para Mac
  - Bitdefender Mobile Security
- Controlar e renovar suas assinaturas do Bitdefender.
- Adicionar novos dispositivos à sua rede e controlar suas funções de onde quer que você esteja.
- Proteja os dispositivos de rede e seus dados contra roubo ou perda com o **Antifurto**.
- Ajuste as configurações do **Consultor Parental** dos dispositivos dos seus filhos para monitorar sua atividade de onde você estiver.
- Acesse o relatório **Atividades** para ver o status da sua assinatura e os dispositivos adicionados à sua rede, e sempre que necessário, melhorar remotamente o desempenho dos seus dispositivos com Windows.

## Acessando a Bitdefender Central

Há várias formas de acessar a Bitdefender Central. Dependendo da tarefa que você quiser realizar, você pode utilizar qualquer uma das seguintes opções:

- Na interface principal do Bitdefender:
  1. Clique no ícone ⓘ na barra lateral esquerda da **interface do Bitdefender**.



2. Selecione o link **Ir para a Central do Bitdefender**.
  3. Inicie sessão na sua conta Bitdefender com o seu endereço de e-mail e senha.
- No seu navegador da Internet:
    1. Abrir um navegador em qualquer dispositivo com acesso à Internet.
    2. Acesse: <https://central.bitdefender.com>.
    3. Inicie sessão na sua conta Bitdefender com o seu endereço de e-mail e senha.

## Minhas assinaturas

A plataforma da Bitdefender Central possibilita que você controle facilmente as assinaturas de todos os seus dispositivos.

## Verificar assinaturas disponíveis

Para verificar suas assinaturas disponíveis:

1. Acesse **Bitdefender Central**.
2. Selecione o painel **Minhas Assinaturas**.

Aqui você pode acessar informações sobre a disponibilidade das assinaturas que você possui e o número de dispositivos utilizando cada uma delas.

Você pode adicionar um novo dispositivo a uma assinatura ou renová-la selecionando um cartão de assinatura.



### Nota

É possível ter uma ou mais assinaturas em sua conta, desde que sejam para plataformas diferentes (Windows, Mac OS X, ou Android).

## Adicionar novo dispositivo

Caso sua assinatura cubra mais de um dispositivo, você pode adicionar um novo dispositivo e instalar seu Bitdefender Total Security nele, como descrito abaixo:

1. Acesse **Bitdefender Central**.
2. Selecione o painel **Meus Dispositivos**.
3. Na janela **MEUS DISPOSITIVOS**, clique em **INSTALAR Bitdefender**.



4. Escolha uma das duas opções disponíveis:

● **DOWNLOAD**

Clique no botão e salve o arquivo de instalação.

● **Em outro dispositivo**

Selecione **Windows** para fazer download do seu produto Bitdefender e, em seguida, clique em **CONTINUAR**. Digite um endereço de e-mail no campo correspondente e clique em **ENVIAR**.

5. Espere o download ser concluído, depois execute o instalador:

## Renove assinatura

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

1. Acesse **Bitdefender Central**.
2. Selecione o painel **Minhas Assinaturas**.
3. Selecione o cartão de assinatura desejado.
4. Clique em **Renovar** para continuar.

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

## Ativar assinatura

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

Caso tenha adquirido um código de ativação em um de nossos revendedores ou recebido como presente, você pode acrescentar sua disponibilidade em qualquer assinatura Bitdefender existente disponível na conta, desde que seja para o mesmo produto.

Para ativar uma assinatura usando um código de ativação:

1. Acesse **Bitdefender Central**.
2. Selecione o painel **Minhas Assinaturas**.
3. Clique no botão **CÓDIGO DE ATIVAÇÃO** e então digite o código no campo correspondente.




4. Clique em **CÓDIGO DE ATIVAÇÃO** para continuar.

A assinatura está ativada agora. Vá ao painel **Meus dispositivos** e selecione **INSTALAR o Bitdefender** para instalar o produto em um de seus dispositivos.

## Meus dispositivos


A área **Meus Dispositivos** na Bitdefender Central lhe dá a possibilidade de instalar, gerenciar e tomar ações remotas no seu produto Bitdefender em qualquer dispositivo, desde que esteja ligado e conectado à internet. Os cartões de dispositivos exibem o nome do dispositivo, o estado de sua proteção e tempo disponível da assinatura.

Para identificar facilmente seus dispositivos, você pode personalizar o nome de cada dispositivo:

1. Acesse **Bitdefender Central**.
2. Selecione o painel **Meus Dispositivos**.
3. Clique no ícone  no cartão de dispositivo desejado, e então selecione **Configurações**.
4. Altere o nome do dispositivo no campo correspondente, e então selecione **Salvar**.


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

Você pode criar e atribuir um proprietário a cada um de seus dispositivos para uma melhor gestão:

1. Acesse **Bitdefender Central**.
2. Selecione o painel **Meus Dispositivos**.
3. Clique no ícone  no cartão de dispositivo desejado, e então selecione **Perfil**.
4. Clique **Adicionar proprietário** e preencha os campos correspondentes. Defina o Sexo, Data de nascimento e selecione até uma Foto de perfil.
5. Clique em **ADICIONAR** para salvar o perfil.
6. Selecione o proprietário desejado na lista **Proprietário do dispositivo** e clique em **ATRIBUIR**.

Para atualizar o Bitdefender remotamente no seu dispositivo:



1. Acesse **Bitdefender Central**.
2. Selecione o painel **Meus Dispositivos**.
3. Clique no ícone  no cartão de dispositivo desejado, e então selecione **Atualizar**.

Para mais ações remotas e informações sobre seu produto Bitdefender em um dispositivo específico, clique no cartão de dispositivo desejado.

Quando você clicar no cartão de dispositivo, as abas a seguir aparecerão:

- **PAINEL**. Nesta janela você pode verificar o estado da proteção dos seus produtos Bitdefender e o número de dias restantes em sua assinatura. O estado da proteção pode estar verde, quando não houver problemas afetando seu dispositivo, ou vermelho quando o dispositivo estiver em risco. Quando houver problemas afetando seu produto, clique em **Visualizar incidências** para descobrir mais detalhes. Daqui você poderá resolver manualmente os problemas que afetam a segurança de seus dispositivos.
- **Proteção**. Desta janela você pode executar uma Verificação Rápida ou do Sistema em seus dispositivos remotamente. Clique no botão **VERIFICAR** para iniciar o processo. Você também pode conferir quando a última verificação foi realizada no dispositivo e acessar um relatório da última verificação, contendo as informações mais importantes. Para mais informações sobre esses dois processos de verificação, acesse **“Executando uma Análise do Sistema”** (p. 92) e **“Executar uma Análise Rápida”** (p. 92).
- **Otimizador**. Aqui você pode melhorar remotamente o desempenho de um dispositivo com a verificação, detecção e limpeza remota de arquivos inúteis. Clique no botão **INICIAR** e então selecione as áreas que você deseja otimizar. Clique no botão **INICIAR** para iniciar o processo de otimização. Clique no link **Mais detalhes** para acessar um relatório detalhado sobre os problemas reparados.

Além disso, você pode melhorar a inicialização do seu dispositivo ao identificar as aplicações que consomem muitos recursos do sistema. Clique no botão **MAIS DETALHES**, depois escolha o que deseja fazer com as aplicações detectadas. Para mais detalhes sobre essas funções, acesse **“Otimizando a velocidade do seu sistema com apenas um clique”** (p. 171) e **“Otimizando o tempo de inicialização do seu PC.”** (p. 172).



- **Anti-theft.** Caso tenha perdido seu dispositivo, ou ele tenha sido roubado, você pode localizá-lo e realizar ações remotas com a função Antifurto. Clique em **LOCALIZAR** para descobrir a localização de seu dispositivo. A última localização conhecida será exibida, com a hora e a data. Para mais detalhes sobre esta função, por favor acesse "*Dispositivo Anti-Roubo*" (p. 167).
- **Vulnerabilidade.** Para verificar um dispositivo e identificar vulnerabilidades, como a falta de atualizações do Windows, aplicativos desatualizados ou senhas fracas, clique no botão **VERIFICAR** na aba Vulnerabilidade. Vulnerabilidades não podem ser corrigidas remotamente. Caso qualquer vulnerabilidade seja descoberta, é necessário executar uma nova verificação no dispositivo e, em seguida, tomar as providências recomendadas. Clique em **Mais detalhes** para acessar um relatório detalhado sobre os problemas encontrados. Para mais detalhes sobre esta função, por favor acesse "*Vulnerabilidade*" (p. 126).

## Atividade

A área de Atividade na Bitdefender Central está disponível apenas para os usuários que têm uma assinatura Bitdefender Family Pack 2017 ou Bitdefender Total Security 2017 vinculada às suas contas. Sua função é informar como o Bitdefender protegeu nos últimos sete dias os dispositivos nos quais está instalado e exibir informações sobre a assinatura inclusa.

Ao acessar a janela **ATIVIDADE**, os seguintes cartões são disponibilizados:

- **Proteção.** Aqui, você pode ver informações sobre os arquivos, aplicativos e URLs que foram bloqueados devido a comportamentos suspeitos. Para lhe mostrar quando os problemas ocorreram, são disponibilizados gráficos exibindo os dados coletados, divididos em dias e número de ameaças detectadas. Além disso, você pode mover o mouse sobre os dados exibidos para descobrir o número de ameaças detectadas.

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

- **Otimizar.** Aqui você pode otimizar o desempenho dos dispositivos do Windows nos quais instalou o produto Bitdefender Total Security. As informações exibidas são baseadas no módulo Otimizador de Inicialização do Bitdefender, que exibe quais aplicativos estão em execução durante a inicialização do sistema e permite que você gerencie o comportamento deles nessa etapa. Dependendo das decisões tomadas pela comunidade



ao aplicar o comando **Atrasar**, somente os três primeiros dispositivos são exibidos. Clique em **Aplicar** para aplicar as alterações sugeridas no dispositivo selecionado.

Para ver as decisões de outros usuários do Bitdefender, clique no link que exibe o número de aplicativos detectados e o tempo economizado. São exibidos detalhes sobre o tempo que seu sistema precisa para se iniciar, o tempo que os aplicativos precisam na inicialização e o tempo otimizado. Selecione **ATRASAR TODOS** se deseja que os aplicativos parem de ser executados na inicialização. Para mais informações sobre o módulo Otimizador de Inicialização do Bitdefender, por favor, acesse "[Otimizando o tempo de inicialização do seu PC.](#)" (p. 172).



## Nota

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

- **Assinatura.** Aqui, você pode ver quantos dispositivos estão incluídos na sua assinatura e quantos dispositivos têm a proteção Bitdefender instalada. Para instalar o Bitdefender em outros dispositivos, clique no botão **INSTALAR** no sistema operacional desejado e siga os passos necessários.


O nome da assinatura em uso é exibido junto de um ponto colorido:

- Roxo - sua assinatura está ativa.
- Vermelho - sua assinatura está prestes a expirar. Recomendamos que você a renove o mais breve possível para continuar mantendo seus dispositivos protegidos.

Clique no link **Mais detalhes** para ser redirecionado para a página de **Assinaturas**, onde é possível ver informações detalhadas sobre a sua assinatura ativa.

## Minha Conta

Na área **Minha conta** você pode personalizar seu perfil, alterar a senha associada à sua conta, gerenciar as sessões de login e as mensagens de ajuda da Bitdefender Central.


Quando você clicar no ícone  no lado superior direito da tela, as seguintes abas aparecerão:





- **Perfil** - aqui você pode adicionar e editar informações da conta.
- **Alterar senha** - aqui você pode alterar a senha associada à sua conta.
- **Gerenciamento de sessão** - aqui você pode visualizar e gerenciar as últimas sessões inativas e ativas executadas em dispositivos associados à sua conta.
- **Configurações** - aqui você pode habilitar e desabilitar as mensagens de ajuda da Bitdefender Central e decidir se deseja ser notificado quando fotos forem tiradas nos seus dispositivos.

## Notificações

Para ajudá-lo a permanecer informado sobre o que acontece com os dispositivos associados à sua conta, disponibilizamos o ícone . Ao clicar nesse ícone, você tem uma imagem geral com informações sobre a atividade dos produtos Bitdefender instalados nos seus dispositivos.

## 2.4. Mantendo o seu Bitdefender atualizado

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

Se você se conectar a Internet através de banda-larga ou DSL, o Bitdefender se encarrega da atualização. Por padrão, o mesmo verifica se há atualizações quando você liga o computador e depois disso, a cada **hora**. Se alguma atualização for detectada, esta será automaticamente baixada e instalada em seu computador.

O processo de actualização é executado em tempo real, o que significa que os arquivos são substituídos progressivamente. Desta forma, o processo de atualização não afetará o funcionamento do produto e, ao mesmo tempo, exclui qualquer possibilidade de vulnerabilidade.



### Importante

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

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




- Se o seu computador se conectar à Internet através de um servidor proxy, você deve configurar as definições do proxy conforme escrito em **“Como posso configurar Bitdefender para usar um proxy de conexão à Internet?”** (p. 79).
- Podem ocorrer erros ao baixar atualizações com uma conexão lenta à Internet. Para saber como superar tais erros, consulte **“Como atualizar o Bitdefender numa ligação à Internet lenta”** (p. 194).
- Se você estiver conectado a Internet através de uma conexão discada, é uma boa idéia gerar o hábito de atualizar o Bitdefender a pedido do usuário. Para mais informações, por favor consulte **“Efetuar uma atualização”** (p. 44).

## Verifique se o Bitdefender está atualizado

Para conferir quando foi a última atualização do seu Bitdefender, confira o **Status de Segurança**, no lado esquerdo da área de Status.

Para informações mais detalhadas sobre as mais recentes atualizações, verifique os eventos de atualização:

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

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

## Efetuar uma atualização

Para realizar atualizações, é necessária uma conexão à Internet.

Para iniciar uma atualização, faça o seguinte:

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

O módulo Atualização irá conectar-se ao servidor de atualização de Bitdefender e verificará se existem atualizações. Se uma atualização é



detectada, poderá ser notificado para confirmar a atualização ou a mesma é realizada automaticamente, dependendo das **configurações de atualização**.




## Importante

Talvez seja necessário reiniciar o computador depois da atualização. Nós recomendamos que você o faça o mais rápido possível.


Você também pode realizar atualizações remotamente em seus dispositivos, desde que estejam ligados e conectados à Internet.

Para atualizar o Bitdefender remotamente no seu dispositivo:

1. Acesse **Bitdefender Central**.
2. Selecione o painel **Meus Dispositivos**.
3. Clique no ícone  no cartão de dispositivo desejado, e então selecione **Atualizar**.

## Ligar ou desligar a atualização automática

Para desativar a atualização automática:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Selecione a aba **ATUALIZAR**.
3. Clique no botão correspondente para ativar ou desativar a atualização automática.
4. Uma janela de alerta aparece. Você deve confirmar a sua escolha selecionando no menu por quanto tempo deseja desativar a atualização automática. Você pode desativar as atualizações automáticas por 5, 15 ou 30 minutos, por uma hora, permanentemente ou até a próxima reinicialização do sistema.



## Atenção

Esta é uma incidência de segurança crítica. Recomendamos que desative a atualização automática pelo menor tempo possível. Se o Bitdefender não for atualizado regularmente, não será capaz de protegê-lo contra as ameaças mais recentes.




## Ajuste das configurações de atualização

Atualizações podem ser feitas da rede local, pela Internet, diretamente ou por um servidor Proxy. Por padrão, o Bitdefender verificará as atualizações de hora em hora, via Internet, e instalará as que estejam disponíveis sem alertar você.

As configurações de atualização padrão são adequadas à maioria dos usuários e normalmente não precisam ser alteradas.

Para ajustar as configurações de atualização:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Selecione a aba **ATUALIZAR** e ajuste as configurações de acordo com suas preferências.

## Frequência de atualização

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

## Local de atualização

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

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

Você pode voltar para o local genérico de atualização da internet clicando em **PADRÃO**.

## Regras de processamento da atualização

Pode escolher entre três formas para baixar e instalar atualizações:

- **Atualização Silenciosa** - O Bitdefender faz download automaticamente e implementa a atualização.



- **Consultar antes do download** - sempre que uma atualização estiver disponível, você será consultado antes do download ser efetuado.
- **Avisar antes de instalar** - cada vez que uma atualização for baixada, você será consultado antes da instalação ser feita.

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

Se quiser ser avisado quando uma atualização exigir uma reinicialização, desligue a opção **Adiar reiniciar** clicando no botão correspondente.



## 3. COMO

### 3.1. Instalação

#### Como instalo o Bitdefender num segundo computador?

Se a assinatura que você comprou cobre mais de um computador, você pode usar sua conta Bitdefender para ativar um segundo PC.

Para instalar o Bitdefender em um segundo computador:

1. Clique no link **INSTALAR EM OUTRO DISPOSITIVO**.

Você será redirecionado à página da conta Bitdefender. Assegure-se de acessar a conta com suas creden

2. Na janela que aparecer, selecione o sistema operacional desejado e clique em **CONTINUAR**.
3. Digite o endereço de e-mail para o qual devemos enviar o link de instalação da plataforma escolhida.
4. Execute o Bitdefender que você baixou. Aguarde até que o processo de instalação esteja concluído e feche a janela.

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

#### Quando devo reinstalar o Bitdefender?

Em algumas situações poderá ser necessário reinstalar o seu produto Bitdefender.

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

- você reinstalou o sistema operacional.
- adquiriu um computador novo.
- deseja alterar a língua da interface do Bitdefender.

Para reinstalar o Bitdefender, você pode usar o disco de instalação que comprou ou baixar uma nova versão a partir da Bitdefender Central.

Para mais informações sobre o processo de instalação do Bitdefender, por favor consulte o *"Instalando seu produto Bitdefender"* (p. 4).



## Onde posso baixar meu produto Bitdefender?

Você pode instalar o Bitdefender do disco de instalação, ou utilizando o instalador baixado na plataforma Bitdefender Central.



### Nota

Antes de executar o kit é recomendável remover qualquer solução antivírus instalada no seu sistema. Quando utiliza mais do que uma solução de segurança no mesmo computador, o sistema torna-se instável.

Para instalar o Bitdefender da Bitdefender Central:

1. Acesse **Bitdefender Central**.
2. Selecione o painel **Meus Dispositivos**.
3. Na janela **MEUS DISPOSITIVOS**, clique em **INSTALAR Bitdefender**.
4. Escolha uma das duas opções disponíveis:

#### ● **DOWNLOAD**

Clique no botão e salve o arquivo de instalação.

#### ● **Em outro dispositivo**

Selecione **Windows** para fazer download do seu produto Bitdefender e, em seguida, clique em **CONTINUAR**. Digite um endereço de e-mail no campo correspondente e clique em **ENVIAR**.

5. Execute o Bitdefender que você baixou.

## Como posso mudar o idioma do meu produto Bitdefender?

Caso você deseje usar o Bitdefender em outro idioma, terá de reinstalar o produto com o idioma adequado.

Para usar o Bitdefender em outro idioma:

1. Remova o Bitdefender seguindo estes passos:

#### ● **No Windows 7:**


- a. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Programas e Recursos**.
- b. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
- c. Clique em **REMOVER** na janela que aparecer, depois escolha quais dados devem ser salvos para uma instalação posterior:



- Arquivos em quarentena
  - Carteiras
  - Arquivos Cofre
- d. Clique em **CONTINUAR**.
- e. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.
- No **Windows 8 e Windows 8.1**:
- a. No tela inicial do Windows, localize **Painel de Controle** (por exemplo, você pode começar digitando "Painel de Controle" diretamente na tela inicial) e depois clique no ícone.
- b. Clique em **Desinstalar um programa** ou **Programas e Recursos**.
- c. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
- d. Clique em **REMOVER** na janela que aparecer, depois escolha quais dados devem ser salvos para uma instalação posterior:
- Arquivos em quarentena
  - Carteiras
  - Arquivos Cofre
- e. Clique em **CONTINUAR**.
- f. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.
- No **Windows 10**:
- a. Clique em **Iniciar** e depois em Configurações.
- b. Clique no ícone **Sistema** na área de Configurações e então selecione **Aplicativos instalados**.
- c. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
- d. Clique em **Desinstalar** novamente para confirmar sua escolha.
- e. Clique em **REMOVER** na janela que aparecer, depois escolha quais dados devem ser salvos para uma instalação posterior:
- Arquivos em quarentena
  - Carteiras





- Arquivos Cofre
- f. Clique em **CONTINUAR**.
  - g. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.
2. Altere o idioma da Bitdefender Central:
    - a. Acesse **Bitdefender Central**.
    - b. Clique no ícone  no canto superior direito da tela.
    - c. Clique em **Minha Conta** no menu deslizante.
    - d. Selecione a aba **Perfis**.
    - e. Selecione um idioma da lista **Idioma** e depois clique em **SALVAR**.
  3. Baixe o arquivo de instalação:
    - a. Selecione o painel **Meus Dispositivos**.
    - b. Na janela **MEUS DISPOSITIVOS**, clique em **INSTALAR Bitdefender**.
    - c. Escolha uma das duas opções disponíveis:
      - **DOWNLOAD**  
Clique no botão e salve o arquivo de instalação.
      - **Em outro dispositivo**  
Selecione **Windows** para fazer download do seu produto Bitdefender e, em seguida, clique em **CONTINUAR**. Digite um endereço de e-mail no campo correspondente e clique em **ENVIAR**.
  4. Execute o Bitdefender que você baixou.

## Como utilizar minha assinatura do Bitdefender após uma atualização do Windows?

Esta situação ocorre quando você atualiza seu sistema operacional e deseja continuar utilizando sua assinatura do Bitdefender.

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

- Da versão anterior do Bitdefender Antivirus para a versão mais recente do Bitdefender Antivirus.



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

## Há duas possibilidades de caso que podem aparecer:

- Você atualizou o sistema operacional utilizando o Windows Update e você percebe que o Bitdefender não está mais funcionando.

Neste caso, será necessário reinstalar o produto usando a versão mais recente disponível.

Para resolver este problema:

1. Remova o Bitdefender seguindo estes passos:

- **No Windows 7:**

- a. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Programas e Recursos**.
- b. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
- c. Clique em **REMOVER** na janela que aparecer, depois escolha quais dados devem ser salvos para uma instalação posterior:
  - Arquivos em quarentena
  - Carteiras
  - Arquivos Cofre
- d. Clique em **CONTINUAR**.
- e. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

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

- a. No tela inicial do Windows, localize **Painel de Controle** (por exemplo, você pode começar digitando "Painel de Controle" diretamente na tela inicial) e depois clique no ícone.
- b. Clique em **Desinstalar um programa** ou **Programas e Recursos**.
- c. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
- d. Clique em **REMOVER** na janela que aparecer, depois escolha quais dados devem ser salvos para uma instalação posterior:



- Arquivos em quarentena
  - Carteiras
  - Arquivos Cofre
- e. Clique em **CONTINUAR**.
- f. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.
- **No Windows 10:**
- a. Clique em **Iniciar** e depois em Configurações.
  - b. Clique no ícone **Sistema** na área de Configurações e então selecione **Aplicativos instalados**.
  - c. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
  - d. Clique em **Desinstalar** novamente para confirmar sua escolha.
  - e. Clique em **REMOVER** na janela que aparecer, depois escolha quais dados devem ser salvos para uma instalação posterior:
    - Arquivos em quarentena
    - Carteiras
    - Arquivos Cofre
  - f. Clique em **CONTINUAR**.
  - g. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.
2. Baixe o arquivo de instalação:
- a. Acesse **Bitdefender Central**.
  - b. Selecione o painel **Meus Dispositivos**.
  - c. Na janela **MEUS DISPOSITIVOS**, clique em **INSTALAR Bitdefender**.
  - d. Escolha uma das duas opções disponíveis:
    - **DOWNLOAD**  
Clique no botão e salve o arquivo de instalação.
    - **Em outro dispositivo**



Selecione **Windows** para fazer download do seu produto Bitdefender e, em seguida, clique em **CONTINUAR**. Digite um endereço de e-mail no campo correspondente e clique em **ENVIAR**.

3. Execute o Bitdefender que você baixou.

- Você mudou seu sistema e deseja continuar usando a proteção Bitdefender.

Portanto, será necessário reinstalar o produto usando a versão mais recente.

Para resolver este problema:

1. Baixe o arquivo de instalação:

- a. Acesse **Bitdefender Central**.
- b. Selecione o painel **Meus Dispositivos**.
- c. Na janela **MEUS DISPOSITIVOS**, clique em **INSTALAR Bitdefender**.
- d. Escolha uma das duas opções disponíveis:

- **DOWNLOAD**

Clique no botão e salve o arquivo de instalação.

- **Em outro dispositivo**

Selecione **Windows** para fazer download do seu produto Bitdefender e, em seguida, clique em **CONTINUAR**. Digite um endereço de e-mail no campo correspondente e clique em **ENVIAR**.

2. Execute o Bitdefender que você baixou.

Para mais informações sobre o processo de instalação do Bitdefender, por favor consulte o *"Instalando seu produto Bitdefender"* (p. 4).

## Como posso reparar o Bitdefender?

Se deseja reparar seu Bitdefender Total Security no menu inicial do Windows:

- **No Windows 7:**

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

Isso pode levar alguns minutos.



4. Você precisa reiniciar o computador para completar esse processo.

● **No Windows 8 e Windows 8.1:**

1. No tela inicial do Windows, localize **Painel de Controle** (por exemplo, você pode começar digitando "Painel de Controle" diretamente na tela inicial) e depois clique no ícone.

2. Clique em **Desinstalar um programa** ou **Programas e Recursos**.

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

4. Clique em **REPARAR** na janela que aparece.

Isso pode levar alguns minutos.

5. Você precisa reiniciar o computador para completar esse processo.

● **No Windows 10:**

1. Clique em **Iniciar** e depois em Configurações.

2. Clique no ícone **Sistema** na área de Configurações e então selecione **Aplicativos e recursos**.

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

4. Clique em **Desinstalar** novamente para confirmar sua escolha.

5. Clique em **REPARAR**.

Isso pode levar alguns minutos.

6. Você precisa reiniciar o computador para completar esse processo.

## 3.2. Assinaturas

### Como ativo minha assinatura do Bitdefender utilizando um botão de licença?

Se você tem uma chave de licença e deseja utilizá-la para ativar uma assinatura do Bitdefender Total Security, há dois possíveis casos que podem ser aplicáveis:


● **Você atualizou uma versão anterior do Bitdefender para a mais recente:**

1. Uma vez que a atualização para o Bitdefender Total Security estiver completa, será solicitado que você acesse sua conta Bitdefender.



2. Clique em **Entrar** e depois digite o endereço de e-mail e a senha da sua conta Bitdefender.
3. Clique em **ENTRAR** para continuar.
4. Uma notificação informando que uma assinatura foi criada aparecerá na tela da sua conta. A assinatura criada será válida pelo número de dias restantes em sua chave de licença e para o mesmo número de usuários.

Dispositivos que utilizem versões anteriores do Bitdefender que estiverem registradas com a chave de licença que você converteu a uma assinatura precisam ativar o produto na mesma conta Bitdefender.

- O Bitdefender não foi instalado anteriormente no sistema:
  1. Assim que o processo de instalação estiver completo, será solicitado que você acesse sua conta Bitdefender.
  2. Clique em **Entrar** e depois digite o endereço de e-mail e a senha da sua conta Bitdefender.
  3. Clique em **ENTRAR** para continuar, e depois no botão **FINALIZAR** para acessar a interface do Bitdefender Total Security.
  4. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
  5. Selecione o link **Código de Ativação**.  
Uma nova janela aparece.
  6. Clique no link **Obtenha seu upgrade GRATUITO agora!**.
  7. Digite a sua chave de licença no campo correspondente e clique em **ATUALIZAR MEU PRODUTO**. Uma assinatura com a mesma validade e número de usuários de sua chave de licença está associada à sua conta.

## 3.3. Bitdefender Central

### Como acesso Bitdefender Central utilizando outra conta online?

Você criou uma nova conta Bitdefender e deseja utilizá-la de agora em diante. Para usar outra conta com sucesso:



1. Clique no ícone ⓘ na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **TROCAR CONTA** para mudar a conta vinculada ao computador.
3. Digite o endereço de e-mail e a senha da sua conta nos campos correspondentes, e então clique em **ENTRAR**.



## Nota

O produto Bitdefender em seu dispositivo muda automaticamente de acordo com a assinatura associada à nova conta Bitdefender.

Se não houver uma assinatura associada à nova conta Bitdefender, ou caso você deseje transferi-la da conta anterior, você pode contatar o Bitdefender para obter suporte, como descrito na seção "*Solicite Ajuda*" (p. 287).

## Como desativo as mensagens de ajuda da Bitdefender Central?

Para ajudá-lo a entender a utilidade de cada opção na Bitdefender Central, mensagens de ajuda são exibidas no painel.

Se deseja parar de ver essas mensagens:

1. Acesse **Bitdefender Central**.
2. Clique no ícone ⓘ no canto superior direito da tela.
3. Clique em **Minha Conta** no menu deslizante.
4. Selecione a aba **Configurações**.
5. Desabilite a opção **Ativar/desativar mensagens de ajuda**.

## Como paro de ver as fotos tiradas nos meus dispositivos?

Para parar a exibição de fotos tiradas nos seus dispositivos:


1. Acesse **Bitdefender Central**.
2. Clique no ícone ⓘ no canto superior direito da tela.
3. Clique em **Minha Conta** no menu deslizante.
4. Selecione a aba **Configurações**.
5. Desative a opção **Mostrar/não mostrar fotos tiradas nos seus dispositivos**.




## Esqueci a senha para a minha conta Bitdefender. Como posso redefini-la?

Há duas possibilidades para inserir uma nova senha para a sua conta Bitdefender:

● Na **interface do Bitdefender**:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **CRIAR CONTA**.  
Uma nova janela aparece.
3. Clique no link **Esqueci minha senha**.
4. Digite o endereço de e-mail usado para criar sua conta Bitdefender e depois clique no botão **ESQUECI A SENHA**.
5. Confira seu e-mail e clique no botão fornecido.
6. Digite o seu endereço de e-mail no campo respectivo.
7. Digite a nova senha. A senha deve possuir no mínimo 8 caracteres e incluir números.
8. Clique no botão **REDEFINIR SENHA**.

● A partir da sua conta Bitdefender:

1. Acesse **Bitdefender Central**.
2. Clique no ícone  no canto superior direito da tela.
3. Clique em **Minha Conta** no menu deslizante.
4. Selecione a aba **Mudar senha**.
5. Digite a senha antiga no campo **Senha antiga**.
6. Digite a nova senha que você deseja para a sua conta no campo **Nova senha**.
7. Clique no botão **MUDAR SENHA**.


Para acessar sua conta Bitdefender daqui em diante, digite seu endereço de e-mail e a senha que você acabou de definir.





## Como posso gerenciar as sessões de login associadas à minha conta Bitdefender?

Na sua conta Bitdefender você pode visualizar as últimas sessões inativas e ativas executadas em dispositivos associados à sua conta. Além disso, você pode se desconectar remotamente seguindo os seguintes passos:

1. Acesse **Bitdefender Central**.
2. Clique no ícone  no canto superior direito da tela.
3. Clique em **Minha Conta** no menu deslizante.
4. Selecione a aba **Gerenciamento de sessão**.
5. Na área **Sessões ativas**, selecione a opção **SAIR** próxima ao dispositivo em que você deseja encerrar sessão.

## 3.4. A analisar com Bitdefender

### Como posso analisar um arquivo ou uma pasta?

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

Para concluir a análise, siga o assistente de Análise Antivírus. O Bitdefender executará automaticamente as ações recomendadas nos arquivos detectados.

Se ainda houver ameaças não resolvidas, será solicitado que você escolha as ações a serem tomadas com relação às mesmas.


Situações típicas da maneira que você pode utilizar esse método de análise:

- Você suspeita que um arquivo específico ou diretório esteja infectado.
- Quando você fizer download de arquivos da internet que você achar que são perigosos.
- Analisar um compartilhamento de rede antes de copiar os arquivos para o computador.

### Como posso analisar o meu sistema?

Para realizar uma verificação completa no sistema:




1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **ANTIVÍRUS**, selecione **Verificação do Sistema**.
4. Siga as instruções do assistente de Verificação de Sistema para completar a verificação. O Bitdefender executará automaticamente as ações recomendadas nos arquivos detectados.

Se ainda houver ameaças não resolvidas, será solicitado que você escolha as ações a serem tomadas com relação às mesmas. Para mais informações, por favor consulte "**Assistente do analisador Antivírus**" (p. 96).

## Como programar uma verificação?

Você pode configurar seu produto Bitdefender para iniciar a verificação de locais importantes do sistema quando você não estiver utilizando o computador.

Para programar uma verificação:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **ANTIVÍRUS**, selecione **Gerenciar Verificações**.
4. Escolha o tipo de verificação que deseja agendar, Verificação do Sistema Completa ou Verificação Rápida, depois clique em **Opções de Verificação**.

Você também pode criar um tipo de verificação que atenda às suas necessidades clicando em **Nova tarefa personalizada**.

5. Ativar o botão **Programar**.

Escolha uma das opções correspondentes para definir uma agenda:

- No início do sistema
- Uma vez
- Periodicamente


Na janela **Verificar metas**, você pode selecionar os locais que você deseja verificar.



## Como posso criar uma tarefa de análise personalizada?

Se você deseja analisar locais específicos no seu computador ou configurar as opções de análise, configure e execute uma análise personalizada.

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

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **ANTIVÍRUS**, selecione **Gerenciar Verificações**.
4. Clique em **Nova tarefa personalizada**. Insira um nome para a análise na aba **Básico** e selecione as localizações a serem escaneadas.
5. Se quiser configurar as opções de verificação com detalhe, clique na aba **Avançado**.

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

Também pode optar por desligar o computador sempre que a análise termina, se não forem encontradas ameaças. Lembre-se de que esta será a ação padrão sempre que executar esta tarefa.

6. Clique em **OK** para guardar as alterações e fechar a janela.
7. Utilize o botão correspondente se você deseja definir um agendamento para a sua tarefa de verificação.
8. Clique em **Iniciar verificação** e siga as instruções do **assistente de verificação** para completar a verificação. Ao final da análise, será solicitado que você escolha as ações a serem tomadas nos arquivos detectados, caso haja algum.
9. Se quiser, você pode refazer rapidamente a verificação customizada anterior ao clicar na entrada correspondente na lista.

## Como posso excluir uma pasta da análise?



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

As exceções devem ser usadas pelos usuários que possuem conhecimentos avançados em informática e apenas nas seguintes situações:





- Você tem uma pasta grande no seu sistema onde guarda filmes e música.
- Você tem um arquivo grande no seu sistema onde guarda diferentes dados.
- Você mantém uma pasta onde instalar diferentes tipos de software e aplicativos para testes. A análise da pasta pode resultar na perda de alguns dados.

Para adicionar uma pasta à Lista de exclusões:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **ANTIVÍRUS**.
4. Selecione a aba **EXCLUSÕES**.
5. Clique no menu deslizável **Lista de arquivos e pastas excluídos da verificação**.
6. Clique no botão **ADD**.
7. Clique em **Buscar**, selecione a pasta que você quer excluir da verificação, depois clique em **OK**.
8. Clique em **Adicionar** para salvar as mudanças e fechar a janela.

## O que fazer se o Bitdefender identificou um arquivo limpo como infectado?



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

1. Desative a proteção antivírus em tempo real do Bitdefender:
  - a. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
  - b. Selecione o link **VER MÓDULOS**.
  - c. Selecione o ícone  no canto superior direito do módulo **ANTIVÍRUS**.
  - d. Na aba **PROTEÇÃO**, clique no botão correspondente para desativar a Verificação no acesso.

Uma janela de alerta aparece. Tem de confirmar a sua escolha seleccionando no menu durante quanto tempo pretende desactivar a



proteção em tempo real. Você pode desativar a proteção em tempo real por 5, 15 ou 30 minutos, por uma hora, permanentemente ou até a próxima reinicialização do sistema.

2. Mostrar objetos ocultos no Windows. Para saber como fazer isto, consulte [“Como posso mostrar objetos ocultos no Windows?”](#) (p. 80).
3. Restaurar o arquivo da área de Quarentena:
  - a. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
  - b. Selecione o link **VER MÓDULOS**.
  - c. Selecione o ícone  no canto superior direito do módulo **ANTIVÍRUS**.
  - d. Selecione a aba **QUARENTENA**.
  - e. Selecione o arquivo e depois clique em **RESTAURAR**.
4. Adicionar o arquivo à lista de Exceções. Para saber como fazer isto, consulte [“Como posso excluir uma pasta da análise?”](#) (p. 61).
5. Active a proteção antivírus em tempo real do Bitdefender.
6. Contate os nossos representantes do suporte para que possamos remover a assinatura de detecção. Para saber como fazer isto, consulte [“Solicite Ajuda”](#) (p. 287).


## Como posso verificar quais vírus o Bitdefender detectou?

Cada vez que uma análise é realizada, um registro de análise é criado e o Bitdefender registra as incidências detectadas.

O relatório da análise contém informação detalhada sobre os processos de análise registados, tal como as opções da análise, o alvo da análise, as ameaças encontradas e as ações tomadas sobre essas ameaças.

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

Para conferir um registro de verificação ou qualquer infecção detectada em um posteriormente:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Na aba **Todas**, selecione a notificação relacionada à última verificação.



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


3. Na lista de notificações, você pode ver quais verificações foram realizadas recentemente. Clique em uma notificação para ver seus detalhes.
4. Para abrir um registro de verificação, clique em **VER REGISTRO**.

## 3.5. Consultor Parental

### Como posso proteger os meus filhos de ameaças online?

O Consultor Parental do Bitdefender permite que você restrinja acesso à Internet e a aplicativos específicos, prevenindo que seus filhos visualizem conteúdos inapropriados quando você não estiver por perto.

Para configurar o Consultor Parental:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão de ação **Consultor Parental**.

Você será redirecionado à página da conta Bitdefender. Assegure-se de acessar a conta com suas creden

3. O painel do Consultor Parental abrirá. Aqui você poderá checar e alterar as configurações do Consultor Parental.
4. Clique em **ADICIONAR PERFIL** no lado direito da janela **MEUS FILHOS**.
5. Insira as informações específicas nos campos correspondentes, como nome, gênero e data de nascimento. Para adicionar uma foto de perfil, clique no link **Escolher arquivo**. Clique em **PRÓXIMO PASSO** para continuar.

Com base no desenvolvimento infantil, definir a idade da criança carrega automaticamente as especificações consideradas apropriadas para sua faixa etária.

6. Se o dispositivo do seu filho já tem o Bitdefender Total Security instalado, selecione o seu dispositivo na lista disponível e depois selecione a conta que deseja monitorar. Clique em **SALVAR**.

Se seu filho usa um dispositivo Android e o aplicativo do Consultor Parental Bitdefender não estiver instalado, clique em **ADICIONAR**



**DISPOSITIVO.** A opção do **Consultor Parental Bitdefender para Android** é selecionada por padrão. Clique em **PRÓXIMO PASSO** para continuar.

7. Digite o endereço de e-mail para onde devemos enviar o link de download do Consultor Parental Bitdefender e depois clique em **ENVIAR LINK DE INSTALAÇÃO**.

Em dispositivos com Windows, o Bitdefender Total Security que você incluiu em sua assinatura deverá ser baixado e instalado. Em dispositivos Android, o Agente Consultor Parental do Bitdefender deverá ser baixado e instalado.

Verifique as atividades de seus filhos e altere as configurações do Consultor Parental utilizando a conta Bitdefender desde qualquer computador ou dispositivo móvel conectado à Internet.

## Como bloqueio o acesso do meu filho a um website?

O Consultor Parental do Bitdefender permite que você controle o conteúdo acessado por seus filhos em seus dispositivos, e permite que você bloqueie acesso a determinados sites.

Para bloquear o acesso a um sítio, você precisa adicioná-lo à lista de Exceções, como abaixo:

1. Acesse: <https://central.bitdefender.com>.
2. Inicie sessão na sua conta Bitdefender com o seu endereço de e-mail e senha.
3. Clique em **Consultor Parental** para acessar o painel de controle.
4. Selecione o perfil do seu filho na janela **MEUS FILHOS**.
5. Selecione a aba **Websites**.
6. Clique no botão **GERENCIAR**.
7. Digite o endereço da página que deseja bloquear no campo correspondente.
8. Selecione **Permitir** ou **Bloquear**.
9. Clique em **FINISH** para salvar as alterações.



## Como impeço o meu filho de jogar um jogo?

O Consultor Parental do Bitdefender permite que você controle o conteúdo acessado por seus filhos enquanto utilizam o computador.

Para bloquear o acesso a um jogo:

1. Acesse: <https://central.bitdefender.com>.
2. Inicie sessão na sua conta Bitdefender com o seu endereço de e-mail e senha.
3. Clique em **Consultor Parental** para acessar o painel de controle.
4. Selecione o perfil do seu filho na janela **MEUS FILHOS**.
5. Selecione a aba **Aplicativos**.

Uma lista com cartões será exibida. Os cartões representam os aplicativos que seu filho utiliza.

6. Selecione o cartão com o aplicativo que você deseja que seu filho pare de utilizar.

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

## Como previno que meus filhos entrem em contato com pessoas não confiáveis?

O Consultor Parental do Bitdefender possibilita que você bloqueie ligações de números desconhecidos ou de amigos na lista de contatos de seu filho.

Para bloquear um contato específico em um dispositivo Android que tem o aplicativo Consultor Parental Bitdefender instalado:

1. Acesse: <https://central.bitdefender.com>.
2. Inicie sessão na sua conta Bitdefender com o seu endereço de e-mail e senha.
3. Clique em **Consultor Parental** para acessar o painel de controle.
4. Selecione o perfil da criança para qual deseja estabelecer restrições.
5. Selecione a aba **Contatos telefônicos**.

Uma lista com cartões será exibida. Os cartões representam os contatos do telefone de seu filho.





6. Selecione o cartão com o número de telefone que você deseja bloquear.

O símbolo de marcação que aparecerá indica que seu filho não receberá ligações do número de telefone selecionado.

Para bloquear um contato específico em um dispositivo com Android que não tem o aplicativo Consultor Parental Bitdefender instalado:

1. Acesse: <https://central.bitdefender.com>.
2. Inicie sessão na sua conta Bitdefender com o seu endereço de e-mail e senha.
3. Clique em **Consultor Parental** para acessar o painel de controle.
4. Selecione o perfil da criança para qual deseja estabelecer restrições.
5. Clique no link **Instalar o Consultor Parental em um dispositivo** no cartão desejado.
6. Clique em **ADICIONAR DISPOSITIVO** na janela que aparece.
7. A opção do **Consultor Parental Bitdefender para Android** é selecionada por padrão. Selecione a aba **Localização do seu filho**.
8. Selecione a aba **Contatos telefônicos**.

Uma lista com cartões será exibida. Os cartões representam os contatos do telefone de seu filho.

9. Selecione o cartão com o número de telefone que você deseja bloquear.

O símbolo de marcação que aparecerá indica que seu filho não receberá ligações do número de telefone selecionado.

Para bloquear números desconhecidos, ative a opção **nenhuma interação de identificação de chamadas**.

## Como posso definir um local como seguro ou restrito para meu filho?

O Consultor Parental do Bitdefender permite que você defina um local como seguro ou restrito para seu filho.

Para determinar um local:

1. Acesse: <https://central.bitdefender.com>.
2. Inicie sessão na sua conta Bitdefender com o seu endereço de e-mail e senha.



3. Clique em **Consultor Parental** para acessar o painel de controle.
4. Selecione o perfil do seu filho na janela **MEUS FILHOS**.
5. Selecione a aba **Localização do seu filho**.
6. Clique em **Dispositivos** no quadro da janela **Localização do seu filho**.
7. Clique em **ESCOLHER DISPOSITIVOS** e então selecione o dispositivo que você deseja configurar.
8. Na janela **Áreas**, clique no botão **ADICIONAR ÁREA**.
9. Escolha o tipo de local, **SEGURO** ou **RESTRITO**.
10. Digite um nome válido para a área onde seu filho tem ou não permissão para ir.
11. Defina a distância que deverá ser utilizada para monitoramento na barra **Raio**.
12. Clique em **ADICIONAR ÁREA** para salvar suas configurações.

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

## Como bloqueio o acesso do meu filho aos dispositivos designados durante os dias de escola?

O Consultor Parental da Bitdefender lhe permite limitar o acesso do seu filho aos dispositivos designados durante as horas de escola e quando ele tiver que fazer o dever de casa.

Para configurar as restrições:

1. Acesse o painel do **Consultor Parental** na Bitdefender Central.
2. Na janela **MEUS FILHOS**, selecione o perfil do filho para o qual deseja ajustar as restrições.
3. Selecione a aba **Horário**.
4. Na área **LIMITES DIURNOS**, clique em **ESPECÍFICOS**.
5. Selecione a caixa **Limites de tempo em dias de escola**.
6. Selecione na grade os intervalos de tempo durante os quais o acesso deve ser bloqueado.



## Como bloqueio o acesso do meu filho aos dispositivos designados durante as noites em semana de aula?

O Consultor Parental da Bitdefender lhe permite limitar o acesso do seu filho aos dispositivos designados durante as noites em semana de aula.

Para configurar as restrições:

1. Acesse o painel do **Consultor Parental** na Bitdefender Central.
2. Na janela **MEUS FILHOS**, selecione o perfil do filho para o qual deseja ajustar as restrições.
3. Selecione a aba **Horário**.
4. Na área **Hora de dormir**, selecione a caixa **Noites em semana de aula**.
5. Use as setas para cima e para baixo das caixas correspondentes para estabelecer os intervalos de tempo durante os quais o acesso deve ser bloqueado.

## Como bloqueio o acesso do meu filho aos dispositivos designados durante os fins de semana?

O Consultor Parental da Bitdefender lhe permite limitar o acesso do seu filho aos dispositivos designados durante as noites e dias dos fins de semana.

Para configurar as restrições:

1. Acesse o painel do **Consultor Parental** na Bitdefender Central.
2. Na janela **MEUS FILHOS**, selecione o perfil do filho para o qual deseja ajustar as restrições.
3. Selecione a aba **Horário**.
4. Na área **HORA DE DORMIR** selecione a caixa **Noites de fim de semana**.
5. Use as setas para cima e para baixo das caixas correspondentes para estabelecer os intervalos de tempo durante os quais o acesso deve ser bloqueado.
6. Na área **LIMITES DIURNOS**, você tem as seguintes opções:
  - **CUMULATIVO**
    - a. Selecione a caixa **Limites de tempo em fins de semana**.



- b. Arraste os marcadores na escala para estabelecer por quanto tempo o acesso aos dispositivos é permitido.


## ● ESPECÍFICO

- a. Selecione a caixa **Limites de tempo em fins de semana**.
- b. Selecione na grade os intervalos de tempo durante os quais o acesso deve ser bloqueado.

Note que as configurações **CUMULATIVO** e **ESPECÍFICO** foram designadas para trabalhar separadamente.

## Como remover um perfil de criança

Se você deseja remover um perfil infantil existente:

1. Acesse: <https://central.bitdefender.com>.
2. Inicie sessão na sua conta Bitdefender com o seu endereço de e-mail e senha.
3. Clique em **Consultor Parental** para acessar o painel de controle.
4. Clique no ícone  no perfil da criança que você deseja apagar, e então selecione **Remover**.


## 3.6. Privacidade

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


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

O Bitdefender Safepay™ é um navegador projetado para proteger a informação do seu cartão de crédito, número de conta ou qualquer outro dado pessoal que você possa utilizar enquanto acessa diferentes locais on-line.

Para manter sua atividade online segura e privada:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão de ação **Safepay**.



3. Clique no ícone  para acessar o **Teclado Virtual**.




Use o **Teclado Virtual** ao digitar informações delicadas como senhas.

## O que posso fazer se meu dispositivo tiver sido roubado?

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

O Antifurto do Bitdefender permite não só que você bloqueie o dispositivo roubado, como também apague todos os dados para garantir que ele não será usado pelo ladrão.

Para acessar as funções antifurto da sua conta:

1. Acesse **Bitdefender Central**.
2. Selecione o painel **Meus Dispositivos**.
3. Na janela **MEUS DISPOSITIVOS**, selecione o dispositivo em questão.
4. Clique em **Anti-Roubo**.
5. Selecciona as características que você deseja usar
  - **LOCALIZAR** - exibir a localização de seu dispositivo no Google Maps.
  -  **Alerta** - emitir um alerta no dispositivo.
  -  **Bloquear** - bloqueia seu computador e define um código numérico PIN para desbloquear. De forma alternativa, ative a opção correspondente para permitir que o Bitdefender tire fotos da pessoa que está tentando acessar seu dispositivo.
  -  **Limpar** - apaga toda a informação do seu computador.



### Importante

Após apagar um dispositivo, todos os recursos Anti-Roubo deixam de funcionar.

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



## Como posso utilizar cofres de arquivo?

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

Ao criar um cofre de arquivos, há duas coisas importantes: o tamanho e a senha. O tamanho padrão de 100 MB deverá ser suficiente para seus documentos particulares, arquivos Excel e outros dados similares. No entanto, para vídeos ou arquivos maiores você poderá precisar de mais espaço.

Para armazenar com segurança seus arquivos ou pastas confidenciais ou sensíveis nos cofres de arquivos do Bitdefender:

### ● Crie um cofre de arquivos e defina a senha forte para ele.

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

Uma nova janela aparece. Proceder da seguinte forma:

1. Clique em **Explorar** para seleccionar a localização do cofre e guarde o cofre de arquivos sob o nome desejado.
2. Escolha a letra da drive a partir do menu. Quando o cofre é aberto, um disco virtual rotulado com a letra selecionada aparecerá em **Meu Computador**.
3. Insira a senha do cofre nos campos **Senha** e **Confirmar**.
4. Se deseja mudar o tamanho padrão (100 MB) do cofre, use as setas para cima ou para baixo na caixa **Tamanho do cofre (MB)**.
5. Clique em **Criar**.



### Nota

Ao abrir o cofre, um disco virtual aparece em **Meu Computador**. A drive tem a denominação da letra que atribuiu ao cofre.

### ● Adicione os arquivos e as pastas que deseja proteger no cofre.



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

1. Procure o arquivo de cofre .bvd.
2. Clique com o botão direito no arquivo do cofre, aponte para Cofre de Arquivos Bitdefender e selecione **Abrir**.
3. Na janela que aparecer, insira a senha, selecione uma letra de drive para dar ao cofre e clique em **OK**.

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

### ● **Mantenha o cofre sempre fechado.**

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

### ● **Certifique-se que não elimina o arquivo de cofre .bvd.**

Eliminar o arquivo também elimina o conteúdo do cofre.

Para mais informações sobre como trabalhar com cofres de arquivos, por favor consulte "*Criptografia de Arquivos*" (p. 121).

## Como removo um arquivo permanentemente com o Bitdefender?

Caso deseje remover um arquivo permanentemente do seu sistema, é necessário apagar a informação fisicamente do seu disco rígido.

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

1. Clique com o botão direito do mouse no arquivo ou pasta que deseja apagar permanentemente, aponte para o Bitdefender e selecione **Destruidor de Arquivos**.
2. Uma janela de confirmação aparecerá. Clique em **SIM, ELIMINAR** para iniciar o assistente do Destruidor de Arquivos.



Aguarde que o Bitdefender termine a destruição dos arquivos.

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

## 3.7. Ferramentas de Otimização

### Como posso melhorar o desempenho do meu sistema?

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


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

- “Otimize o desempenho do seu sistema com um único clique” (p. 74)
- “Analise o seu sistema periodicamente” (p. 74)

### Otimize o desempenho do seu sistema com um único clique

A opção Otimizador de Um Clique poupa o seu tempo quando você quer uma maneira rápida de melhorar o desempenho do sistema analisando, detectando e limpando arquivos inúteis rapidamente.

Para iniciar o processo do Otimizador em um Clique:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão de ação **Otimizador em um Clique**.
3. Deixe que o Bitdefender busque por arquivos que podem ser excluídos, depois clique no botão **OTIMIZAR** para finalizar o processo.

Para mais informações sobre como você pode melhorar a velocidade do seu computador com um único clique, consulte “**Otimizando a velocidade do seu sistema com apenas um clique**” (p. 171).

### Analise o seu sistema periodicamente

A velocidade do seu sistema e o seu comportamento geral também podem ser afetados pelo malware.






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

Recomenda-se o uso da Análise do Sistema pois a mesma analisa todos os tipos de malware que estejam ameaçando a segurança do seu sistema e também analisa dentro dos arquivos.


Para iniciar a Verificação do Sistema:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **ANTIVÍRUS**, selecione **Verificação do Sistema**.
4. Siga os passos do assistente.

## Como posso melhorar o tempo de inicialização do meu sistema?

Os aplicativos desnecessários que deixam o tempo de inicialização irritantemente mais lento quando você abre o seu PC podem ter sua abertura desativada ou adiada com o Otimizador de Inicialização, poupando assim o seu tempo.

Para usar o Otimizador de Inicialização:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão de ação **Otimizador de Inicialização**.
3. Selecione os aplicativos que você quer adiar na inicialização do sistema.

Para mais informações sobre como otimizar o tempo de inicialização do seu PC, consulte **“Otimizando o tempo de inicialização do seu PC.”** (p. 172).

## 3.8. Informações Úteis

### Como testar minha solução antivírus?

Assegure-se que seu produto Bitdefender esteja sendo executado adequadamente, recomendamos utilizar o teste Eicar.

O teste Eicar permite que você verifique sua proteção antivírus utilizando um arquivo de segurança desenvolvido para este propósito.

Para testar sua solução antivírus:



1. Baixe o teste da página web oficial da organização EICAR <http://www.eicar.org/>.
2. Clique na aba **Arquivo de Teste Anti-Malware**.
3. Clique em **Baixar** no menu do lado esquerdo.
4. A partir da **area de download utilizando o protocolo padrão http** clique no arquivo de teste **eicar.com**.
5. Você será informado que a página que está tentando acessar contém o Arquivo de Teste EICAR (não é um vírus).

Caso clique em **Compreendo os riscos, leve-me até lá assim mesmo**, o download do teste irá iniciar e um pop-up do Bitdefender irá informá-lo que um vírus foi detectado.

Clique em **Maiores Detalhes** para obter maiores informações sobre esta ação.

Caso não receba nenhum alerta de Bitdefender, recomendamos que entre em contato com Bitdefender para suporte conforme descrito na seção *"Solicite Ajuda"* (p. 287).

## Como eu posso remover o Bitdefender?

Se deseja remover seu Bitdefender Total Security:

### ● No Windows 7:

1. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Programas e Recursos**.
2. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
3. Clique em **REMOVER** na janela que aparecer, depois escolha quais dados devem ser salvos para uma instalação posterior:
  - Arquivos em quarentena
  - Carteiras
  - Arquivos Cofre
4. Clique em **CONTINUAR**.
5. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

### ● No Windows 8 e Windows 8.1:



1. No tela inicial do Windows, localize **Painel de Controle** (por exemplo, você pode começar digitando "Painel de Controle" diretamente na tela inicial) e depois clique no ícone.
  2. Clique em **Desinstalar um programa** ou **Programas e Recursos**.
  3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
  4. Clique em **REMOVER** na janela que aparecer, depois escolha quais dados devem ser salvos para uma instalação posterior:
    - Arquivos em quarentena
    - Carteiras
    - Arquivos Cofre
  5. Clique em **CONTINUAR**.
  6. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.
- No **Windows 10**:
1. Clique em **Iniciar** e depois em Configurações.
  2. Clique no ícone **Sistema** na área de Configurações e então selecione **Aplicativos instalados**.
  3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
  4. Clique em **Desinstalar** novamente para confirmar sua escolha.
  5. Clique em **REMOVER** na janela que aparecer, depois escolha quais dados devem ser salvos para uma instalação posterior:
    - Arquivos em quarentena
    - Carteiras
    - Arquivos Cofre
  6. Clique em **CONTINUAR**.
  7. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.




## Como desligo automaticamente o meu computador após a análise?

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

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

Por exemplo: você terminou de trabalhar no seu computador e deseja ir dormir. Gostaria de ter o seu sistema completamente analisado em busca de malware pelo Bitdefender.

Eis como você deve configurar Bitdefender para desligar o seu computador ao término da análise:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **ANTIVÍRUS**, selecione **Gerenciar Verificações**.
4. Na janela **GERENCIAR TAREFAS DE VERIFICAÇÃO**, clique em **Nova tarefa personalizada** para definir um nome para a verificação e selecionar os locais a serem verificados.
5. Se quiser configurar as opções de verificação com detalhe, clique na aba **Avançado**.
6. Opte por desligar o computador sempre que a análise terminar e se não forem encontradas ameaças.
7. Clique em **OK** para guardar as alterações e fechar a janela.
8. Clique no botão **Iniciar verificação** para verificar seu sistema.

Se não forem encontradas ameaças, o computador irá desligar.

Se ainda houver ameaças não resolvidas, será solicitado que você escolha as ações a serem tomadas com relação às mesmas. Para mais informações, por favor consulte "**Assistente do analisador Antivírus**" (p. 96).



## Como posso configurar Bitdefender para usar um proxy de conexão à Internet?


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



### Importante

As ligações à internet domésticas normalmente não usam um servidor proxy. Como regra de ouro, verifique e configure as definições da conexão proxy do seu programa Bitdefender quando as atualizações não funcionarem. Se o Bitdefender atualizar, ele está devidamente configurado para se conectar à Internet.

Para gerenciar as configurações de proxy:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Selecione a aba **AVANÇADO**.
3. Ative ou desative a utilização de Proxy clicando no botão.
4. Clique no link **Gerenciar proxies**.
5. Existem duas opções para definir as configurações de proxy:

- **Importar configurações de proxy do navegador padrão** - configurações de proxy do usuário atual, extraídas do navegador padrão. Caso o servidor proxy exija um nome de usuário e uma senha, você deverá inseri-los nos campos correspondentes.



### Nota

O Bitdefender pode importar as configurações de proxy dos navegadores mais populares, incluindo as versões mais recentes do Internet Explorer, Mozilla Firefox e Google Chrome.

- **Definições de proxy personalizadas** - definições de proxy que você pode configurar. As seguintes definições devem ser especificadas:
  - **Endereço** - introduza o IP do servidor proxy.
  - **Porta** - insira a porta que o Bitdefender usa para se ligar ao servidor proxy.
  - **Usuário do proxy** - digite um usuário reconhecido pelo Proxy.



- **Senha do proxy** - digite a senha válida para o usuário especificado anteriormente.

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

O Bitdefender usará as configurações de proxy disponíveis até conseguir conexão à Internet.

## Estou usando uma versão de 32 ou 64 Bit do Windows?

Para descobrir se você tem um sistema operacional de 32 bits ou 64 bits:

### ● No Windows 7:

1. Clique em **Iniciar**.
2. Localize o **Computador** no menu **Iniciar**.
3. Clique com o botão direito em **Computador** e selecione **Propriedades**.
4. Procure na seção **Sistema** a informação sobre o seu sistema.

### ● No Windows 8:

1. A partir da tela Iniciar do Windows, localize **Computador** (por exemplo, você pode começar a digitar "Computador" diretamente no menu Iniciar) e então clicar com o botão direito do mouse em seu ícone.

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

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

### ● No Windows 10:

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

## Como posso mostrar objetos ocultos no Windows?

Estes passos são úteis nos casos de malware e tiver de encontrar e remover os arquivos infectados, que poderão estar ocultos.

Siga os seguintes passos para mostrar objetos ocultos no Windows:

1. Clique em **Iniciar**, acesse **Painel de Controle**.



No **Windows 8 e Windows 8.1**: No tela inicial do Windows, localize **Painel de Controle** (por exemplo, você pode começar digitando "Painel de Controle" diretamente na tela inicial) e depois clique no ícone.

2. Selecione **Opções de Pasta**.
3. Acesse a aba **Visualizar**.
4. Selecione **Mostrar arquivos e pastas ocultos**.
5. Desmarque **Ocultar extensões nos tipos de arquivo conhecidos**.
6. Desmarque **Ocultar arquivos protegidos do sistema operativo**.
7. Clique em **Aplicar**, depois em **OK**.

No **Windows 10**:

1. Digite "Mostrar arquivos e pastas ocultos" na caixa de pesquisa da barra de tarefas e então clique no ícone correspondente.
2. Selecione **Mostrar arquivos, pastas e diretórios ocultos**.
3. Desmarque **Ocultar extensões nos tipos de arquivo conhecidos**.
4. Desmarque **Ocultar arquivos protegidos do sistema operativo**.
5. Clique em **Aplicar**, depois em **OK**.

## Como posso remover outras soluções de segurança?

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

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

Se você não removeu as outras soluções de segurança durante a instalação inicial:

### ● No **Windows 7**:

1. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Programas e Recursos**.
2. Aguarde alguns momentos até que a lista do software instalado seja apresentada.



3. Encontre o nome do programa que pretende remover e selecione **Desinstalar**.
4. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

## ● No Windows 8 e Windows 8.1:

1. No tela inicial do Windows, localize **Painel de Controle** (por exemplo, você pode começar digitando "Painel de Controle" diretamente na tela inicial) e depois clique no ícone.
2. Clique em **Desinstalar um programa** ou **Programas e Recursos**.
3. Aguarde alguns momentos até que a lista do software instalado seja apresentada.
4. Encontre o nome do programa que pretende remover e selecione **Desinstalar**.
5. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

## ● No Windows 10:

1. Clique em **Iniciar** e depois em Configurações.
2. Clique no ícone **Sistema** na área de Configurações e então selecione **Aplicativos instalados**.
3. Encontre o nome do programa que pretende remover e selecione **Desinstalar**.
4. Clique em **Desinstalar** novamente para confirmar sua escolha.
5. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

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

## Como posso reiniciar no Modo de Segurança?

O Modo de Segurança é um modo operativo de diagnóstico, utilizado principalmente para detectar e resolver problemas que estejam a afectar o funcionamento normal do Windows. As causas destes problemas vão desde a incompatibilidade de controladores a vírus que impedem o arranque normal





do Windows. No Modo de Segurança funcionam apenas algumas aplicações e o Windows só carrega os controladores básicos e os componentes mínimos do sistema operativo. É por isso que a maioria dos vírus está inactiva quando o Windows está no Modo de Segurança e podem ser facilmente removidos.

Para iniciar o Windows no Modo de Segurança:

## ● No **Windows 7**:

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

## ● No **Windows 8, Windows 8.1 e Windows 10**:

1. Execute a **Configuração do Sistema** no Windows pressionando simultaneamente as teclas **Windows + R** no seu teclado.
2. Digite **msconfig** na caixa de diálogo **Abrir**, depois clique em **OK**.
3. Selecione a aba **Inicialização do sistema**.
4. Na área **Opções de inicialização** selecione a caixa **Inicialização segura**.
5. Clique em **Rede** e depois em **OK**.
6. Clique em **OK** na janela **Configuração do Sistema**, que o informa de que o sistema precisa ser reiniciado para as mudanças serem efetivas.

Seu sistema será reiniciado no Modo de Segurança com Rede.

Para inicializar no modo normal, reverta as configurações executando novamente a **Operação do Sistema** e desmarcando a caixa **Inicialização segura**. Clique em **OK** e depois em **Reiniciar**. Espere que as novas configurações sejam aplicadas.



## 4. GERENCIAR A SUA SEGURANÇA

### 4.1. Proteção Antivírus

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

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

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



#### Importante

Para prevenir que o seu computador seja infectado por vírus, mantenha ativada a **análise no acesso**.

- **Análise a-pedido** - permite detectar e remover malware que já se encontra a residir no seu sistema. Esta é uma análise clássica iniciada pelo usuário – você escolhe qual a drive, pasta ou arquivo o Bitdefender deverá analisar, e o mesmo é analisado – a-pedido.

O Bitdefender analisa automaticamente qualquer mídia removível que esteja conectada ao computador para garantir um acesso seguro. Para mais informações, por favor consulte **“Análise automática de mídia removível”** (p. 100).

Os utilizadores avançados podem configurar as exclusões da análise se não quiserem que certos arquivos ou tipos de arquivos sejam analisados. Para mais informações, por favor consulte **“Configurar exceções da análise”** (p. 102).

Quando detecta um vírus ou outro malware, o Bitdefender irá tentar remover automaticamente o código de malware do arquivo e reconstruir o arquivo original. Esta operação é designada por desinfecção. Os arquivos que não podem ser desinfetados são movidos para a quarentena de modo a conter a infecção. Para mais informações, por favor consulte **“Gerenciar arquivos em quarentena”** (p. 105).



Se o seu computador estiver infectado com malware, por favor consulte "*Remover malware do seu sistema*" (p. 207). Para ajudá-lo a remover o malware do computador que não pode ser removido no sistema operacional Windows, o Bitdefender lhe fornece o **Modo de Recuperação**. Este é um ambiente confiável especialmente concebido para a remoção de malware, o que lhe permite inicializar o computador independentemente do Windows. Quando o computador estiver sendo executado no Modo de Recuperação, o malware do Windows fica inativo, tornando-se mais fácil a sua remoção.

Para protegê-lo contra ransomware e aplicações maliciosas e desconhecidas, o Bitdefender usa o Controle Ativo de Ameaças, uma tecnologia heurística avançada que monitora continuamente as aplicações em execução no seu sistema. O Controle Ativo de Ameaças bloqueia automaticamente aplicativos que exibam comportamentos semelhantes a malwares para impedir que danifiquem seu computador. Ocasionalmente, aplicativos legítimos podem ser bloqueados. Em tais situações, você pode configurar o Controle Ativo de Ameaças para não bloquear os mesmos aplicativos novamente criando regras de exclusão. Para saber mais, favor consultar "*Controle Ativo de Ameaças*" (p. 106).



## Análise no acesso (proteção em tempo real)

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

As predefinições da proteção em tempo real asseguram uma ótima proteção contra malware, com um impacto mínimo no desempenho do seu sistema. Pode alterar facilmente as definições da proteção em tempo real de acordo com as suas necessidades mudando para um dos níveis de proteção predefinidos. Ou, no modo avançado, pode configurar as definições de análise em detalhe criando um nível de proteção personalizado.

## Ligar ou desligar a proteção em tempo real

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

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Selecione o link **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **ANTIVÍRUS**.



4. Na janela **PROTEÇÃO** clique no botão correspondente para ativar ou desativar a Verificação no acesso.
5. Se você desejar desabilitar a proteção em tempo real, uma janela de alerta aparecerá. Tem de confirmar a sua escolha seleccionando no menu durante quanto tempo pretende desactivar a proteção em tempo real. Você pode desativar a proteção em tempo real por 5, 15 ou 30 minutos, por uma hora, permanentemente ou até a próxima reinicialização do sistema. A proteção em tempo real será ativada automaticamente quando o tempo selecionado expirar.





## Atenção

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

## Ajustar o nível de proteção em tempo real

O nível de proteção em tempo real determina as definições de análise da proteção em tempo real. Pode alterar facilmente as definições da proteção em tempo real de acordo com as suas necessidades mudando para um dos níveis de proteção predefinidos.

Para ajustar o nível de protecção em tempo real:



1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **ANTIVÍRUS**.
4. Na janela **PROTEÇÃO**, arraste o marcador na escala para determinar o nível desejado de proteção. Utilize a descrição do lado direito da escala para escolher o nível de proteção que melhor se adequa às suas necessidades de segurança.

## Configurar as definições da proteção em tempo-real

Os usuários avançados podem tirar proveito das configurações que o Bitdefender oferece. Pode configurar as definições da proteção em tempo real criando um nível de proteção personalizado.



Para configurar a proteção em tempo real:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **ANTIVÍRUS**.
4. Arraste o marcador de **Verificação no acesso** para o nível **PERSONALIZADO**.

Uma nova janela aparece.

5. Configure as definições de análise como necessário.
6. Clique em **OK** para guardar as alterações e fechar a janela.

## Informação sobre as opções de análise

Poderá achar esta informação útil:

- Se não está familiarizado com alguns dos termos, procure-os no **glossário**. Você também pode encontrar informações úteis ao pesquisar na internet.
- **Opções de análise para arquivos acessados**. Pode configurar o Bitdefender para analisar todos os arquivos ou apenas os aplicativos (arquivos de programas) acessados. A análise de todos os arquivos acessados proporciona uma maior segurança, enquanto a análise apenas das aplicações pode ser utilizada para melhorar o desempenho do sistema.

Por padrão, ambas as pastas locais e compartilhamentos de rede estão sujeitos a análise no acesso. Para um melhor desempenho do sistema, você pode excluir os locais de rede da análise no acesso.

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

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fpx; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam;



pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsn; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

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

Se decidir usar esta opção, você pode definir um tamanho limite aceitável para os arquivos analisados no acesso. Selecione a caixa correspondente e digite o tamanho máximo do arquivo (em MB).

- **Opções de verificação para e-mail e tráfego HTTP.** Para impedir que seja transferido malware para o seu computador, o Bitdefender analisa automaticamente os seguintes pontos de entrada de malware:

- e-mails recebidos e enviados
- Tráfego HTTP

Analisar o tráfego na Internet poderá abrandar um pouco a navegação, mas vai bloquear o malware proveniente da Internet, incluindo transferências "drive-by".

Embora não seja recomendado, você pode desativar a análise do antivírus de e-mail ou da internet para aumentar o desempenho do sistema. Se desactivar as respectivas opções de análise, as mensagens electrónicas e os arquivos recebidos e transferidos da Internet não serão analisados, permitindo que arquivos infectados sejam guardados no seu computador. Esta é uma ameaça grave pois a proteção em tempo real vai bloquear o malware quando os arquivos infectados forem acessados (abertos, movidos, copiados ou executados).

- **Verificar setor de boot.** Pode definir o Bitdefender para analisar os setores de saída do seu disco rígido. Este setor do disco rígido contém o código do computador necessário para iniciar o processo de reinício. Quando um vírus infecta o setor de saída, o drive pode tornar-se inacessível e você poderá não conseguir iniciar o sistema e acessar seus dados.





- **Analisar apenas arquivos novos e alterados.** Ao analisar apenas arquivos novos e modificados, pode melhorar significativamente o desempenho do seu sistema sem comprometer a sua segurança.
- **Análise de keyloggers.** Selecione esta opção para analisar o seu sistema em busca de aplicativos keylogger. Os keyloggers gravam o que você digita no seu teclado e enviam relatórios pela Internet para uma pessoa maliciosa (hacker). O hacker pode descobrir informação sensível a partir de dados roubados, tais como números de contas bancárias e senhas, e usá-las em benefício pessoal.
- **Verificar na inicialização do sistema.** Selecione a opção **Verificação de inicialização antecipada** para verificar seu sistema na inicialização assim que todos os serviços essenciais tenham sido carregados. A missão desta ferramenta é melhorar a detecção de vírus na inicialização do sistema e o tempo de inicialização do sistema.

## Ações efetuadas em malware detectado

Você poderá configurar as ações a serem realizadas pela proteção em tempo-real.

Para configurar as ações:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **ANTIVÍRUS**.
4. Arraste o marcador de **Verificação no acesso** para o nível **PERSONALIZADO**.

Uma nova janela aparece.

5. Selecione a aba **Ações** e ajuste as configurações de verificação como for necessário.
6. Clique em **OK** para guardar as alterações e fechar a janela.

As seguintes ações podem ser tomadas pela proteção em tempo-real do Bitdefender:

### Tomar medidas adequadas

Bitdefender executará as ações recomendadas dependendo do tipo de arquivo detectado:



- **Arquivos infectados.** Os arquivos detectados como infectados correspondem a uma assinatura de malware na Base de Dados de Assinaturas de Malware do Bitdefender. O Bitdefender tentará remover automaticamente o código malware do arquivo infectado e reconstruir o arquivo original. Esta operação é designada por desinfecção.

Os arquivos que não podem ser desinfetados são movidos para a quarentena de modo a conter a infecção. O arquivos em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece. Para mais informações, por favor consulte **“Gerenciar arquivos em quarentena”** (p. 105).



## Importante

Para determinados tipos de malware, a desinfecção não é possível porque o arquivo detectado é totalmente malicioso. Nestes casos, o arquivo infectado é eliminado do disco.

- **Arquivos suspeitos.** Os arquivos são detectados como suspeitos pela análise heurística. Não foi possível desinfetar os arquivos suspeitos por não estar disponível uma rotina de desinfecção. Eles serão removidos para a quarentena para evitar uma potencial infecção.

Por padrão, os arquivos da quarentena são automaticamente enviados para os Laboratórios Bitdefender para serem analisados pelos pesquisadores de malware da Bitdefender. Se a presença de malware for confirmada, é emitida uma assinatura para possibilitar a remoção do malware.

- **Arquivos que contêm arquivos infectados.**

- Os arquivos que contêm apenas arquivos infectados são eliminados automaticamente.
- Se um arquivo tiver arquivos infectados e limpos, o Bitdefender tentará eliminar os arquivos infectados desde que possa reconstruir o arquivo com os arquivos limpos. Caso a reconstrução do arquivo não seja possível, você será informado de que qualquer ação não pode ser tomada para evitar a perda de arquivos limpos.

## Mover arquivos para a quarentena

Move os arquivos detectados para a quarentena. O arquivos em quarentena não podem ser executados ou abertos; logo o risco de





infectarem o seu computador desaparece. Para mais informações, por favor consulte **“Gerenciar arquivos em quarentena”** (p. 105).



## Negar acesso

Caso um arquivo infectado seja detectado, o acesso a ele será negado.

## Restaurar configurações padrão

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

Para restaurar as definições da proteção em tempo real:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **ANTIVÍRUS**.
4. Arraste o marcador de **Verificação no acesso** para o nível **NORMAL**.

## Verificação solicitada

O objetivo principal do Bitdefender é manter seu computador livre de vírus. Isso é feito ao manter novos vírus fora de seu computador e verificar seus e-mails e novos arquivos copiados ao seu sistema.

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

A análise a-pedido está baseada em tarefas de análise. As tarefas de análise especificam as opções de análise e os objetos a serem analisados. Você pode analisar o computador sempre que desejar, executando as tarefas de análise padrão, ou as suas próprias tarefas de análise (tarefas definidas pelo usuário). Se você deseja analisar locais específicos no seu computador ou configurar as opções de análise, configure e execute uma análise personalizada.

## Procurar malware em um arquivo ou pasta

Deve analisar os arquivos e as pastas sempre que suspeitar de uma infecção. Clique com o botão direito do sobre o arquivo ou pasta que pretende analisar,





aponte para o **Bitdefender** e selecione **Analisar com o Bitdefender**. O **Assistente do analisador Antivírus** aparecerá e irá lhe guiar através do processo de análise. Ao final da análise, será solicitado que você escolha as ações a serem tomadas nos arquivos detectados, caso haja algum.

## Executar uma Análise Rápida

A Análise Rápida utiliza a análise nas nuvens para detectar malware em execução no seu sistema. Normalmente, a realização de uma Análise Rápida demora menos de um minuto e utiliza uma facção dos recursos do sistema necessários para uma análise de vírus normal.

Para realizar uma verificação rápida:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **ANTIVÍRUS**, selecione **Verificação Rápida**.
4. Siga o **assistente de Análise Antivírus** para completar a análise. O Bitdefender executará automaticamente as ações recomendadas nos arquivos detectados. Se ainda houver ameaças não resolvidas, será solicitado que você escolha as ações a serem tomadas com relação às mesmas.

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

## Executando uma Análise do Sistema

A tarefa de Análise do Sistema procura em todo o computador todos os tipos de malware que ameaçam a sua segurança, tais como vírus, spyware, adware, rootkits e outros.



### Nota

Como a **Análise do Sistema** realiza uma análise minuciosa de todo o seu computador, a mesma poderá levar algum tempo. Portanto, recomenda-se executar esta tarefa quando não estiver usando o seu computador.

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

- Certifique-se de que o Bitdefender apresente as assinaturas de malware atualizadas. Analisar o seu computador utilizando vacinas desatualizadas




pode impedir que o Bitdefender detecte novos malwares criados desde a última atualização. Para mais informações, por favor consulte *“Mantendo o seu Bitdefender atualizado”* (p. 43).

- Encerre todos os programas abertos.


Se você deseja analisar locais específicos no seu computador ou configurar as opções de análise, configure e execute uma análise personalizada. Para mais informações, por favor consulte *“Configurando uma análise personalizada”* (p. 93).

Para realizar uma verificação do sistema:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **ANTIVÍRUS**, selecione **Verificação do Sistema**.
4. Siga o **assistente de Análise Antivírus** para completar a análise. O Bitdefender executará automaticamente as ações recomendadas nos arquivos detectados. Se ainda houver ameaças não resolvidas, será solicitado que você escolha as ações a serem tomadas com relação às mesmas.

## Configurando uma análise personalizada

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

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **ANTIVÍRUS**, selecione **Gerenciar Verificações**.
4. Clique no botão **Nova tarefa personalizada**. Insira um nome para a análise na aba **Básico** e selecione as localizações a serem escaneadas.
5. Se quiser configurar as opções de verificação com detalhe, clique na aba **Avançado**. Uma nova janela aparece. Siga esses passos:
  - a. Você pode facilmente configurar as opções de análise ajustando o nível de análise. Arraste o cursor pela escala para definir o nível de análise pretendido. Utilize a descrição do lado direito da escala para escolher o nível de análise que melhor se adequa às suas necessidades.



Os usuários avançados podem tirar proveito das configurações que o Bitdefender oferece. Para configurar as opções de análise em detalhe, clique em **Personalizar**. Você encontrará informações sobre as mesmas no final desta seção.

b. Também pode configurar as seguintes opções gerais:

- **Executar a tarefa com prioridade Baixa** . Diminui a prioridade do processo de análise. Você permitirá que outros programas sejam executados mais rapidamente e aumentem o tempo de verificação.
- **Minimizar o Assistente de Análise para a área de notificação** . Minimiza a janela da análise para a **área de notificação**. Clique duplamente no ícone Bitdefender para abrir.
- Especifique a ação a aplicar se não forem encontradas ameaças.

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

6. Se deseja programar sua tarefa de verificação, use o botão **Programar** na janela **Básico**. Escolha uma das opções correspondentes para definir uma agenda:

- No início do sistema
- Uma vez
- Periodicamente

7. Clique em **Iniciar Análise** e siga o **assistente de Análise Antivírus** para completar a análise. Dependendo das localizações a serem analisadas, a análise pode demorar um pouco. Ao final da análise, será solicitado que você escolha as ações a serem tomadas nos arquivos detectados, caso haja algum.

8. Se quiser, você pode refazer rapidamente a verificação customizada anterior ao clicar na entrada correspondente na lista.

## Informação sobre as opções de análise

Poderá achar esta informação útil:

- Se não está familiarizado com alguns dos termos, procure-os no **glossário**. Você também pode encontrar informações úteis ao pesquisar na internet.
- **Verificar arquivos**. Pode configurar o Bitdefender para analisar todos os tipos de arquivos ou apenas os aplicativos (arquivos de programas). A



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

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

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



## Nota

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

- **Verificar setor de boot.** Pode definir o Bitdefender para analisar os setores de saída do seu disco rígido. Este setor do disco rígido contém o código do computador necessário para iniciar o processo de reinício. Quando um vírus infecta o setor de saída, o drive pode tornar-se inacessível e você poderá não conseguir iniciar o sistema e acessar seus dados.
- **Analisar a Memória.** Selecione esta opção para analisar programas executados na memória do seu sistema.
- **Analisar registo.** Selecione esta opção para analisar as chaves de registo. O Registo do Windows é uma base de dados que armazena as definições



de configuração e as opções para os componentes do sistema operacional Windows, bem como para os aplicativos instalados.

- **Analisar cookies.** Selecione esta opção para analisar os cookies armazenados pelos navegadores no seu computador.
- **Analisar apenas arquivos novos e alterados.** Ao analisar apenas arquivos novos e modificados, pode melhorar significativamente o desempenho do seu sistema sem comprometer a sua segurança.
- **Ignorar keyloggers comerciais.** Selecione esta opção se você tiver instalado e usar programas de controle e registro comerciais em seu computador. O programa de Controle e Registro comercial é um software legítimo de monitoramento do computador cuja função mais básica é registrar tudo o que é digitado no teclado.
- **Analisar em busca de rootkits.** Selecione esta opção para analisar **rootkits** e objetos ocultos usando tal software.

## Assistente do analisador Antivírus

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



### Nota

Se o assistente de análise não aparecer, a análise pode estar configurada para executar silenciosamente no computador, enquanto você o utiliza. Você pode visualizar o ícone **B** Progresso da análise **na área de notificação**. Você pode clicar nesse ícone para abrir a janela de análise e para visualizar o progresso da mesma.

## Passo 1 - Realizar Análise

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

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



**Parando ou suspendendo a análise.** Você pode interromper a análise no momento que quiser clicando em **PARAR**. Você irá diretamente para o último passo do assistente. Para pausar temporariamente o processo de análise, clique em **PAUSA**. Você deverá clicar em **RETOMAR** para retomar a análise.

**Arquivos comprimidos protegidos por senha.** Quando é detectado um arquivo protegido por senha, dependendo das definições da análise, poderá ter de indicar a senha. Os arquivos protegidos por senha não podem ser analisados a não ser que forneça a senha. As seguintes opções estão disponíveis:

- **Senha.** Se você deseja que o Bitdefender analise o arquivo, selecione essa opção e digite a senha. Se você não sabe a senha, escolha uma das outras opções.
- **Não solicite uma senha e não analise este objeto.** Selecione essa opção para pular a análise desse arquivo.
- **Pular todos os itens protegidos por senha.** Selecione essa opção caso não deseje ser questionado sobre arquivos protegidos por senha. O Bitdefender não será capaz de os analisar, porém um registro será mantido no relatório da análise.

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

## Passo 2 - Escolher ações

Ao final da análise, será solicitado que você escolha as ações a serem tomadas nos arquivos detectados, caso haja algum.



### Nota

Quando você realizar uma verificação rápida ou do sistema, o Bitdefender automaticamente tomará as ações recomendadas em arquivos detectados durante a verificação. Se ainda houver ameaças não resolvidas, será solicitado que você escolha as ações a serem tomadas com relação às mesmas.

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

Você pode escolher uma ação geral sendo executada para todos os problemas ou escolher ações separadas para cada grupo de problemas. Uma ou várias das seguintes opções podem aparecer no menu:



## Tomar medidas adequadas

Bitdefender executará as ações recomendadas dependendo do tipo de arquivo detectado:

- **Arquivos infectados.** Os arquivos detectados como infectados correspondem a uma assinatura de malware na Base de Dados de Assinaturas de Malware do Bitdefender. O Bitdefender tentará remover automaticamente o código malware do arquivo infectado e reconstruir o arquivo original. Esta operação é designada por desinfecção.

Os arquivos que não podem ser desinfetados são movidos para a quarentena de modo a conter a infecção. O arquivos em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece. Para mais informações, por favor consulte **“Gerenciar arquivos em quarentena”** (p. 105).



### Importante

Para determinados tipos de malware, a desinfecção não é possível porque o arquivo detectado é totalmente malicioso. Nestes casos, o arquivo infectado é eliminado do disco.

- **Arquivos suspeitos.** Os arquivos são detectados como suspeitos pela análise heurística. Não foi possível desinfetar os arquivos suspeitos por não estar disponível uma rotina de desinfecção. Eles serão removidos para a quarentena para evitar uma potencial infecção.

Por padrão, os arquivos da quarentena são automaticamente enviados para os Laboratórios Bitdefender para serem analisados pelos pesquisadores de malware da Bitdefender. Se a presença de malware for confirmada, é emitida uma assinatura para possibilitar a remoção do malware.

- **Arquivos que contêm arquivos infectados.**
  - Os arquivos que contêm apenas arquivos infectados são eliminados automaticamente.
  - Se um arquivo tiver arquivos infectados e limpos, o Bitdefender tentará eliminar os arquivos infectados desde que possa reconstruir o arquivo com os arquivos limpos. Caso a reconstrução do arquivo não seja possível, você será informado de que qualquer ação não pode ser tomada para evitar a perda de arquivos limpos.





## Excluir

Remove os arquivos detectados do disco.

Se os arquivos infectados estiverem armazenados num arquivo junto com arquivos limpos, o Bitdefender tentará eliminar os arquivos infectados e reconstruir o arquivo com arquivos limpos. Caso a reconstrução do arquivo não seja possível, você será informado de que qualquer ação não pode ser tomada para evitar a perda de arquivos limpos.

## Não tome medida alguma

Nenhuma ação será tomada em arquivos detectados. Após a análise terminar, pode abrir o relatório da análise para ver informação sobre esses arquivos.

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

## Passo 3 - Resumo

Quando o Bitdefender termina de reparar estas incidências, o resultado da análise aparecerá numa nova janela. Se deseja uma informação completa sobre o processo de análise, clique em **MOSTRAR RELATÓRIO** para ver o relatório da análise.

### **Importante**

Na maioria dos casos o Bitdefender desinfecta com sucesso o arquivo infectado ou isola a infecção. No entanto, há incidências que não puderam ser automaticamente resolvidas. Se necessário, ser-lhe-á solicitado que reinicie o seu computador, para que o processo de limpeza seja completado. Para mais informações e instruções sobre como remover manualmente o malware, por favor consulte *"Remover malware do seu sistema"* (p. 207).


## Ver os relatórios da análise

Sempre que uma análise for feita, um registro de análise é criado e o Bitdefender registra as incidências detectados na janela Antivírus. O relatório da análise contém informação detalhada sobre os processos de análise registados, tal como as opções da análise, o alvo da análise, as ameaças encontradas e as ações tomadas sobre essas ameaças.

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



Para conferir um registro de verificação ou qualquer infecção detectada em um posteriormente:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Na aba **Todas**, selecione a notificação relacionada à última verificação. Aqui poderá encontrar todos os eventos de análise malware, incluindo ameaças detectadas na análise no acesso, análises iniciadas pelo usuário e alterações de status para as análises automáticas.
3. Na lista de notificações, você pode ver quais verificações foram realizadas recentemente. Clique em uma notificação para ver seus detalhes.
4. Para abrir o registro de verificação, clique em **VER REGISTRO**.

## Análise automática de mídia removível


O Bitdefender detecta automaticamente quando você conectar um dispositivo de armazenamento removível em seu computador e analisa-o em segundo plano. Isto é recomendado, a fim de evitar vírus e outros malwares de infectarem seu computador.

Os dispositivos detectados se enquadram em uma destas categorias:

- CDs/DVDs
- Dispositivos de armazenamento USB, tais como pen drives e HDs externos.
- Diretórios de rede mapeados (remotos)

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

## Como funciona?

Quando detecta dispositivos de armazenamento removíveis, o Bitdefender começa a verificar se existe malware em segundo plano (desde que a análise automática esteja ativada para aquele tipo de dispositivo). Um ícone de análise do Bitdefender  irá aparecer na **barra do sistema**. Você pode clicar nesse ícone para abrir a janela de análise e para visualizar o progresso da mesma.

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



Se o Piloto Automático estiver desativado:

1. Será notificado através de uma janela de pop-up que um novo dispositivo foi detectado e está a ser analisado.
2. Na maioria dos casos, o Bitdefender remove automaticamente o malware detectado ou isola os arquivos infectados na quarentena. Se houver ameaças não resolvidas depois da análise, será solicitado que você escolha as ações a serem tomadas com relação às mesmas.

## **Nota**

Leve em conta que nenhuma ação pode ser efetuada nos arquivos que estiverem infectados ou suspeitos em CDs / DVDs. Do mesmo modo, nenhuma ação pode ser tomada nos arquivos infectados ou suspeitos que estejam nos drives da rede mapeada caso você não tenha os privilégios adequados.

3. Quando a análise estiver concluída, é apresentada a janela dos resultados da análise para informar se você pode acessar com segurança aos arquivos nos dispositivos removíveis.


Esta informação pode ser útil para você:

- Tenha cuidado ao usar um CD/DVD infectado com malware, porque o malware não pode ser removido do disco (é apenas para leitura). Certifique-se que a proteção em tempo real está ativada para evitar que o malware se propague no seu sistema. É recomendado copiar quaisquer dados valiosos do disco no seu sistema e depois descartar o disco.
- Em alguns casos, o Bitdefender poderá não conseguir remover o malware de arquivos específicos devido a restrições legais ou técnicas. Exemplo disso são os arquivos guardados usando uma tecnologia patenteada (isto acontece porque o arquivo não pode ser recriado corretamente).


Para saber como lidar com malware, por favor consulte "*Remover malware do seu sistema*" (p. 207).

## Gerenciamento da análise de mídia removível

Para gerenciar a verificação automática de mídias removíveis:

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



3. Selecione o ícone  no canto superior direito do módulo **ANTIVÍRUS**.
4. Selecione a aba **DRIVES E DISPOSITIVOS**.


Para uma melhor proteção, recomenda-se que ative a análise automática para todos os tipos de dispositivos de armazenamento removíveis.

As opções de análise são pré-configuradas para obter os melhores resultados em detecção. Caso sejam detectados arquivos infectados, o Bitdefender tentará desinfecá-los (remover o código malware) ou movê-los para a quarentena. Se ambas as ações falharem, o assistente da Análise Antivírus permite especificar outras ações a serem adotadas com os arquivos infectados. As opções de análise são padrão e você não pode as alterar.

## Analisar arquivo hosts

O arquivo hosts vem por padrão com a instalação do seu sistema operacional e é usado para mapear nomes de host para endereços de IP cada vez que você acessa uma página da web, conecta-se a um FTP ou a outros serviços da internet. É um arquivo de texto comum e programas maliciosos podem modificá-lo. Usuários avançados sabem como usá-lo para bloquear anúncios irritantes, banners, cookies de terceiros ou hijackers.

Para configurar a verificação do arquivo hosts:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Selecione a aba **AVANÇADO**.
3. Clique no botão correspondente para ativar ou desativar a verificação do arquivo hosts.

## Configurar exceções da análise

O Bitdefender permite excluir arquivos, pastas ou extensões de arquivos específicos da análise. Esta característica visa evitar interferência ao seu trabalho e também pode ajudar a melhorar o desempenho do sistema. As exceções devem ser usadas por usuários com conhecimentos avançados de informática ou sob as recomendações de um representante da Bitdefender.

Pode configurar as exceções para aplicar apenas na análise no acesso ou a pedido, ou ambos. Os objetos excluídos da análise por demanda não serão analisados, independentemente deles serem acessados por você, ou por um aplicativo.





## Nota

As exclusões NÃO serão aplicadas à análise contextual. Análise Contextual é um tipo de análise por demanda: Você dá um clique com o botão direito do mouse no arquivo ou diretório que pretende analisar e seleciona **Analisar com o Bitdefender**.

## Excluindo arquivos e pastas da verificação

Para excluir arquivos específicos da verificação:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **ANTIVÍRUS**.
4. Selecione a aba **EXCLUSÕES**.
5. Clique no menu deslizável **Lista de arquivos e pastas excluídos da verificação**. Na janela que surge, pode gerenciar os arquivos e pastas excluídos da análise.
6. Adicionar exceções seguindo estes passos:
  - a. Clique no botão **ADD**.
  - b. Clique em **Buscar**, selecione o arquivo ou pasta que você quer excluir da verificação, depois clique em **OK**. Alternativamente, pode digitar (ou copiar e colar) o caminho para o arquivo ou pasta no campo editar.
  - c. Por padrão, o arquivo ou pasta selecionado é excluído tanto da análise no acesso quanto na análise a pedido. Para alterar o aplicativo da exclusão, selecione uma das outras opções.
  - d. Clicando **Adicionar**.

## Excluir extensões de arquivos da análise



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



## Importante

Tenha cuidado ao excluir as extensões da análise, porque tais exclusões podem tornar o seu computador vulnerável ao malware.



Para excluir extensões de arquivo da análise:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **ANTIVÍRUS**.
4. Selecione a aba **EXCLUSÕES**.
5. Clique no menu **Lista de extensões excluídas da verificação**. Na janela que surge, pode gerenciar o arquivo e extensões excluídos da análise.
6. Adicionar exceções seguindo estes passos:
  - a. Clique no botão **ADD**.
  - b. Introduza as extensões que deseja excluir da análise, separando-as com ponto e vírgula (;). Eis um exemplo:  
`txt;avi;jpg`
  - c. Por padrão, todos os arquivos com as extensões especificadas são excluídos da análise no acesso e a pedido. Para alterar o aplicativo da exclusão, selecione uma das outras opções.
  - d. Clicando **Adicionar**.

## Gerenciar exclusões de análise

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

Para gerir as exclusões da análise:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **ANTIVÍRUS**.
4. Selecione a aba **EXCLUSÕES**.
5. Use as opções no menu **Lista de arquivos e pastas excluídos da verificação** para gerenciar exclusões da verificação.



6. Para remover ou editar exceções da análise, clique em um dos links disponíveis. Proceder da seguinte forma:
  - Para remover uma entrada da tabela, selecione-a e clique no botão **REMOVER**.
  - Para editar uma entrada da tabela, dê um clique duplo (ou selecione e clique no botão **EDITAR**). Uma nova janela aparece quando você muda a extensão ou o caminho a ser excluído e o tipo de verificação que deseja que sejam excluídos, conforme necessário. Faça as alterações necessárias, depois clique em **Modificar**.



## Gerenciar arquivos em quarentena

O Bitdefender isola os arquivos infectados com malware que não consegue desinfetar numa área segura denominada quarentena. Quando o vírus está na quarentena não pode prejudicar de nenhuma maneira, porque não pode ser executado ou lido.

Por padrão, os arquivos da quarentena são automaticamente enviados para os Laboratórios Bitdefender para serem analisados pelos pesquisadores de malware da Bitdefender. Se a presença de malware for confirmada, é emitida uma assinatura para possibilitar a remoção do malware.

Além disso, o Bitdefender analisa os arquivos em quarentena após cada atualização da vacina de malware. Os arquivos limpados são movidos automaticamente de volta ao seu local original.

Para conferir e gerenciar arquivos em quarentena:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **ANTIVÍRUS**.
4. Selecione a aba **QUARENTENA**.
5. Os arquivos da quarentena são gerenciados automaticamente pelo Bitdefender de acordo com as predefinições da quarentena. Embora não seja recomendado, pode ajustar as definições da quarentena de acordo com as suas preferências.

### Reanalisar quarentena após a atualização de definições de vírus

Mantenha esta opção ativada para analisar automaticamente os arquivos da quarentena após cada atualização das definições de



vírus. Os arquivos limpados são movidos automaticamente de volta ao seu local original.

### **Enviar arquivos suspeitos da quarentena para posterior análise.**

Mantenha esta opção ligada para enviar automaticamente os arquivos da quarentena para os Laboratórios da Bitdefender. As amostras de arquivos serão analisadas pelos investigadores de malware da Bitdefender. Se a presença de malware for confirmada, é emitida uma assinatura para possibilitar a remoção do malware.

### **Apagar conteúdo com mais de {30} dias**

Por definição, arquivos de quarentena mais antigos que 90 dias são automaticamente apagados. Se quiser alterar este intervalo, digite um novo valor no campo correspondente. Para desabilitar a exclusão automática dos antigos arquivos em quarentena, digite 0.

6. Para apagar um arquivo em quarentena, selecione-o e clique no botão **APAGAR**. Se você deseja restaurar um arquivo em quarentena para seu local original, selecione-o e clique em **RESTAURAR**.

## Controle Ativo de Ameaças

O Controle Ativo de Ameaças do Bitdefender é uma tecnologia de detecção inovadora e proativa que usa métodos heurísticos avançados para detectar ransomware e outras novas ameaças potenciais em tempo real.

O Controle Ativo de Ameaças monitora continuamente os aplicativos em execução no computador, procurando ações semelhantes a malwares. Cada uma destas ações é classificada e é calculada uma pontuação geral para cada processo. Quando a classificação geral para um processo atinge um dado limite, o processo é considerado perigoso e é bloqueado automaticamente.

Se o Autopilot estiver desligado, você será notificado por uma janela pop-up acerca do ransomware detectado ou aplicação bloqueada. Caso contrário, o aplicativo será bloqueado sem qualquer notificação. Você pode conferir quais aplicações foram detectadas pelo Controle Ativo de Ameaças na janela **Notificações**.

## Verificar aplicativos detectados

Para ver as aplicações detectadas pelo Controle Ativo de Ameaças:

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







2. Na aba **Todas**, selecione a notificação relacionada à verificação do Controle Ativo de Ameaças.
3. Se você considera a aplicação confiável, pode configurar o Controle Ativo de Ameaças para não bloqueá-la mais clicando em **PERMITIR E MONITORAR**. O Controle Ativo de Ameaças continuará a monitorar aplicativos excluídos. Caso um aplicativo excluído seja detectado realizando atividades suspeitas, o evento será simplesmente registrado e comunicado à Nuvem do Bitdefender como uma detecção de erro.

## Ligando ou desligando o Controle Ativo de Ameaças

Para ativar ou desativar o Controle Ativo de Ameaças:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **ANTIVÍRUS**.
4. Na janela **PROTEÇÃO** clique no botão correspondente para ativar ou desativar o Controle Ativo de Ameaças.

## Ajustando a proteção do Controle Ativo de Ameaças

Se você perceber que o Controle Ativo de Ameaças detecta aplicativos legítimos com frequência, você deve definir um nível de proteção mais permissivo.

Para ajustar a proteção do Controle Ativo de Ameaças, arraste o marcador ao longo da escala para definir o nível de proteção desejado.

Utilize a descrição do lado direito da escala para escolher o nível de proteção que melhor se adequa às suas necessidades de segurança.



### Nota



Ao definir um nível de proteção mais alto, o Controle Ativo de Ameaças irá solicitar alguns sinais de comportamentos semelhantes a malwares para relatar um processo. Isto provocará um aumento do número de aplicativos que são comunicados e, ao mesmo tempo, um aumento da probabilidade de falsos positivos (aplicativos limpos detectados como maliciosos).



## Gerenciar processos excluídos

Você pode configurar regras de exclusão para aplicativos confiáveis de forma que o Controle Ativo de Ameaças não os bloqueie se apresentarem comportamentos semelhantes a malwares. O Controle Ativo de Ameaças continuará a monitorar aplicativos excluídos. Caso um aplicativo excluído seja detectado realizando atividades suspeitas, o evento será simplesmente registrado e comunicado à Nuvem do Bitdefender como uma detecção de erro.

Para gerenciar os processos excluídos do Controle Ativo de Ameaças:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **ANTIVÍRUS**.
4. Selecione a aba **EXCLUSÕES**.
5. Clique no menu **Lista de processos excluídos da verificação**.

Daqui é possível gerenciar os processos excluídos do Controle Ativo de Ameaças.

6. Adicionar exceções seguindo estes passos:
  - a. Clique no botão **ADD**.
  - b. Clique em **Buscar**, selecione a aplicação que você quer excluir da verificação, depois clique em **OK**.
  - c. Mantenha a opção **Permitir** selecionada para prevenir que o Controle Ativo de Ameaças bloqueie o aplicativo.
  - d. Clicando **Adicionar**.
7. Para remover ou editar exceções, proceda da seguinte forma:
  - Para remover uma entrada da tabela, selecione-a e clique no botão **APAGAR**.
  - Para editar uma entrada da tabela, dê um clique duplo (ou selecione-a e clique no botão **EDITAR**). Faça as alterações necessárias, depois clique em **Modificar**.



## 4.2. Antispam

Spam é o termo utilizado para descrever mensagens electrónicas não solicitadas. Spam é um problema crescente, tanto para usuários quanto para empresas. Não é bonito, você não gostaria que seus filhos vissem, pode fazer você perder o emprego (por desperdiçar muito tempo ou por receber e-mails impróprios no e-mail do escritório) e você não pode impedir as pessoas de enviá-lo. A melhor coisa a fazer é, obviamente, parar de recebê-los. Infelizmente, spams chegam em inúmeras formas e tamanhos, e em grandes quantidades.

O Bitdefender Antispam emprega inovações tecnológicas surpreendentes e um conjunto de filtros de antispam padrão para limpar o spam antes de o mesmo chegar à caixa de correio A receber do usuário. Para mais informações, por favor consulte **“Compreender o Antispam”** (p. 110).

A proteção Antispam do Bitdefender está disponível apenas para clientes de correio eletrônico configurado para receber mensagens de e-mail via protocolo POP3. POP3 é um dos protocolos mais utilizados para fazer o download de mensagens de e-mail a partir de um servidor de correio.



### Nota

O Bitdefender não proporciona protecção antispam para contas de correio eletrônico a que acede através de sítios de Internet (webmail).

As mensagens não solicitadas detectadas pelo Bitdefender são marcadas com o prefixo [SPAM] no campo do assunto. O Bitdefender move automaticamente mensagens de spam para um diretório específico, como abaixo:

- No Microsoft Outlook, as mensagens de spam são movidas para um diretório **Spam**, localizado no diretório **Itens Excluídos**. A pasta **Spam** é criada quando um e-mail é rotulado como spam.
- No Mozilla Thunderbird, as mensagens de spam são movidas para uma pasta **Spam**, localizada na pasta **Lixeira**. A pasta **Spam** é criada quando um e-mail é rotulado como spam.

Se você utiliza outros clientes de e-mail, você deve criar uma regra para mover as mensagens de e-mail marcadas como [SPAM] pelo Bitdefender para uma pasta de quarentena customizada. Se os itens detectados ou arquivos da lixeira forem apagados, a pasta Spam será apagada também. No entanto,



uma nova pasta de spam será criada assim que um e-mail for rotulado como spam.

## Compreender o Antispam

### Filtros Anti-spam

O Motor Antispam do Bitdefender inclui proteção em nuvem e outros filtros diferenciados que asseguram que sua Caixa de Entrada fique livre de SPAM, como a **Lista de Amigos**, **Spammers list** e **Filtro de Caracteres**.

### Lista de Amigos / Lista de Spammers

A maioria das pessoas se comunica regularmente com um grupo de pessoas ou mesmo recebe mensagens de empresas e organizações do mesmo domínio. Usando as **listas de amigos ou spammers**, você pode facilmente classificar de quais pessoas você quer receber e-mails (amigos) não importa o que a mensagem contenha, ou de quais pessoas você nem quer ouvir falar (spammers).



#### Nota

Nós recomendamos que você adicione os nomes e e-mails de seus amigos à **Lista de Amigos**. O Bitdefender não bloqueia mensagens das pessoas nesta lista; portanto, adicionar amigos assegura que e-mails legítimos vão chegar ao destino.

### Filtro de Caracteres

Muitas mensagens de spam estão escritas em caracteres cirílicos e/ou asiáticos. O filtro de Caracteres detecta este tipo de mensagens e marca-as como SPAM.

### Operação Antispam

O mecanismo do Bitdefender Antispam utiliza todos os filtros antispam combinados para determinar se uma determinada mensagem de e-mail deverá entrar em sua **Caixa de Entrada** ou não.

Todo o e-mail proveniente da Internet é inicialmente verificado pelo filtro da **Lista Amigos / Lista Spammers**. Se o endereço do remetente se encontrar na **Lista Amigos**, o e-mail é movido diretamente para a sua **Caixa de Entrada**.



Caso contrário, o filtro da **Lista de Spammers** irá apoderar-se do seu correio eletrônico para verificar se o endereço do remetente se encontra na lista. Se for encontrada uma correspondência, a mensagem será marcada como SPAM e movida para a pasta de **Spam**.

Em seguida, o **Filtro de caracteres** checa se o e-mail está escrito em caracteres Cirílicos ou Asiáticos. Caso esteja o e-mail será marcado como SPAM e movido para a pasta **Spam**.



## Nota

Se o e-mail é marcado como SEXUALLY EXPLICIT na linha do assunto, o Bitdefender vai considerá-lo SPAM.

## Cientes de e-mail e protocolos suportados



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

- Microsoft Outlook 2007 / 2010 / 2013
- Mozilla Thunderbird 14 ou superior

## Ligar ou desligar a proteção antispam

A proteção Antispam está ativada por padrão.

Para desativar o módulo antispam:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **ANTISPAM**.
4. Clique no botão correspondente para ativar ou desativar o **Antispam**.

## Utilizar a barra de ferramentas Antispam na janela do seu cliente de email

Na parte superior do seu programa de e-mail você pode ver a barra de ferramentas Antispam. A Barra de Ferramentas Antispam ajuda a gerenciar a proteção antispam diretamente do seu cliente de e-mail. Você pode facilmente corrigir o Bitdefender se ele marcou uma mensagem legítima como spam.



## ! Importante

O Bitdefender integra-se aos e-mails mais comumente usados pelos clientes através de uma barra de ferramentas muito fácil de usar. Para uma lista completa de clientes de e-mail suportados, por favor vá para **“Clientes de e-mail e protocolos suportados”** (p. 111).

Cada botão será explicado abaixo:

⚙️ **Configurações** - abre uma janela onde pode configurar as definições da barra de ferramentas e dos filtros antispam.

🗑️ **É Spam** - indica que o e-mail selecionado é spam. O e-mail será removido imediatamente para a pasta **Spam**. Se os serviços da nuvem antispam estiverem ativados, a mensagem é enviada para a Nuvem do Bitdefender para análise mais aprofundada.

📁 **Não Spam** - indica que o e-mail selecionado não é spam e o Bitdefender não deveria tê-lo identificado como tal. O e-mail será movido da pasta **Spam** para o diretório **Caixa de entrada**. Se os serviços da nuvem antispam estiverem ativados, a mensagem é enviada para a Nuvem do Bitdefender para análise mais aprofundada.

## ! Importante

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

👤 **Adicionar Spammer** - adiciona o remetente do e-mail selecionado para a lista de Spammers. Você poderá ter que clicar **OK** para acusar recebimento. As mensagens de e-mail recebidas destes endereços na lista de Spammers, são automaticamente marcados como [spam].

👤 **Adicionar Amigo** - adiciona o remetente do e-mail selecionado à lista de Amigos. Você poderá ter que clicar **OK** para acusar recebimento. Você sempre receberá e-mails desse endereço, não importa o que a mensagem contenha.

👤 **Spammers** - abre a **Lista de Spammers** que contém todos os endereços de e-mail, dos quais não quer receber mensagens, independentemente do seu conteúdo. Para mais informações, por favor consulte **“Configurar a lista de Spammers”** (p. 115).

👤 **Amigos** - abre a **Lista de amigos** que contém todos os endereços de e-mail dos quais deseja receber mensagens de e-mail, independentemente do seu conteúdo. Para mais informações, por favor consulte **“Configurar a Lista de Amigos”** (p. 114).




## Indicar os erros de detecção

Se você está usando um cliente de e-mail suportado, você pode facilmente corrigir o filtro antispam (indicando qual mensagem de e-mail não deve ser marcada como [spam]). Fazendo isto, a eficiência do filtro antispam melhorará consideravelmente. Siga esses passos:


1. Abra seu cliente de e-mail.
2. Vá para a pasta de lixo, aonde os spams são levados.
3. Selecione a mensagem legítima incorretamente marcada como [spam] pelo Bitdefender.
4. Clique o botão  **Adicionar Amigos** na barra de ferramentas do antispam do Bitdefender para adicionar o remetente à lista de Amigos. Você poderá ter que clicar **OK** para acusar recebimento. Você sempre receberá e-mails desse endereço, não importa o que a mensagem contenha.
5. Clique no botão  **Não Spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de e-mail do cliente). A mensagem de e-mail será removida para a pasta de Entrada.

## Indicar mensagens de spam não detectadas

Se você está usando um cliente de e-mail suportado, você pode facilmente indicar quais mensagens de e-mail foram detectadas como spam. Fazendo isto, a eficiência do filtro antispam melhorará consideravelmente. Siga esses passos:



1. Abra seu cliente de e-mail.
2. Vá para a Pasta de Entrada.
3. Selecione as mensagens spam não detectadas.
4. Clique no botão  **É Spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de e-mail do cliente). Elas são marcadas imediatamente como [spam] e movidas para a pasta lixo.

## Configurar definições da barra de ferramentas

Para configurar a barra de ferramentas antispam para o seu cliente de e-mail, clique no botão  **Configurações** na barra de ferramentas, depois na aba **Configurações de barra de ferramentas**.



Você tem as seguintes opções:

- **Marque as mensagens de e-mail indesejadas como 'ler'** - marque as mensagens indesejadas como ler automaticamente, de forma que não sejam um incômodo quando chegarem.
- Você pode optar por visualizar ou não janelas de confirmação quando clica nos botões  **Adicionar Spammer** e  **Adicionar Amigo** na barra de ferramentas antispam.

As janelas de confirmação podem evitar a adição acidental de destinatários de e-mail à lista de Amigos / Spammers.

## Configurar a Lista de Amigos



A **Lista de Amigos** é uma lista de todos os endereços de quem você sempre deseja receber mensagens, não importa o conteúdo. Mensagens de seus amigos não são marcadas como Spam, mesmo se o conteúdo se assemelhe a Spam.



### Nota

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

Para configurar e gerir a lista de Amigos:

- Se você estiver usando Microsoft Outlook ou Thunderbird, clique no botão  **Amigos** na **barra de ferramentas antispam do Bitdefender**.
- Alternativa:
  1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
  2. Clique no botão **VER MÓDULOS**.
  3. No módulo **ANTISPAM**, selecione **Gerenciar Amigos**.

Para adicionar um endereço de e-mail, selecione a opção **Endereço de e-mail**, insira o endereço e clique em **Adicionar**. Syntax: nome@domínio.com.

Para adicionar os endereços de e-mail de um domínio específico, selecione a opção **Nome do domínio**, insira o nome do domínio e clique em **Adicionar**. Syntax:

- @domínio.com, \*domínio.com e domínio.com - todos os e-mails vindos de domínio.com chegarão em sua **Caixa de entrada** não importando qual o seu conteúdo;





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

É recomendado que evite adicionar domínios completos, mas isto poderá ser útil em algumas situações. Por exemplo, pode adicionar o domínio do endereço eletrônico da empresa para a qual trabalha ou de parceiros de confiança.

Para eliminar um item da lista, clique no link **Remover** correspondente. Para apagar todas as entradas da lista, clique no botão **Limpar Lista**.

Você pode salvar a lista de Amigos em um arquivo que poderá ser usado em outro computador ou após a reinstalação do produto. Para salvar a lista de Amigos, clique no botão **Salvar** e salve o arquivo no local desejado. O arquivo terá a extensão **.bwl**.



Para carregar a lista de amigos salva anteriormente, clique no botão **Carregar** e abra o arquivo **.bwl** correspondente. Para redefinir o conteúdo da lista existente ao carregar uma lista salva anteriormente, selecione **Sobrescrever lista atual**.

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

## Configurar a lista de Spammers

**Lista de Spammers** é uma lista de todos os endereços de quem você não quer receber mensagens, não importa qual o conteúdo. Qualquer mensagem vinda de um e-mail na **Lista de Spammers** será marcado como Spam, sem mais processamentos.

Para configurar e gerir a lista de Spammers:

- Se você estiver usando Microsoft Outlook ou Thunderbird, clique no botão  **Spammers** na **barra de ferramentas antisпам do Bitdefender** integrada ao seu cliente de e-mail.
- Alternativa:
  1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
  2. Clique no botão **VER MÓDULOS**.
  3. No módulo **ANTISPAM**, selecione **Gerenciar Spammers**.



Para adicionar um endereço de e-mail, selecione a opção **Endereço de e-mail**, insira o endereço e clique em **Adicionar**. Syntax: nome@domínio.com.

Para adicionar os endereços de e-mail de um domínio específico, selecione a opção **Nome do domínio**, insira o nome do domínio e clique em **Adicionar**. Syntax:

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

É recomendado que evite adicionar domínios completos, mas isto poderá ser útil em algumas situações.

## **Atenção**

Não adicione domínios de serviços de e-mail legítimos (tais como Yahoo!, Gmail, Hotmail, ou outros) à lista de spammers. Caso contrário, os e-mails recebidos de qualquer usuário registrado de tais serviços serão detectados como spams. Se, por exemplo, você adicionar o yahoo.com à lista de Spammers, todos os e-mails vindos deste yahoo.com endereço serão marcados como [spam].

Para eliminar um item da lista, clique no link **Remover** correspondente. Para apagar todas as entradas da lista, clique no botão **Limpar Lista**.

Você pode salvar a lista de Spammers em um arquivo que poderá ser usado em outro computador ou após a reinstalação do produto. Para salvar a lista de Spammers, clique no botão **Salvar** e salve o arquivo no local desejado. O arquivo terá a extensão .bwl .

Para carregar uma lista de Spammers salva anteriormente clique no botão **Carregar** e abra o arquivo .bwl correspondente. Para redefinir o conteúdo da lista existente ao carregar uma lista salva anteriormente, selecione **Sobrescrever lista atual**.

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



## Configurando filtros antispam locais



Como descrito em “**Compreender o Antispam**” (p. 110), o Bitdefender utiliza um conjunto de diferentes filtros antispam para identificar o spam. Os filtros antispam são pré-configurados para uma proteção eficaz.




### Importante

Dependendo se recebe ou não mensagens electrónicas fiáveis ou não escrita com caracteres asiáticos ou cirílicos, desactive ou active a definição que bloqueia automaticamente estas mensagens. A respectiva definição está desativada nas versões localizadas do programa que utilizam conjuntos de caracteres (por exemplo, na versão russa ou chinesa).

Para configurar filtros antispam locais:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **ANTISPAM**.
4. Clique nos botões para ativar ou desativar os filtros locais antispam.

Se você estiver usando Microsoft Outlook ou Thunderbird, pode configurar os filtros antispam locais diretamente no seu cliente de e-mail. Clique no botão  **Configurações** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela do cliente de e-mail) e depois na aba **Filtros Antispam**.


## Configurando os Ajustes em Nuvem

Na detecção na nuvem faz uso dos Serviços na Nuvem do Bitdefender para lhe proporcionar uma proteção antispam eficaz e sempre atualizada.


As funções de proteção em nuvem enquanto mantiver o Antispam Bitdefender ativado.


As amostras de e-mails legítimos ou spam podem ser enviados para a Nuvem Bitdefender quando você indica erros de detecção ou e-mails de spam não detectados. Isto ajuda a melhorar a detecção antispam do Bitdefender.

Configurar o envio de amostra de e-mail para Nuvem Bitdefender através da seleção das opções desejadas, ao seguir estes passos:

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



2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **ANTISPAM**.
4. Selecione as opções desejadas na aba **CONFIGURAÇÕES**.

Se você estiver usando Microsoft Outlook ou Thunderbird, pode configurar a detecção na nuvem diretamente desde o seu cliente de e-mail. Clique no botão  **Configurações** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela do cliente de e-mail) e depois na aba **Configurações da nuvem**.



## 4.3. Proteção da Internet

A Proteção na web do Bitdefender garante uma navegação segura ao alertá-lo sobre páginas da web potencialmente maliciosas.



O Bitdefender fornece proteção da Internet em tempo real para:

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

Para configurar a proteção na web:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **PROTEÇÃO NA WEB**.

Clique nos botões para ligar ou desligar:

- O consultor de pesquisa, um componente que qualifica os resultados do seu motor de pesquisa e dos links colocados nos websites das redes sociais ao colocar um ícone ao lado de cada resultado:
  -  Você não deve visitar esta página da rede.
  -  Esta página pode ter conteúdo perigoso. Tenha cautela caso decida visitá-la.



● Esta página é segura.

O Consultor de Pesquisa qualifica os resultados da pesquisa dos seguintes motores de busca:

- Google
- Yahoo!
- Bing
- Baidu

O Consultor de Pesquisa classifica os links publicados nos seguintes serviços de redes sociais:

- Facebook
- 114

● Verificando SSL.

Ataques mais sofisticados podem usar tráfego da web seguro para enganar as suas vítimas. É, por isso, recomendado que ative a análise SSL.

- Proteção contra fraudes.
- Proteção contra phishing.

Você pode criar uma lista de páginas que não serão analisadas pelos mecanismos antimalware, antiphishing e antifraude do Bitdefender. A lista deve conter apenas os websites em que você confia plenamente. Por exemplo, adicione os websites onde costuma frequentemente fazer compras on-line.

Para configurar e gerenciar páginas usando a proteção da Internet fornecida pelo Bitdefender, clique no link **Lista Segura**. Uma nova janela aparece.

Para adicionar um site à lista segura, insira o seu endereço no campo correspondente e depois clique em **Adicionar**.

Para remover um site desta lista, selecione-o na lista e clique no link **Remover** correspondente.

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

## Alertas de Bitdefender no navegador

Sempre que tenta visitar uma página Web classificada como insegura, esta é bloqueada e é apresentada uma página de aviso no seu navegador.

A página contém informações como a URL do site e a ameaça detectada.



Você precisa decidir o que fará a seguir. As seguintes opções estão disponíveis:

- Navegue para fora da página web clicando em **Leve-me de volta à segurança**.
- Prosseguir para a página web, apesar do aviso, clicando em **eu compreendo os riscos, avançar assim mesmo**.

## 4.4. Proteção de Dados

### Apagar arquivos permanentemente


Ao apagar um arquivo, o mesmo já não fica acessível por meios normais. No entanto o arquivo continua armazenado no disco rígido até que seja sobrescrito com a cópia de novos arquivos.

O Destruidor de Arquivos do Bitdefender o ajuda a apagar dados permanentemente removendo-os fisicamente de seu disco rígido.

Pode rapidamente destruir arquivos ou pastas do seu computador usando o menu contextual Windows, seguindo estes passos:

1. Clique botão direito sobre o arquivo ou pasta que deseja apagar permanentemente.
2. Selecione **Bitdefender > Destruidor de Arquivos** no menu contextual que aparece.
3. Uma janela de confirmação aparecerá. Clique em **SIM, ELIMINAR** para iniciar o assistente do Destruidor de Arquivos. Aguarde que o Bitdefender termine a destruição dos arquivos.
4. Os resultados são apresentados. Clique em **FINALIZAR** para sair do assistente.

Como alternativa, você pode destruir arquivos a partir da interface do Bitdefender da seguinte forma:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **PROTEÇÃO DE DADOS**, selecione **Destruidor de Arquivos**.
4. Siga o assistente do Destruidor de Arquivos:



- a. Clique no botão **ADICIONAR ARQUIVOS...** para adicionar os arquivos ou pastas que deseja remover permanentemente.

Você também pode arrastar esses arquivos ou pastas para esta janela.

- b. Clique em **ELIMINAR ARQUIVOS PERMANENTEMENTE** e depois confirme que deseja continuar com o processo.

Aguarde que o Bitdefender termine a destruição dos arquivos.

- c. **Resumo dos Resultados**

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

## 4.5. Criptografia de Arquivos


A Criptografia de Arquivos do Bitdefender permite você criar drives lógicos criptografados e protegidos por senha (ou cofres), no seu computador onde você pode armazenar de forma segura seus documentos confidenciais e sensíveis. Os dados armazenados nos cofres apenas podem ser acessados pelos usuários que sabem a senha.

A senha permite-lhe abrir, armazenar dados no cofre e fechá-lo ao mesmo tempo que o mantém seguro. Enquanto um cofre estiver aberto, você pode adicionar novos arquivos, acessar arquivos atuais ou alterá-los.

Fisicamente, o cofre é um arquivo armazenado no seu disco rígido local com a extensão `.bvd`. Apesar dos arquivos físicos que representam os drives de cofre poderem ser acessados a partir de um sistema operacional diferente (tal como Linux), a informação armazenada não pode ser lida por estar criptografada.

Os cofres de arquivos podem ser gerenciados a partir da janela do **Bitdefender** ou com o menu contextual do Windows e da unidade lógica associada ao cofre.

## Gerenciando os cofres de arquivos


Para gerenciar os cofres de arquivos do Bitdefender, clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.

Os cofres de arquivos existentes aparecerão no módulo **Cofres de arquivos**.



## Criar cofre de arquivos

Para criar um novo cofre:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **CRIPTOGRAFIA DE ARQUIVOS**, selecione **Criar cofre de arquivos**.
4. Especifique o nome e o local do cofre de arquivos.
  - Digite o nome do cofre de arquivos no campo correspondente.
  - Clique em **Explorar** para seleccionar a localização do cofre e guarde o cofre de arquivos sob o nome desejado.
5. Escolha uma letra do disco do menu correspondente. Quando abre o cofre, um disco virtual com a letra seleccionada aparecerá em O Meu Computador.
6. Se deseja mudar o tamanho padrão (100 MB) do cofre, use as setas para cima ou para baixo na caixa **Tamanho do cofre (MB)**.
7. Digite a senha escolhida para o cofre nos campos **Senha** e **Confirmar senha**. A senha deve ter pelo menos oito caracteres. Qualquer pessoa que tente abrir o cofre e acessar seus arquivos, precisa fornecer a senha.
8. Clique **Criar**.

O Bitdefender irá informá-lo imediatamente sobre o resultado da operação. Se um erro ocorrer, use a mensagem de erro para solucionar o problema.

Para criar um novo cofre mais rapidamente, clique com o botão direito do mouse em sua área de trabalho ou em uma pasta em seu computador, selecione **Bitdefender** e **Cofre de arquivos do Bitdefender** e clique em **Criar cofre de arquivos**.



### Nota

Pode ser conveniente salvar todos os arquivos dos cofres na mesma localização. Desta forma, você pode encontrá-los mais rapidamente.






## Abrir cofre de arquivos

Para poder acessar e trabalhar com os arquivos armazenados no cofre, você precisa abrir o cofre. Quando abre o cofre, um disco virtual aparece em O Meu Computador. A drive tem a denominação da letra que atribuiu ao cofre.

Para abrir um cofre:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**. Os cofres de arquivos existentes aparecerão no módulo **Cofres de arquivos**.
2. Clique no link **Ver cofres** e depois selecione o cofre que deseja abrir.
3. Clique no botão **Desbloquear** e depois digite a senha exigida.
4. Clique em **OK** e depois no botão **Abrir** para abrir seu cofre.



O Bitdefender irá informá-lo imediatamente sobre o resultado da operação. Se ocorreu um erro, use a mensagem de erro para solucionar o erro.

Para abrir um cofre mais rapidamente, localize em seu computador o arquivo `.bvd` que representa o cofre que você deseja abrir. Clique com o botão-direito no arquivo, aponte para **Cofre de Arquivos Bitdefender** e selecione **Abrir**. Digite a senha requisitada, e clique em **OK**.

## Adicionar arquivos aos cofres

Antes de adicionar arquivos ou pastas à um cofre, você deve abrir o cofre.

Para adicionar arquivos novos ao seu cofre:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **CRIOGRAFIA DE ARQUIVOS**.
4. Na janela **Meus cofres**, selecione o cofre que deseja abrir.
5. Clique no botão **Desbloquear** e depois digite a senha exigida.
6. Clique no botão **Abrir** para abrir seu cofre.
7. Adicione arquivos ou pastas da mesma forma que faria no Windows (por exemplo, você pode usar o método de copiar e colar).




Para adicionar arquivos a seu cofre mais rapidamente, clique com o botão direito do mouse no arquivo ou pasta que você deseja copiar para o cofre, selecione **Cofre de arquivos do Bitdefender** e clique em **Adicionar ao cofre de arquivos**.

- Se apenas um Cofre está aberto, o arquivo ou pasta é copiado diretamente para o cofre.
- Se vários cofres estão abertos, será solicitado que você escolha o cofre ao qual deseja copiar o item. Selecione no menu a letra correspondente ao Cofre desejado e clique em **OK** para copiar o item.

## Fechar cofres

Quando terminou de trabalhar sobre um cofre de arquivos, deve de o fechar de forma a proteger os seus dados. Ao bloquear o cofre, a unidade de disco virtual correspondente desaparece do diretório Meu Computador. Consequentemente, o acesso aos dados armazenados no cofre está completamente bloqueado.

Para trancar um cofre:


1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. No módulo **Cofres de arquivos**, selecione **Ver cofres**.
3. Na janela **Meus cofres**, selecione o cofre que deseja trancar.
4. Clique no botão **Trancar**.

O Bitdefender irá informá-lo imediatamente sobre o resultado da operação. Se um erro ocorrer, use a mensagem de erro para solucionar o problema.


Para trancar um cofre mais rapidamente, clique com o botão direito no arquivo **.bvd** que representa o cofre, selecione **Cofre de arquivos do Bitdefender** e clique em **Trancar**.

## Remover arquivos do cofre

A fim de remover arquivos ou pastas de um cofre, o cofre deve estar aberto. Para remover arquivos ou pastas de um cofre:

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





3. Selecione o ícone  no canto superior direito do módulo **CRIOGRAFIA DE ARQUIVOS**.
4. Na janela **Meus cofres**, selecione o cofre de onde deseja remover arquivos.
5. Clique no botão **Destrancar**, caso esteja trancado.
6. Clique no botão **Abrir**.

Apague os arquivos ou diretórios como você faz normalmente no Windows (por exemplo, clicar com o botão direito do mouse em um arquivo que você deseja excluir e selecione **Excluir**).

## Mudar senha do cofre

A senha protege o conteúdo de um cofre de acessos não autorizados. Apenas os usuários que conhecem a senha podem abrir o cofre e acessar os documentos e dados armazenados no seu interior.

O cofre deve estar bloqueado antes que você possa alterar a sua senha. Para mudar a senha de um cofre:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **CRIOGRAFIA DE ARQUIVOS**.
4. Na janela **MEUS COFRES**, selecione o cofre para o qual deseja mudar a senha.
5. Clique no botão **Configurações**.
6. Digite a senha atual do cofre no campo **Senha Antiga**.
7. Digite a nova senha do cofre nos campos **Nova Senha** e **Confirme a Nova Senha**.



### Nota

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

O Bitdefender irá informá-lo imediatamente sobre o resultado da operação. Se um erro ocorrer, use a mensagem de erro para solucionar o problema.



Para alterar a senha de um cofre mais rapidamente, localize em seu computador o arquivo `.bvd` que representa o cofre. Clique com o botão direito do mouse sobre o arquivo, selecione **Arquivo Cofre Bitdefender** e selecione **Mudar Senha do Cofre**.

## 4.6. Vulnerabilidade

Um passo importante na proteção do seu computador contra as ações e aplicações maliciosas é manter atualizado o seu sistema operacional e as aplicações que usa regularmente. Além disso, para evitar o acesso físico não autorizado ao seu computador, senhas fortes (aquelas que não são facilmente descobertas) devem ser configuradas para cada conta de usuário do Windows e também para as redes Wi-Fi às quais você se conecta.

O Bitdefender verifica automaticamente o seu sistema por vulnerabilidades e alerta você sobre elas. Ele verifica em busca de:

- aplicativos desatualizados em seu computador.
- Falta de atualizações do Windows.
- Senhas fracas para contas de usuário do Windows.
- redes sem fio e roteadores não seguros.


O Bitdefender proporciona duas formas fáceis de resolver as vulnerabilidades do seu sistema:

- Você pode analisar o seu sistema em busca de vulnerabilidades e repará-las passo a passo com a opção **Análise de Vulnerabilidades**.
- Usando o monitoramento automático de vulnerabilidades, você pode conferir e reparar vulnerabilidades detectadas na janela **Notificações**.

Você deve verificar e corrigir vulnerabilidades do sistema a cada uma ou duas semanas.

## Procurar vulnerabilidades no seu sistema

Para reparar vulnerabilidades usando a opção de verificação de vulnerabilidades:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão de ação **Verificação de vulnerabilidade**.



3. Espere o Bitdefender analisar as vulnerabilidades do seu sistema. Para interromper o processo de análise, clique no botão **Pular** na parte inferior da janela.

## ● **Atualizações Críticas do Windows**

Clique em **Ver detalhes** para ver uma lista de atualizações críticas do Windows que não estão instaladas em seu computador.

Para iniciar a instalação das atualizações selecionadas, clique em **Instalar atualizações**. Note que a instalação das atualizações poderá demorar um pouco e algumas delas podem exigir a reinicialização do sistema para concluir a instalação. Se necessário, reinicie o sistema quando lhe convier.

## ● **Atualizações do aplicativo**

Caso um aplicativo não esteja atualizado, clique no link **Fazer download da nova versão** para fazer download da última versão.

Clique em **Ver detalhes** para ver informações sobre o aplicativo que precisa ser atualizado.

## ● **Senhas fracas de contas do Windows**

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

Clique em **Alterar senha ao fazer login** para definir uma nova senha para seu sistema.

Clique em **Ver detalhes** para modificar as senhas fracas. Você pode escolher entre pedir ao usuário para alterar a senha no próximo acesso ou alterar a senha imediatamente. Para obter uma senha forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, \$ ou @).

## ● **Redes Wi-Fi fracas**

Clique em **Ver detalhes** para saber mais sobre a rede sem fio à qual está conectado. Caso seja recomendado definir uma senha mais forte para sua rede doméstica, clique no link correspondente.

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




No canto superior direito da janela, você pode filtrar os resultados de acordo com suas preferências.

## Usando o monitoramento automático de vulnerabilidade



O Bitdefender verifica seu sistema em busca de vulnerabilidades regularmente, em segundo plano, e mantém registros de problemas detectados na janela **Notificações**.

Para ver e reparar os problemas detectados:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Na aba **Todas**, selecione a notificação relacionada à Verificação de vulnerabilidades.
3. Pode ver a informação detalhada sobre as vulnerabilidades detectadas do sistema. Dependendo da incidência, para consertar uma vulnerabilidade específica, proceda da seguinte forma:
  - Se atualizações para o Windows estiverem disponíveis para o Windows, clique em **INSTALAR**.
  - Se a atualização automática para o Windows estiver desativada, clique em **ATIVAR**.
  - Se a aplicação estiver desatualizada, clique em **ATUALIZAR AGORA** para encontrar um link da página do distribuidor de onde você poderá instalar a versão mais recente da aplicação.
  - Se a conta de usuário do Windows tiver uma senha fraca, clique em **MUDAR SENHA** para forçar o usuário a mudar a senha na próxima inicialização ou para mudá-la você mesmo. Para obter uma senha forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, \$ ou @).
  - Caso a função Execução Automática do Windows esteja ativada, clique em **REPARAR** para desativá-la.
  - Se o roteador que você configurou tem uma senha fraca, clique em **ALTERAR SENHA** para acessar a interface, onde você pode definir uma senha forte.
  - Se a rede à qual você está conectado tem vulnerabilidades que podem por seu sistema em risco, clique em **ALTERAR CONFIGURAÇÕES DO WI-FI**.



Para configurar o monitoramento de vulnerabilidades:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **VULNERABILIDADE**.
4. Clique no botão correspondente para ligar ou desligar a verificação de vulnerabilidades.



## **Importante**

Para ser notificado automaticamente sobre vulnerabilidades no sistema ou em aplicações, mantenha a opção **Vulnerabilidade** ativa.

5. Escolha as vulnerabilidades do sistema que deseja que sejam regularmente verificadas usando os botões correspondentes.

### **Atualizações Críticas do Windows**

Verifique se o seu sistema operacional Windows possui as mais recentes e importantes atualizações de segurança da Microsoft.

### **Atualizações do aplicativo**

Verifique se os aplicativos instalados em seu sistema estão atualizados. As aplicações desatualizadas podem ser exploradas por software malicioso, tornando o PC vulnerável a ataques externos.

### **Senhas inadequadas**

Confira se as senhas para as contas do Windows e roteadores configurados no sistema são fáceis de descobrir ou não. A configuração de senhas difíceis de descobrir (senhas altamente seguras) torna muito difícil a invasão do seu sistema pelos hackers. Uma senha segura inclui letras maiúsculas e minúsculas, números e caracteres especiais (tais como #, \$ ou @).

### **Execução automática de conteúdos multimídia**

Verifique o status do recurso Windows Autorun. Esta característica permite que os aplicativos se iniciem automaticamente a partir dos CDs, DVDs, drives USB ou outros dispositivos externos.

Alguns tipos de malware usam Autorun para se propagar automaticamente na mídia removível do PC. Por isso, recomenda-se desativar este recurso do Windows.



## Notificações do Consultor de Segurança do Wi-Fi

Confira se a rede sem fio doméstica à qual você está conectado é segura e se tem vulnerabilidades. Confira também se a senha do seu roteador doméstico é forte o suficiente e como você pode torná-la mais segura.

A maioria das redes sem fio desprotegidas não é segura, permitindo, assim, que os hackers tenham acesso às suas atividades privadas.



### Nota

Se você desligar o monitoramento de uma vulnerabilidade específica, os problemas relacionados não serão mais registrados na janela de notificações.

## Consultor de Segurança Wi-Fi

A solução mais rápida quando se está em movimento pode ser conectar-se a uma rede sem fio pública para fazer pagamentos, verificar e-mails ou redes sociais enquanto trabalha em uma cafeteria ou espera em um aeroporto. Mas os olhos atentos de hackers tentando roubar seus dados podem estar lá, assistindo como as informações vazam pela rede.

Dados pessoais significam as senhas e nomes de usuários que você usa para acessar suas contas online, como e-mails, contas de bancos, mídias sociais, mas também incluem as mensagens que você envia.

Normalmente, as redes sem fio públicas são mais propensas a serem não seguras, uma vez que não requerem uma senha para entrar, e quando requerem, a senha é disponibilizada para qualquer um que deseja se conectar. Além disso, elas podem ser redes maliciosas ou do tipo pote de mel, representando um alvo para criminosos cibernéticos.

Para protegê-lo contra os perigos dos hotspots de conexão sem fio públicos não seguros ou não criptografados, o Consultor de Segurança do Wi-Fi do Bitdefender analisa a segurança de uma rede sem fio e, quando necessário, recomenda que você use o Bitdefender Safepay™ com a opção de Wi-Fi Hotspot ativa.

O Consultor de Segurança do Wi-Fi do Bitdefender lhe dá informação sobre:



- **Redes Wi-Fi domésticas**
- **Redes Wi-Fi públicas**






## Desligando ou ligando as notificações do Consultor de Segurança do Wi-Fi

Para desligar as notificações do Consultor de Segurança do Wi-Fi:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **VULNERABILIDADE**.
4. Clique no botão correspondente para ativar ou desativar as **notificações do Consultor de Segurança do Wi-Fi**.

## Configurando a rede Wi-Fi doméstica

Para começar a configurar sua rede doméstica:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **VULNERABILIDADE**, selecione **Consultor de Segurança do Wi-Fi**.
4. Na aba **Wi-Fi DOMÉSTICA**, clique no botão **SELECIONAR WI-FI DOMÉSTICA**.

Uma lista com as redes sem fio às quais você já se conectou até o momento é exibida.

5. Escolha sua rede doméstica e depois clique em **SELECIONAR**.

Se uma rede é considerada desprotegida ou não segura, serão exibidas recomendações para reforçar sua segurança.

Para remover a rede sem fio que você definiu como rede doméstica, clique no botão **REMOVER**.

## Wi-Fi pública


Enquanto estiver conectado a uma rede sem fio desprotegida ou não segura, o perfil Wi-Fi Pública é ativado. Enquanto o perfil estiver ativado, o Bitdefender Total Security está configurado para realizar automaticamente os seguintes ajustes:




- O Controle Ativo de Ameaças é ligado
- O Firewall do Bitdefender está ligado e as seguintes configurações são aplicadas ao seu adaptador sem fio:
  - Modo Sigiloso - Ligado
  - Genérico - Desligado
  - Tipo de rede - Pública
- As seguintes configurações da Proteção na Web são ativadas:
  - Analisar SSL
  - Proteção contra fraudes
  - Proteção contra phishing
- Um botão que abre o Bitdefender Safepay™ é ativado. Neste caso, a Proteção de hotspot para redes desprotegidas é ativada por padrão.

## Conferindo informações sobre redes Wi-Fi

Para conferir informações sobre as redes sem fio às quais você normalmente se conecta:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **VULNERABILIDADE**, selecione **Consultor de Segurança do Wi-Fi**.
4. Dependendo das informações que você precisar, selecione uma das abas, **Wi-Fi** ou **Wi-Fi PÚBLICA**.
5. Clique em **Ver detalhes**, próximo à rede para a qual você deseja ver mais informações.

Há três tipos de redes sem fio filtradas pela importância, cada tipo indicado por um ícone específico:

●  ● **Wi-Fi inseguro** - indica que o nível de segurança da rede é baixo. Ou seja, é muito arriscado usá-la e não é recomendado fazer pagamentos ou conferir contas bancárias sem uma proteção extra. Em tais situações, recomendamos usar o Bitdefender Safepay™ com a proteção para pontos de acesso de redes não seguras ativada.



■ ■ ■ **Wi-Fi inseguro** - indica que o nível de segurança da rede é moderado. Ou seja, ela pode ter vulnerabilidades e não é recomendado fazer pagamentos ou conferir contas bancárias sem uma proteção extra. Em tais situações, recomendamos usar o Bitdefender Safepay™ com a proteção para pontos de acesso de redes não seguras ativada.

■ ■ ■ **Wi-Fi seguro** - indica que a rede que você está usando é segura. Neste caso, você pode usar dados sensíveis para fazer operações online.

Ao clicar no link **Ver detalhes** na área de cada rede, os seguintes detalhes são exibidos:

- **Segura** - aqui você pode ver se a rede selecionada é segura ou não. Redes criptografadas podem deixar seus dados expostos.
- **Tipo de criptografia** - aqui você pode ver o tipo de criptografia usado para a rede selecionada. Certos tipos de criptografia podem não ser seguros. Portanto, recomendamos veementemente que você confira as informações sobre o tipo de criptografia exibidas para ter certeza de que está protegido enquanto navega na internet.
- **Canal/Frequência** - aqui você pode ver a frequência do canal usado pela rede selecionada.
- **Força da senha** - aqui você pode ver a força da senha. Lembre-se que redes que têm senhas fracas representam um alvo para criminosos cibernéticos.
- **Tipo de conexão** - aqui você pode ver se a rede selecionada é protegida por senha ou não. É recomendável conectar-se somente a redes que têm senhas fortes.
- **Tipo de autenticação** - aqui você pode ver o tipo de autenticação usado pela rede.

Mantenha a opção **Notificar** ativada para receber notificações sempre que seu sistema se conectar a essa rede.

## 4.7. Firewall

O Firewall protege o seu computador contra tentativas de conexão de saída e entrada não autorizadas, seja em redes locais ou Internet. É bastante semelhante a um guarda à sua porta - mantém o controle de tentativas de conexão e decide o que permitir e o que bloquear.



A firewall do Bitdefender usa um conjunto de regras para filtrar dados transmitidos para ou a partir do seu sistema. As regras estão organizadas em 2 categorias:

## Regras Gerais

Regras que determinam os protocolos através dos quais a comunicação é permitida.

É usado um conjunto de regras padrão que proporciona uma ótima proteção. Você pode editar as regras permitindo ou impedindo as conexões através de determinados protocolos.

## Regras de Aplicativos

As regras que determinam como cada aplicativo pode acessar os recursos da rede e à Internet.



Em condições normais, o Bitdefender cria automaticamente uma regra sempre que um aplicativo tenta acessar a Internet. Também pode adicionar ou editar manualmente regras dos aplicativos.

O Bitdefender atribui automaticamente um tipo de rede a cada conexão de rede que detecta. Dependendo do tipo de rede, a proteção firewall é definida ao nível apropriado para cada ligação.

Para saber mais sobre as configurações da firewall para cada tipo de rede e como editar as configurações de rede, por favor consulte [“Gerenciando Configurações de Conexão”](#) (p. 138).

## Ligar ou desligar a proteção firewall

Para ativar ou desativar a proteção por firewall:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **FIREWALL**.
4. Ative ou desative o firewall usando o botão correspondente.



### Atenção

Devido ao fato de expor o seu computador a conexões não autorizadas, desligar a firewall deveria ser uma medida temporária. Volte a ligar a firewall assim que possível.





## Gerenciando regras do Firewall

### Regras gerais

Sempre que determinados dados são transmitidos pela Internet, são usados certos protocolos.

As regras gerais permitem-lhe configurar os protocolos através dos quais o tráfego é permitido. Por padrão, as regras gerais não são exibidas ao abrir o Firewall. Para editar as regras:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **FIREWALL**.
4. Selecione a aba **REGRAS**.
5. Marque a caixa **Mostrar regras gerais** no canto inferior esquerdo da janela.

As regras padrão são exibidas. Para editar a prioridade de uma regra, clique na seta correspondente na coluna **Permissão** e selecione **Permitir** ou **Negar**.

#### **DNS sobre UDP / TCP**

Permitir ou negar DNS sobre o UDP e o TCP.

Este tipo de conexão é permitido por padrão.

#### **Enviando e-mails**

Permite ou nega envio de email por SMTP.

Este tipo de conexão é permitido por padrão.

#### **Navegação na Rede HTTP**

Permitir ou impedir navegação na web HTTP.

Este tipo de conexão é permitido por padrão.

#### **Entrada de ICMP / ICMPv6**

Permitir ou impedir mensagens ICMP / ICMPv6.

As mensagens ICMP são frequentemente usadas pelos hackers para atacarem as redes de computadores. Este tipo de conexão é permitido por padrão.



## Entrada de Conexões Remotas ao Desktop

Permitir ou impedir o acesso de outros computadores em Conexões Remotas de Desktop.

Este tipo de conexão é permitido por padrão.



## Tráfego do Windows Explorer em HTTP / FTP

Permitir ou impedir tráfego HTTP ou FTP do Windows Explorer.

Este tipo de conexão é permitido por padrão.

## Regras da aplicação

Para ver e gerenciar as regras do firewall controlando o acesso de aplicações a recursos da rede e internet:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **FIREWALL**.
4. Selecione a aba **REGRAS**.

Pode ver na tabela os programas (processos) para os quais as regras de firewall foram criadas. Para verificar as regras criadas para um aplicativo específico, clique nele duas vezes.

Para cada regra é apresentada a seguinte informação:

- **Nome** - o nome do processo ao que as regras se aplicam.
- **Tipo de Rede** - os tipos de adaptador de rede e processo aos que as regras se aplicam. As regras são automaticamente criadas para filtrar o acesso à rede ou à Internet através de qualquer adaptador. Por padrão, as regras se aplicam a qualquer rede. Pode criar manualmente as regras ou editar as regras existentes para filtrar o acesso à rede ou à Internet de um aplicativo através de um determinado adaptador (por exemplo, um adaptador de rede wireless).
- **Protocolo** - o protocolo IP aos quais as regras se aplicam. Por padrão, as regras se aplicam a qualquer protocolo.
- **Permissão** - se o acesso do aplicativo à rede ou à Internet é permitido ou negado sob circunstâncias específicas.

Para gerenciar as regras, use os botões acima da tabela:



- **ADICIONAR REGRA** - abre uma janela onde você pode criar uma nova regra.
- **APAGAR** - apaga a regra selecionada.
- **REDEFINIR REGRAS** - abre uma janela onde você pode remover o conjunto atual de regras e restaurar as regras padrão.

## Adicionar / editar regras de aplicativo

Para adicionar ou editar uma regra de aplicação, clique no botão **ADICIONAR REGRA** acima da tabela ou clique em uma regra atual. Uma nova janela aparece. Proceder da seguinte forma:

Na aba **Configurações** você pode aplicar as seguintes mudanças:

- **Caminho do Programa.** Clique em **Explorar** para selecionar o aplicativos a qual a regra se aplica.
- **Tipo de rede.** Selecione o tipo de rede ao qual a regra se aplica. Pode alterar o tipo abrindo o menu pendente **Tipo de Rede** e selecionando um dos tipos disponíveis na lista.

Tipo de rede	Descrição
<b>Confiável</b>	Desativa o firewall para o respectivo dispositivo.
<b>Casa/Escritório</b>	Permite o tráfego entre o seu computador e os computadores na rede local.
<b>Público</b>	Todo o tráfego é filtrado.
<b>Não Confiável</b>	Bloqueia completamente o tráfego de rede e de Internet através do respectivo adaptador.

- **Permissão.** Selecione uma das seguintes permissões disponíveis:

Permissão	Descrição
<b>Permitir</b>	O aplicativo especificado será permitido o acesso à rede / Internet nas circunstâncias determinadas.
<b>Negar</b>	O aplicativo especificado será negado o acesso à rede / Internet nas circunstâncias determinadas.

Na aba **Avançado** você pode customizar as seguintes mudanças:



- **Endereço Local Customizado.** Especifique o endereço IP local e a porta aos quais a regra se aplica.
- **Endereço Remoto Customizado.** Especifique o endereço IP remoto e a porta à qual a regra se aplica.
- **Direção.** Selecione do menu a direção do tráfego ao qual a regra se aplica.

Direção	Descrição
<b>Saída</b>	As regras valem apenas para tráfego de saída.
<b>Entrada</b>	As regras valem apenas entrada.
<b>Ambos</b>	As regras valem para as duas direções.

- **Protocolo.** Selecione do menu o protocolo IP ao qual a regra se aplica.
  - Se deseja que a regra se aplique a todos os protocolos, selecione **Qualquer uma**.
  - Se você quiser que a regra se aplique a TCP, selecione **TCP**.
  - Se você quiser que a regra se aplique a UDP, selecione **UDP**.
  - Se quiser que a regra se aplique em um protocolo específico, digite o número atribuído ao protocolo que quiser filtrar no campo de edição em branco.



## Nota

Os números dos protocolos IP são atribuídos pelo Internet Assigned Numbers Authority (IANA). Pode encontrar a lista completa de números IP atribuídos em <http://www.iana.org/assignments/protocol-numbers>.

## Gerenciando Configurações de Conexão

Para cada conexão de rede você pode configurar zonas especiais confiáveis ou não confiáveis.



Uma zona confiável é um dispositivo em que você confia plenamente, por exemplo um computador ou uma impressora. Todo o tráfego entre o seu computador e um dispositivo confiável é permitido. Para partilhar recursos com determinados computadores numa rede wireless insegura, adicione-os como computadores autorizados.





Uma zona não confiável é um dispositivo que você não quer de forma alguma que se comunique com o seu computador.

Para ver ou gerenciar zonas nos seus adaptadores de rede:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **FIREWALL**.
4. Selecione a aba **ADAPTADORES**.

Os adaptadores de rede com conexões ativas e as áreas atuais, se houver, são exibidos nesta aba.

Para cada zona a seguinte informação é exibida:

- **Tipo de Rede** - o tipo de rede a que o seu computador está ligado.
- **Modo Invisível** - para não ser detectado por outros computadores.

Para configurar o Modo Stealth, selecione a opção desejada do menu suspenso.

Opção Stealth	Descrição
<b>Ligado</b>	O Modo Stealth está ligado. O seu computador é invisível a partir da rede local e da Internet.
<b>Desligado</b>	O Modo Stealth está desligado. Qualquer pessoa da rede local ou da Internet pode fazer ping e detectar o seu computador.

- **Genérico** - se as regras genéricas são aplicadas a esta ligação.

Se o endereço IP de um adaptador é alterado, o Bitdefender modifica o tipo de rede de acordo com a alteração. Caso deseje manter o mesmo tipo, selecione **Sim** do menu suspenso correspondente.

## Adicionar / editar exceções



Para adicionar ou editar uma exceção, clique no link **Exceções de rede** acima da tabela. Uma nova janela exibindo os Adaptadores disponíveis conectados à rede aparecerá. Proceder da seguinte forma:



1. Selecione o endereço IP do computador que deseja adicionar, ou digite um endereço ou intervalo de endereço na caixa de texto fornecida.
2. Selecione a permissão:
  - **Permitir** - para autorizar o tráfego entre o seu computador e o computador seleccionado.
  - **Negar** - para bloquear o tráfego entre o seu computador e o computador seleccionado.
3. Clique no botão + para adicionar a exceção, fechar a janela.  
Se quiser remover um IP, clique no botão correspondente e feche a janela.

## Configurando definições avançadas

Para configurações avançadas de firewall:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **FIREWALL**.
4. Selecione a aba **CONFIGURAÇÕES**.

A ferramenta a seguir pode ser habilitada ou desabilitada:

- **Bloquear scans de portas na rede** - detecta e bloqueia tentativas de encontrar quais portas estão abertas.

Os scans de portas são frequentemente usados pelos hackers para descobrir que portas se encontram abertas no seu computador. Então eles poderão entrar no seu computador se descobrirem uma porta menos segura ou vulnerável.

## Configurar intensidade de alertas

Bitdefender Total Security foi desenvolvido para ser o mínimo intrusivo possível. Em condições normais, não é necessário tomar decisões sobre permitir ou impedir conexões ou ações tentadas pelos aplicativos em execução no seu sistema.

Se você deseja ter controle completo nas decisões:

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



2. Na janela **GERAL** ligue o **Modo paranoico** clicando no botão correspondente.



## Nota

Quando o Modo Paranoico estiver ligado, os recursos **Autopilot** e **Perfis** serão desligados automaticamente.

O **Modo Paranoico** poderá ser usado simultaneamente com o **Modo de Bateria**.

Enquanto o Modo Paranoico estiver ligado, você receberá notificações para tomar ações cada vez que acontecer o seguinte:

- Um aplicativo tenta conexão à Internet.
- Uma aplicação tenta realizar uma ação considerada suspeita pelo **Controle Ativo de Ameaças**.

O alerta contém informações detalhadas sobre o aplicativo e o comportamento detectado. Selecione **Permitir** ou **Impedir** a ação usando o botão respectivo.

## 4.8. Proteção contra Ransomware

Ransomwares são softwares maliciosos que atacam sistemas vulneráveis travando-os e logo exigindo dinheiro para permitir que o usuário retome controle de seu sistema. Esse software malicioso finge ser inteligente ao exibir mensagens falsas para assustar o usuário, induzindo-o a realizar o pagamento solicitado.

A infecção pode se espalhar por meio de e-mails de spam, downloads de anexos ou ao se visitarem sites infectados e instalar aplicativos maliciosos sem informar ao usuário sobre o que está ocorrendo com seu sistema.

Ransomwares podem ter um dos seguintes comportamentos, prevenindo que o usuário acesse seu sistema:



- Criptar dados privados e pessoais sem a possibilidade de descriptação até que um resgate seja pago pela vítima.
- Travar a tela do computador e exibir uma mensagem pedindo dinheiro. Neste caso, nenhum arquivo é criptado, mas o usuário é forçado a realizar o pagamento.
- Bloquear a execução de aplicativos.



Utilizando a última tecnologia, a Proteção contra Ransomwares do Bitdefender assegura a integridade do sistema ao proteger áreas essenciais do sistema contra danos, sem prejudicar o desempenho do sistema. Contudo, você pode desejar proteger seus arquivos pessoais, como documentos, fotos, filmes ou os arquivos que você armazena na nuvem.

## Ativar ou desativar a Proteção contra Ransomwares



Para desativar o módulo de Proteção contra Ransomware:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **PROTEÇÃO CONTRA RANSOMWARE**.
4. Clique no botão correspondente para ativar ou desativar a **Proteção contra Ransomware**.

Sempre que um aplicativo tentar acessar um arquivo protegido, um pop-up do Bitdefender será exibido. Você poderá permitir ou negar o acesso.

## Proteja seus arquivos pessoais contra ataques de ransomwares

Se você deseja proteger arquivos pessoais:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **PROTEÇÃO CONTRA RANSOMWARE**.
4. Clique no botão **ADD**.
5. Vá para a pasta que queira proteger. Em seguida, clique em **OK** para adicionar a pasta selecionada ao ambiente de proteção.

As configurações de fábrica já protegem as pastas Documentos, Imagens, Vídeos, Músicas, Área de Trabalho, Documentos públicos, Imagens Públicas, Músicas Públicas e Área de Trabalho Pública contra ataques de malware.




## Nota

Pastas personalizadas somente podem ser protegidas para os usuários atuais. Arquivos de sistema e de aplicativos não podem ser adicionadas às exceções.

## Configurando os aplicativos confiáveis


A proteção contra ransomware pode ser desativada para alguns aplicativos, mas apenas aqueles em que você confia devem ser adicionados à lista.

Para adicionar aplicações de confiança às exclusões:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **PROTEÇÃO CONTRA RANSOMWARE**, selecione **Aplicações confiáveis**.
4. Clique em **Adicionar** e procure os aplicativos que deseja proteger.
5. Clique em **OK** para adicionar o aplicativo selecionado ao ambiente de proteção.

## Configurando os aplicativos bloqueados

As aplicações que tentam mudar ou apagar arquivos protegidos podem ser sinalizadas como potencialmente inseguras e adicionadas à lista de aplicações bloqueadas. Se uma aplicação como essa for bloqueada e você tiver certeza de que seu comportamento é normal, pode excluí-la seguindo os seguintes passos:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **PROTEÇÃO CONTRA RANSOMWARE**, selecione **Aplicações bloqueadas**.
4. Clique em **Permitir** e procure a aplicação que você tem certeza de que é segura.
5. Clique em **OK** para adicionar a aplicação selecionada à lista confiável.



## Proteção na inicialização

Sabe-se que muitos aplicativos de malware são configurados para serem executados na inicialização do sistema, o que pode danificar seriamente



uma máquina. A Proteção na inicialização do Bitdefender verifica todas as áreas essenciais do sistema antes que todos os arquivos sejam carregados, sem impacto no desempenho do sistema. Simultaneamente, é fornecida proteção contra certos ataques que dependem da execução de códigos em stack ou heap, injeções de código ou ganchos em certas bibliotecas dinâmicas.

Para desativar a proteção na inicialização:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **PROTEÇÃO CONTRA RANSOMWARE**.
4. Clique no botão correspondente para ativar ou desativar a **Proteção na inicialização**.

## 4.9. Segurança Safepay para transações online

O computador está rapidamente se tornando a principal ferramenta para compras e operações bancárias online. Pagar contas, transferir dinheiro, comprar praticamente qualquer coisa que possa imaginar nunca foi tão fácil e rápido.

Isto engloba o envio de dados pessoais, dados de contas bancárias e cartão de crédito, senhas e outros tipos de informação privada pela Internet; em outras palavras, exatamente o tipo de fluxo de informação que os cibercriminosos estão muito interessados em obter. Os hackers são incansáveis nos seus esforços para roubar estas informações, portanto todo cuidado é pouco em manter seguras as suas transações online.

O Bitdefender Safepay™ é, acima de tudo, um navegador protegido, um ambiente projetado para manter a sua atividade bancária, suas compras on-line e qualquer outra transação online privada e segura.

Para a melhor proteção à privacidade, o Gerenciador de Senhas do Bitdefender foi integrado ao Bitdefender Safepay™ para proteger suas credenciais sempre que você desejar acessar locais privados online. Para mais informações, por favor consulte *"Proteção do Gerenciador de Senhas para suas credenciais"* (p. 149).

O Bitdefender Safepay™ oferece os seguintes recursos:




- O mesmo bloqueia o acesso à sua área de trabalho e qualquer tentativa de capturar imagens de sua tela.
- Ele protege suas senhas enquanto você navega.
- O mesmo apresenta um teclado virtual que, quando usado, torna impossível para os hackers lerem as teclas que usar.
- É completamente independente dos outros navegadores.
- Vem com uma proteção de hotspot embutida para ser usada quando o seu computador se conecta a redes Wi-fi não-seguras.
- Suporta bookmarks e permite-lhe navegar entre os seus sites favoritos de bancos/compras.
- Não está limitado ao banking e às compras online. Qualquer página web pode ser aberta no Bitdefender Safepay™.

## Usando o Bitdefender Safepay™

Por padrão, o Bitdefender detecta quando você entra em uma página de banco ou de compras em qualquer navegador de seu computador e pergunta se você gostaria de usar o Bitdefender Safepay™.

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

- Na **interface do Bitdefender**:
  1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
  2. Clique no botão de ação **Safepay**.
- Do Windows:
  - No **Windows 7**:
    1. Clique **Iniciar** e acesse **Todos os Programas**.
    2. Clique em **Bitdefender**.
    3. Clique em **Bitdefender Safepay™**.
  - No **Windows 8 e Windows 8.1**:

Encontre o Bitdefender Safepay™ na tela inicial do Windows (por exemplo, você pode digitar "Bitdefender Safepay™" diretamente na tela Inicial) e então clique no ícone.



## ● No Windows 10:











Digite "Bitdefender Safepay™" na caixa de pesquisa da barra de tarefas e então clique no ícone correspondente.

### Nota

CAso o plug-in do Adobe Flash Player não esteja instalado ou esteja desatualizado, será apresentada um mensagem do Bitdefender. Clique no botão correspondente para continuar.

Após o processo de instalação, você terá que reabrir o navegador Bitdefender Safepay™ manualmente para continuar o seu trabalho.

Se você estiver acostumado com navegadores de Internet, não terá nenhum problema para usar o Bitdefender Safepay™ - ele parece e se comporta como um navegador comum:

- digite as URLs que deseja acessar na barra de endereços.
- adicione abas para visitar múltiplas páginas na janela do Bitdefender Safepay™ clicando em .
- navegue para a frente e para trás e atualize as páginas usando    respectivamente.
- acesse **configurações** do Bitdefender Safepay™ clicando em  e escolhendo **Configurações**.
- proteja suas senhas com o **Gerenciador de senhas** clicando em .
- gerencie seus **bookmarks** clicando em  ao lado da barra de endereço.
- abra o teclado virtual clicando em .
- aumente ou diminua o tamanho do navegador pressionando as teclas **Ctrl** e **+/-** simultaneamente no teclado numérico.
- veja informações sobre seu Bitdefender clicando em  e escolhendo **Sobre**.
- imprima as informações importantes clicando .

### Nota

Para alternar entre o Bitdefender Safepay™ e a área de trabalho do Windows, pressione as teclas **Alt+Tab** ou clique no botão **Minimizar**.





## Configurando definições

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

- Em **Configurações Gerais** você pode configurar:

### Comportamento do Bitdefender Safepay™

Escolha o que deve de ser feito ao acessar a um site online de compras ou de bancos no seu navegador habitual:

- Abrir sites automaticamente no Safepay.
- Recomendar-me a usar o Safepay.
- Não me recomendar o uso do Safepay.

### Lista de domínios

Escolha como o Bitdefender Safepay™ irá se comportar quando você visitar páginas com domínios específicos no seu navegador adicionando-os à lista de domínios e selecionando o comportamento para cada um:

- Abrir automaticamente no Bitdefender Safepay™.
- Que o Bitdefender avise sobre a ação a ser tomada.
- Nunca utilizar o Bitdefender Safepay™ ao visitar uma página do domínio em um navegador comum.

### Bloqueando pop-ups

Você pode optar por bloquear pop-ups clicando no botão correspondente.

Você também pode criar uma lista de páginas que possam exibir pop-ups. A lista deve conter apenas os websites em que você confia plenamente.

Para adicionar uma página à lista, insira seu endereço no campo correspondente e clique em **Adicionar domínio**.

Para remover uma página da web da lista, selecione o X correspondente à entrada desejada.

### Permitir proteção de hotspot.

Você pode permitir uma proteção extra quando estiver conectado a redes Wi-fi inseguras habilitando esta ferramenta.

Acesse **“Proteção Hotspot em redes não-seguras.”** (p. 149) para mais informações.



- Na área **Configurações Avançadas**, as seguintes opções estão disponíveis:

### Gerenciar Plugins

Você pode escolher se deseja ativar ou desativar plugins específicos no Bitdefender Safepay™.

### Gerenciar certificados

Você pode importar certificados do seu sistema para uma loja de certificados.

Selecione **Importar certificado** e siga o assistente para usar os certificados no Bitdefender Safepay™.

### Exibir o Teclado Virtual automaticamente em campos de senha.

O teclado virtual aparecerá automaticamente quando o campo de senha for selecionado.

Use o botão correspondente para ativar ou desativar a função.


### Confirmar antes de imprimir

Ative esta opção se deseja dar sua confirmação antes que o processo de impressão se inicie.

## Gerenciando bookmarks

Caso você tenha desabilitado a detecção automática de alguma ou de todas as páginas, ou o Bitdefender simplesmente não detectar algumas páginas, você pode adicionar favoritos ao Bitdefender Safepay™ para que você possa abrir as suas páginas favoritas com facilidade no futuro.

Siga estes passos para adicionar um URL aos favoritos do Bitdefender Safepay™

1. Clique no ícone  ao lado da barra de endereços para abrir a página de Favoritos.



### Nota

A página de Favoritos abre por padrão quando você executa o Bitdefender Safepay™.

2. Clique no botão **+** para adicionar um novo bookmark.
3. Inserir o URL e o título do bookmark e clique em **Criar**. Marque a opção **Abrir automaticamente no Safepay** se você quiser que a página favorita




abra com o Bitdefender Safepay™ todas as vezes que você acessá-la. A URL é também adicionada à lista de Domínios na página de **definições**.

## Proteção Hotspot em redes não-seguras.

Ao usar o Bitdefender Safepay™ em redes de Wi-fi inseguras (por exemplo, um hotspot público), uma proteção extra é oferecida pelo recurso Proteção de Hotspot. Este serviço criptografa as comunicações de Internet em conexões não-seguras, ajudando assim a manter a sua privacidade sem importar a que rede esteja ligado.

A proteção de hotspot funciona apenas se o seu computador estiver conectado a uma rede insegura.

A conexão segura será inicializada e uma mensagem irá aparecer na janela do Bitdefender Safepay™ quando a conexão for feita. O símbolo  aparece à frente da URL na barra de endereços para o ajudar a identificar facilmente as conexões seguras.

Pode ser necessário confirmar a ação.

## 4.10. Proteção do Gerenciador de Senhas para suas credenciais

Utilizamos os nossos computadores para efetuar compras online ou pagar as contas, para nos ligarmos a plataformas de comunicação social ou para iniciar sessão em aplicativos de mensagens instantâneas.

Mas como todos sabemos, nem sempre é fácil memorizar a senha!

E se não formos cuidadosos ao navegar online, as nossas informações privadas, tais como endereço de e-mail, ID de mensagens instantâneas ou os dados do cartão de crédito podem ficar comprometidas.

Guardar as suas senhas ou os seus dados pessoais numa folha ou no computador pode ser perigoso, pois estes podem ser acessados e utilizados por pessoas que desejam roubar e utilizar essas informações. E memorizar todas as senhas definidas para as suas contas online ou para os seus websites favoritos não é uma tarefa fácil.

Portanto, há alguma forma de garantir que encontramos as nossas senhas quando necessitamos das mesmas? E podemos ter a certeza de que as nossas senhas secretas estão sempre seguras?



O Gerenciador de Senhas o ajuda a lembrar de suas senhas, protege sua privacidade e fornece uma navegação segura.

Utilizando uma única senha mestre para acessar suas credenciais, o Gerenciador de Senhas facilita sua vida protegendo suas senhas em uma Carteira.


Para oferecer a melhor proteção às suas atividades online, o Gerenciador de Senhas é integrado ao Bitdefender Safepay™ e fornece uma solução unificada para os vários meios em que seus dados podem ser comprometidos.

O Gerenciador de Senhas protege as seguintes informações privadas:

- Informações pessoais, tais como endereço de e-mail e número de telefone
- Credenciais de login para websites
- Informações de contas bancárias ou o número do cartão de crédito
- Dados de acesso às contas de e-mail
- Senhas para os aplicativos
- Senhas para redes Wi-Fi

## Crie uma nova base de dados da Carteira

A Carteira do Bitdefender é onde você pode armazenar seus dados pessoais. Para uma experiência de navegação mais fácil, você precisa criar um banco de dados da Carteira da seguinte forma:


1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **GERENCIADOR DE SENHAS**, selecione **Criar nova Carteira**.
4. Selecione o botão **Criar novo**.
5. Digite as informações necessárias nos campos correspondentes.
  - Título da Carteira - digite um nome personalizado para seu banco de dados da Carteira.
  - Senha Mestre - digite uma senha para sua Carteira.
  - Redigitar Senha - redigite a senha que você definiu.
  - Dica - digite uma dica para lembrar de sua senha.



6. Clique em **Continuar**.
7. Nesta etapa, você pode escolher armazenar suas informações na nuvem. Se você selecionar Sim, suas informações bancárias permanecerão armazenadas localmente em seu dispositivo. Escolha a opção desejada e então clique em **Continuar**.
8. Selecione o navegador da Internet de onde você deseja importar credenciais.
9. Clique em **Finalizar**.



## Importar uma base de dados existente

Para importar um banco de dados da Carteira armazenado localmente:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **GERENCIADOR DE SENHAS**, selecione **Criar nova Carteira**.
4. Selecione o botão **De um local**.
5. Procure pelo local do banco de dados da sua Carteira e selecione-o (o arquivo .db).
6. Clique em **Abrir**.
7. Dê um nome à sua carteira e digite a senha designada quando ela foi criada.
8. Clique em **Importar**.
9. Selecione os programas de onde deseja que a Carteira importe credenciais, depois o botão **Finalizar**.

## Exportar a base de dados da Carteira

Para exportar o banco de dados da sua Carteira:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **GERENCIADOR DE SENHAS**, selecione **Minhas Carteiras**.
4. Clique no ícone  na Carteira desejada, e então selecione **Exportar**.



5. Procure pelo local do banco de dados da sua Carteira e selecione-o (o arquivo .db).
6. Clique em **Guardar**.





## Nota

A Carteira precisa ser aberta para que o botão **Exportar** esteja disponível. Se a Carteira que você precisa exportar estiver bloqueada, clique no botão **ATIVAR CARTEIRA** e depois digite a senha designada quando ela foi criada.

## Sincronize suas carteiras na nuvem

Para ativar ou desativar a sincronização das carteiras na nuvem:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **GERENCIADOR DE SENHAS**, selecione **Minhas Carteiras**.
4. Clique no ícone  na Carteira desejada, e então selecione **Configurações**.
5. Escolha a opção desejada na janela que aparecer, e então clique em **Salvar**.




## Nota

A Carteira precisa ser aberta para que o botão **Exportar** esteja disponível. Se a Carteira que você precisa exportar estiver bloqueada, clique no botão **ATIVAR CARTEIRA** e depois digite a senha designada quando ela foi criada.

## Gerenciar as suas credenciais da Carteira

Para gerenciar suas senhas:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **GERENCIADOR DE SENHAS**, selecione **Minhas Carteiras**.
4. Selecione o banco de dados da Carteira desejado na janela **MINHAS CARTEIRAS**, depois clique no botão **ATIVAR CARTEIRA**.
5. Digite a senha mestre e depois clique em **OK**.

Uma nova janela aparece. Selecione a categoria desejada na parte superior da janela:





- Identidade
- Websites
- Online banking
- E-mails
- Aplicativos
- Redes Wi-Fi

## Adicionar/ editar as credenciais

- Para adicionar uma nova senha, escolha a categoria desejada acima, clique em **+ Adicionar item**, insira as informações nos campos correspondentes e clique no botão **Salvar**.
- Para editar uma entrada da lista, selecione-a e clique no botão **Editar**.
- Para remover uma entrada da tabela, selecione-a e clique no botão **Eliminar**.



## Ativando e desativando a proteção do Gerenciador de Senhas

Para ativar ou desativar a proteção do Gerenciador de Senhas:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **GERENCIADOR DE SENHAS**.
4. Use o botão correspondente para ativar ou desativar o Gerenciador de Senhas.

## Alterando as configurações do Gerenciador de Senhas

Para configurar a senha mestre detalhadamente:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **GERENCIADOR DE SENHAS**.



#### 4. Selecione a aba **CONFIGURAÇÕES DE SEGURANÇA**.

As seguintes opções estão disponíveis:

- **Solicitar a minha senha mestre sempre que eu acessar o meu PC** - você será solicitado a inserir a senha mestre ao acessar o computador.
- **Solicitar senha principal ao abrir navegadores e aplicativos** - será solicitada a senha principal ao acessar um navegador ou aplicativo.
- **Bloquear automaticamente a Carteira quando deixa o meu PC sem supervisão** - será solicitada a senha principal quando regressar ao seu computador após 15 minutos.





#### **Importante**

Não se esqueça da sua senha mestre e guarde-a num local seguro. Caso esqueça a senha, será necessário reinstalar o programa ou contatar o suporte do Bitdefender.

## Melhore a sua experiência

Para selecionar os navegadores ou aplicações onde deseja integrar o Gerenciador de Senhas:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **GERENCIADOR DE SENHAS**.
4. Selecione a aba **PLUGINS**.

Marque um aplicativo para utilizar o Gerenciador de Senhas e melhorar sua experiência:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safepay







## Configurando o Preenchimento Automático

O recurso Preenchimento Automático simplifica a conexão aos seus websites favoritos ou login nas suas contas online. Na primeira vez que você inserir suas informações de login e informações pessoais em um navegador de Internet, eles estarão automaticamente protegidos na Carteira.

Para configurar o **Preenchimento automático**:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **GERENCIADOR DE SENHAS**.
4. Selecione a aba **Configurações de Preenchimento automático**.
5. Configure as seguintes opções:

- **Configure como a Carteira protege suas credenciais:**

- **Salvar as credenciais automaticamente na Carteira** - as credenciais de login e outras informações pessoais como os detalhes do seu cartão de crédito e detalhes pessoais são salvos e atualizados automaticamente na sua Carteira.
- **Perguntar-me sempre** - você será sempre perguntado se pretende adicionar as suas credenciais à Carteira.
- **Não salvar, atualizarei as informações manualmente** - as credenciais só podem ser atualizadas na Carteira manualmente.

- **Preenchimento Automático de Credenciais de Login:**

- **Preencher automaticamente e sempre as credenciais de início de sessão** - as credenciais são inseridas automaticamente no browser.


- **Formulários de preenchimento automático:**

- **Mostre minhas opções de preenchimento quando eu visitar uma página com as formulários** - um pop-up com as opções de preenchimento aparecerá sempre que o Bitdefender detectar que você deseja realizar um pagamento on-line ou fazer um login.



## Controle as informações do Gerenciador de Senhas de seu navegador

Você pode controlar facilmente as informações do Gerenciador de Senhas diretamente de seu navegador, para ter fácil acesso a todos os dados importantes. O plugin da Carteira do Bitdefender é suportado pelos seguintes navegadores: Google Chrome, Internet Explorer e Mozilla Firefox, e também é integrado ao Safepay.

Para acessar a extensão da Carteira do Bitdefender, abra seu navegador, permita a instalação do plugin e clique no ícone  na barra de ferramentas.

A extensão da Carteira do Bitdefender contém as seguintes opções:

- Abrir Carteira - abre a Carteira.
- Fechar Carteira - fecha a Carteira.
- Páginas web - abre um submenu com todos os logins de sites armazenados na Carteira. Clique em **Adicionar página** para adicionar novas páginas à lista.
- Preencher formulário - abre o submenu contendo a informação adicionada para uma categoria específica. Aqui você pode adicionar novos dados à sua Carteira.
- Gerador de Senhas - permite que você gere senhas aleatórias que você pode utilizar para contas novas e existentes. Clique em **Mostrar configurações avançadas** para personalizar a complexidade da senha.
- Configurações - abre a janela de configurações do Gerenciador de Senhas.
- Relatar problema - relate quaisquer problemas que encontrar com o Gerenciador de Senhas do Bitdefender.

### 4.11. Consultor Parental

A função de Consultor Parental permite que você controle o acesso à Internet e a aplicativos específicos para cada dispositivo que tenha a função instalada. Uma vez que você tenha configurado o Consultor Parental, você poderá descobrir facilmente o que seu filho está fazendo nos dispositivos que usa e onde ele esteve nas últimas 24 horas. Ademais, para ajudá-lo a saber melhor o que seu filho está fazendo, o aplicativo apresenta estatísticas sobre suas atividades e interesses.



Tudo o que precisa é um computador com acesso à Internet e um navegador de Internet.

Você pode configurar o Consultor Parental para bloquear:

- Páginas web inapropriadas.
- aplicações tais como: jogos, programas de partilha de arquivos e outros.
- contatos específicos que são proibidos de entrar em contato telefônico com seu filho.

Verifique as atividades de seus filhos e altere as configurações do Consultor Parental utilizando a conta Bitdefender desde qualquer computador ou dispositivo móvel conectado à Internet.


## Acessando o Consultor Parental - MEUS FILHOS

Quando você acessa a seção Consultor Parental, a janela **MEUS FILHOS** fica disponível. Aqui você pode visualizar e editar todos os perfis que criou para seus filhos. Os perfis aparecem como cartões de perfil, permitindo que você os controle com rapidez e verifique seu estado atual com apenas uma olhada.

Assim que você criar um perfil, poderá personalizar configurações mais detalhadas para monitorar e controlar o acesso à Internet e a aplicativos específicos para seus filhos.

Você pode acessar o Consultor Parental da Bitdefender Central em qualquer computador ou dispositivo móvel conectado com a internet.

Acesse sua conta Bitdefender:

- Em qualquer dispositivo com acesso à Internet:
  1. Acesse **Bitdefender Central**.
  2. Inicie sessão na sua conta Bitdefender com o seu endereço de e-mail e senha.
  3. Selecione o módulo **Consultor Parental**.
  4. Na janela **MEUS FILHOS**, você pode gerenciar e configurar os perfis do Consultor Parental para cada dispositivo.
- A partir de sua interface Bitdefender:
  1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
  2. Clique no botão **VER MÓDULOS**.



3. No módulo **CONSULTOR PARENTAL**, selecione **Configurar**.

Você será redirecionado à página da conta Bitdefender. Assegure-se de acessar a conta com suas creden

4. Selecione o módulo **Consultor Parental**.

5. Na janela **MEUS FILHOS**, você pode gerenciar e configurar os perfis do Consultor Parental para cada dispositivo.



## Nota

Certifique-se que tem a sessão iniciada com a conta de administrador. Somente usuários com privilégios administrativos no sistema (administradores) podem acessar e configurar o Consultor Parental.

## Adicionando o perfil do seu filho

Para começar a monitorar as atividades de seus filhos, você precisa configurar um perfil e instalar o Agente Consultor Parental do Bitdefender em dispositivos que ele utiliza.

Para adicionar o perfil do seu filho ao Consultor Parental:

1. Acesse o painel do **Consultor Parental** na Bitdefender Central.
2. Clique em **ADICIONAR PERFIL** no lado direito da janela **MEUS FILHOS**.
3. Insira as informações específicas nos campos correspondentes, como nome, gênero e data de nascimento. Para adicionar uma foto de perfil, clique no link **Escolher arquivo**. Clique em **PRÓXIMO PASSO** para continuar.

Com base no desenvolvimento infantil, definir a idade da criança carrega automaticamente as especificações consideradas apropriadas para sua faixa etária.

4. Se o dispositivo do seu filho já tem o Bitdefender Total Security instalado, selecione o seu dispositivo na lista disponível e depois selecione a conta que deseja monitorar. Clique em **SALVAR**.

Se seu filho usa um dispositivo Android e o aplicativo do Consultor Parental Bitdefender não estiver instalado, clique em **ADICIONAR DISPOSITIVO**. A opção do **Consultor Parental Bitdefender para Android** é selecionada por padrão. Clique em **PRÓXIMO PASSO** para continuar.




5. Digite o endereço de e-mail para onde devemos enviar o link de download do Consultor Parental Bitdefender e depois clique em **ENVIAR LINK DE INSTALAÇÃO**.

Em dispositivos com Windows, o Bitdefender Total Security que você incluiu em sua assinatura deverá ser baixado e instalado. Em dispositivos Android, o Agente Consultor Parental do Bitdefender deverá ser baixado e instalado.

## Como atribuir o mesmo perfil a vários dispositivos

É possível atribuir o mesmo perfil a vários dispositivos pertencentes a mesma criança, de forma que as mesmas restrições sejam aplicadas.

Para atribuir o perfil a vários dispositivos:

1. Acesse **Bitdefender Central**.
2. Selecione o módulo **Consultor Parental**.
3. Clique no ícone  no cartão de perfil desejado, e então selecione **Dispositivos**.
4. Selecione da lista os dispositivos disponíveis para os quais você deseja atribuir o perfil.

Se seu filho usa um dispositivo Android e o aplicativo do Consultor Parental Bitdefender não estiver instalado, clique em **ADICIONAR DISPOSITIVO**. A opção do **Consultor Parental Bitdefender para Android** é selecionada por padrão. Clique em **PRÓXIMO PASSO** para continuar.

Digite o endereço de e-mail para onde devemos enviar o link de download do Consultor Parental Bitdefender e depois clique em **ENVIAR LINK DE INSTALAÇÃO**.

5. Após concluir o processo de instalação no novo dispositivo, selecione-o na lista para aplicar o perfil.
6. Selecione **SALVAR**.

## Vinculando o Consultor Parental à Bitdefender Central

Para monitorar a atividade online de seus filhos no Android, você deve vincular seu dispositivo à sua Bitdefender, acessando a conta no aplicativo.

Para vincular o dispositivo à sua conta Bitdefender:



1. Selecione o botão **Google Play** que aparece no e-mail enviado pelo nosso servidor, depois instale o aplicativo.

Se você não escolheu na sua conta Bitdefender enviar um link para download para o e-mail do seu filho, vá para a Google Play e procure pelo aplicativo do Consultor Parental Bitdefender.

2. Abra o aplicativo de Consultor Parental.
3. Leia o **Acordo de Licença de Usuário Final** e depois toque em **CONTINUAR**.
4. Acesse sua conta Bitdefender existente.

Se você não tiver uma conta, escolha criar uma nova conta usando a opção correspondente.

5. Toque em **Ativar acesso de uso** e marque a caixa correspondente.
6. Ative as permissões de administrador do dispositivo para o aplicativo tocando em **ATIVAR**.

Isso prevenirá que seu filho desinstale o Agente Consultor Parental.

## Monitorando a atividade da criança

O Bitdefender ajuda a manter o registro do que seus filhos estão fazendo online.

Desse modo, você sempre poderá descobrir exatamente que páginas eles visitaram, que aplicativos utilizaram ou que atividades foram bloqueadas pelo Consultor Parental.

Dependendo das configurações que você definir, os relatórios podem conter informações detalhadas sobre cada evento, como:

- O status do evento.
- A severidade da notificação.
- O nome do dispositivo.
- A data e a hora em que ocorreu o evento.

Para monitorar o tráfego na internet, as aplicações acessadas ou a atividade no Facebook do seu filho:

1. Acesse o painel do **Consultor Parental** na Bitdefender Central.
2. Selecione o cartão de dispositivo desejado.



No janela **Atividades**, você pode ver as informações que lhe interessam. Você também pode selecionar o link **Ver atividade de hoje** no cartão do dispositivo monitorado para ser redirecionado para a janela **Atividades**.

## Configurando os Ajustes Gerais


O Consultor Parental já vem configurado de fábrica para registrar as atividades dos seus filhos.

Para receber notificações por e-mail:

1. Acesse o painel do **Consultor Parental** na Bitdefender Central.
2. Selecione a aba **Configurações** no canto superior direito.
3. Habilite a opção correspondente para receber relatórios de atividade.
4. Introduza o endereço eletrônico para onde serão enviadas das notificações por correio eletrônico.
5. Receber notificações via e-mail para os seguintes:
  - Sites bloqueados
  - App bloqueados
  - Áreas restritas
  - Ligação ou SMS recebida de um número de telefone bloqueado
  - Remoção do aplicativo de Consultor Parental para Facebook
6. Clique em **SALVAR**.

## Editando um perfil


Para editar um perfil existente:

1. Acesse **Bitdefender Central**.
2. Selecione o painel **Consultor Parental**.
3. Clique no ícone  no cartão de perfil desejado, e então selecione **Editar**.
4. Depois de personalizar as configurações desejadas, selecione **SALVAR**.

## Removendo um perfil

Para remover um perfil existente:



1. Acesse **Bitdefender Central**.
2. Selecione o painel **Consultor Parental**.
3. Clique no ícone  no cartão de perfil desejado, e então selecione **Remove**.
4. Confirme sua escolha.

## Configurando perfis do Consultor Parental

Para iniciar o monitoramento de seus filhos, um perfil deverá ser designado ao dispositivo que tem o Agente Consultor Parental do Bitdefender instalado.

Após criar um perfil para seu filho, você poderá personalizar configurações mais detalhadas para monitorar e controlar o acesso à Internet e a aplicativos específicos.

Para começar a configurar um perfil, selecione o cartão do perfil desejado na janela **MEUS FILHOS**.

Clique em uma aba para configurar a função correspondente do Consultor Parental para o dispositivo:

- **Atividades** - exibe todas as atividades, interesses, locais e interações do dia com amigos.
- **Aplicativos** - permite bloquear o acesso a certos aplicativos, como jogos, programas de mensagens, filmes, etc.
- **Websites** - permite filtrar a navegação na internet.
- **Contatos do telefone** - aqui você pode especificar quais contatos da lista do seu filho têm permissão para entrar em contato com ele por telefone.
- **Localização do seu filho** - aqui você pode determinar locais que são seguros ou não para o seu filho.
- **Social** - permite que você bloqueie o acesso a redes sociais.
- **Horário** - permite bloquear o acesso aos dispositivos que você especificou no perfil do seu filho.

## Atividade

A janela Atividades lhe dá informações detalhadas sobre as atividades dos seus filhos das últimas 24 horas, dentro e fora de casa. Para ver as atividades





dos dias anteriores, clique no ícone de calendário no canto superior esquerdo da janela.

Dependendo da atividade, essa janela pode incluir informações sobre:

- **Locais** - aqui você pode visualizar os locais onde seu filho esteve durante o dia.
- **Interesses** - aqui você pode visualizar informações sobre que categorias de páginas da Internet seu filho visitou. Clique no link **Revisar conteúdo inapropriado** para permitir ou negar acesso a interesses específicos.
- **Interações Sociais** - aqui é possível visualizar os contatos com os quais seu filho se comunicou. Clique no link **Administrar contatos** para selecionar os contatos com os quais seu filho pode se comunicar ou não.
- **Aplicativos** - aqui você pode visualizar os aplicativos que seu filho utilizou. Clique no link **Rever as restrições de aplicativos** para bloquear ou permitir o acesso a aplicativos específicos.
- **Atividade diária** - aqui você pode ver o tempo passado online em todos os dispositivos atribuídos ao seu filho e o local onde ele esteve ativo. As informações coletadas são do dia atual.

## Aplicativos

A janela Aplicativos ajuda a bloquear a execução de aplicativos. Jogos, mídia e programas de mensagens instantâneas, assim como outras categorias de programa podem ser bloqueadas deste modo.

O módulo pode ser ativado ou desativado utilizando o botão correspondente.

Para configurar o Controle de Aplicações para uma determinada conta de utilizador:

1. Uma lista com cartões será exibida. Os cartões representam os aplicativos que seu filho utiliza.
2. Selecione o cartão com o aplicativo que você deseja que seu filho pare de utilizar.

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



## Websites

A janela Websites permite bloquear websites com conteúdo inadequado. Sites que hospedam vídeos, jogos, mídia e programas de mensagens instantâneas, assim como outras categorias de conteúdo negativo, podem ser bloqueadas desse modo.

O módulo pode ser ativado ou desativado utilizando o botão correspondente.

Dependendo da idade que você definiu para seu filho, a lista de Interesses já vem com uma variedade de categorias ativas. Para permitir ou negar acesso a uma categoria específica, clique nela.

Dependendo da idade que você definiu para seu filho, a lista de Interesses já vem com uma variedade de categorias ativas.

## Permitir ou bloquear um website

Para permitir ou negar acesso a uma categoria específica, clique nela.

1. Clique no botão **GERENCIAR**.
2. Digite o endereço da página que deseja permitir ou bloquear no campo correspondente.
3. Selecione **Permitir** ou **Bloquear**.
4. Clique em **FINISH** para salvar as alterações.

## Contatos Telefônicos

A janela Contatos Telefônicos permite especificar quais amigos da lista do seu filho podem ou não entrar em contato com ele por telefone.

Para restringir um número de telefone específico, você precisa primeiro adicionar ao perfil do seu filho o dispositivo Android que ele usa seguindo estes passos:

1. Selecione a aba **Consultor Parental** na Bitdefender Central.
2. Clique no link **Instalar o Consultor Parental em um dispositivo** no cartão desejado.
3. Clique em **ADICIONAR DISPOSITIVO** na janela que aparece.
4. A opção do **Consultor Parental Bitdefender para Android** é selecionada por padrão. Clique em **PRÓXIMO PASSO** para continuar.



5. Selecione o perfil da criança para qual deseja estabelecer restrições.

6. Selecione a aba **Contatos telefônicos**.

Uma lista com cartões será exibida. Os cartões representam os contatos do telefone de seu filho.

7. Selecione o cartão com o número de telefone que você deseja bloquear.

O símbolo de marcação que aparecerá indica que seu filho não receberá ligações do número de telefone selecionado.

Para bloquear números desconhecidos, ative a opção **nenhuma interação de identificação de chamadas**.

## Localização do seu filho

Visualizar a localização atual do dispositivo no Google Maps. A localização é atualizada a cada 5 segundos, para que você possa rastreá-lo se estivesse em movimento.

A precisão da localização depende de como o Bitdefender é capaz de determiná-la:

- Caso o GPS esteja ativado no aparelho, sua localização pode ser determinada dentro de dois metros, desde que esteja ao alcance dos satélites GPS (ou seja, fora de um edifício).
- Se o aparelho estiver dentro de casa, sua localização pode ser determinada em dezenas de metros caso o Wi-Fi esteja ativado e existam redes sem fio disponíveis no alcance.
- Caso contrário, a localização será determinada utilizando somente informações a partir da rede móvel, que pode oferecer uma precisão não melhor que várias centenas de metros.

## Configurando a localização

Para se assegurar de que seu filho vai a certos locais, você pode criar uma lista de locais seguros e não seguros.

Para configurar um local:

1. Clique em **Dispositivos** na janela **Lugares**.
2. Clique em **ESCOLHER DISPOSITIVOS** e então selecione o dispositivo que você deseja configurar.



3. Na janela **Áreas**, clique no botão **ADICIONAR ÁREA**.
4. Escolha o tipo de local, **SEGURO** ou **RESTRITO**.
5. Digite um nome válido para a área onde seu filho tem ou não permissão para ir.
6. Defina a distância que deverá ser utilizada para monitoramento na barra **Raio**.
7. Clique em **ADICIONAR ÁREA** para salvar suas configurações.

## Social

O Consultor Parental monitora a conta de seu filho no Facebook e relata as principais atividades que ocorrem.

Essas atividades online são verificadas e você receberá um aviso caso elas sejam ameaças à privacidade de seu filho.

Os elementos monitorados da conta online incluem:

- Informações da Conta
- Curtir páginas
- imagens subidas

Para configurar a proteção do Facebook para uma conta específica, digite o e-mail da conta do seu filho e depois clique em **ENVIAR**.

Informe seu filho sobre suas intenções e peça a ele para clicar no botão **PROTEGER CONTA** que ele recebeu no e-mail.

Para acessar a conta do Facebook monitorada, clique no link **Ver no Facebook**.

Para parar de monitorar a conta, use o botão **DESVINCULAR CONTA** no topo.


Para ser avisado por e-mail quando seu filho remover o aplicativo do Consultor Parental do seu dispositivo, marque a caixa correspondente.

## Horário

A janela Horário permite restringir o acesso aos dispositivos que você especificou no perfil do seu filho. As restrições podem ser configuradas para qualquer horário durante a hora de escola e fins de semana.

Para começar a configurar as restrições de horário durante a noite:



1. Na área **HORA DE DORMIR**, selecione as caixas **Noites em semana de aula** e **Noites em fins de semana**.
2. Clique no ícone  das caixas correspondentes e use as setas para cima e para baixo para estabelecer os intervalos de tempo durante os quais o acesso deve ser bloqueado.

Para começar a configurar as restrições de horário durante o dia:

1. Na área **LIMITES DIURNOS**, você tem as seguintes opções:

● **CUMULATIVO**

- a. Selecione as caixas **Limites de tempo em dias de escola** e **Limites de tempo em fins de semana**.
- b. Arraste os marcadores na escala para estabelecer por quanto tempo o acesso aos dispositivos é permitido.

● **ESPECÍFICO**

- a. Selecione as caixas **Limites de tempo em dias de escola** e **Limites de tempo em fins de semana**.
- b. Selecione na grade os intervalos de tempo durante os quais o acesso deve ser bloqueado.



## Nota

As configurações **CUMULATIVO** e **ESPECÍFICO** foram designadas para trabalhar independentemente uma da outra.

## 4.12. Dispositivo Anti-Roubo

O roubo de Laptops é um assunto importante que afeta igualmente indivíduos e empresas. Mais do que perder o hardware em si, é a perda de informação que pode causar danos significativos, tanto financeiramente quanto emocionalmente.

No entanto são poucas as pessoas que tomam as devidas precauções para proteger a sua importante informação pessoal, financeira e de negócio em caso de perda ou roubo.

A função Antifurto do Bitdefender o ajuda a se preparar melhor para tal acontecimento ao permitir que você remotamente localize ou bloqueie seu laptop e até apague todos seus dados, caso tenha de se separar do seu laptop contra sua vontade.



Para usar as funcionalidades de Anti-Roubo, os seguintes pré-requisitos devem ser preenchidos:

- Os comandos só podem ser enviados da conta Bitdefender.
- O laptop deve estar conectado à internet para receber os comandos.

As funcionalidades Anti-roubo funcionam da seguinte forma:

## Localizar

Visualize a localização do seu dispositivo no Google Maps.

A precisão da localização depende de como o Bitdefender é capaz de determiná-la. A localização é determinada em um perímetro de dezenas de metros se o Wi-Fi estiver ativado no seu laptop e se há redes sem fio em alcance.

Se o laptop estiver conectado a uma rede LAN com fio sem uma localização com base no Wi-Fi, a localização será determinada baseada no endereço de IP, que é bastante menos preciso.

## Alerta

Ative um alerta remoto no dispositivo.

Esta função só está disponível em dispositivos móveis.

## Trancar

Bloqueie seu computador e defina um PIN de 4 dígitos para desbloqueá-lo. Quando você envia o comando **Bloquear**, o sistema reinicia e só é possível reaccessar o Windows após inserir o PIN que você estabeleceu.

Caso você queira que o Bitdefender tire fotos da pessoa tentando acessar seu laptop, marque a caixa correspondente. As fotos são tiradas usando a câmera frontal e exibidas com a data e hora no painel da função Antifurto. Apenas as duas fotos mais recentes serão salvas.

Esta ação só está disponível para laptops com câmeras frontais.

## Limpar

Remova todos os dados do seu sistema. Quando você envia o comando **Limpar**, o laptop se reinicia e todos os dados em todas as partições do disco rígido são apagados.

## Mostrar IP


Exibe o último endereço de IP para o dispositivo selecionado. Clique em **MOSTRAR IP** para torná-lo visível.



O Anti-roubo é ativado após a instalação e só pode ser acessado exclusivamente através da sua conta Bitdefender a partir de qualquer dispositivo ligado à Internet, em qualquer lugar.

## Utilizando os Recursos Anti-Roubo

Para acessar as funções Antifurto, utilize uma das opções abaixo:

- Na interface principal do Bitdefender:
  1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
  2. Clique no botão de ação **Antifurto**.
  3. Na janela da Bitdefender Central que abrir, clique no cartão de dispositivo desejado, e então selecione **Antifurto**.
- Em qualquer dispositivo com acesso à Internet:
  1. Abra um navegador da Internet e vá à página: <https://central.bitdefender.com>.
  2. Inicie sessão na sua conta Bitdefender com o seu endereço de e-mail e senha.
  3. Selecione o painel **Meus Dispositivos**.
  4. Clique no cartão de dispositivo desejado, e então selecione **Antifurto**.
  5. Selecione as características que você deseja usar

**Mostrar IP** - exibe o último endereço de IP do seu dispositivo.

**Localizar** - exibe a localização do seu dispositivo no Google Maps.



**Alerta** - emitir um alerta no dispositivo.



**Bloquear** - bloqueia seu computador e define um código PIN para desbloqueá-lo.



**Limpar** - exclui todos os dados do seu laptop.



### Importante

Após apagar um dispositivo, todos os recursos Anti-Roubo deixam de funcionar.



## 4.13. USB Immunizer

A funcionalidade Autorun embutida ao sistema operacional Windows é uma ferramenta bastante útil que permite aos computadores executarem automaticamente um arquivo de um dispositivo de mídia conectado a ele. Por exemplo, as instalações de software podem iniciar automaticamente quando o CD é inserido no drive de CD-ROM.

Infelizmente, esta funcionalidade também pode ser usada pelo malware para iniciar automaticamente e infiltrar no seu computador a partir de dispositivos media graváveis, tais como drives USB flash e cartões de memória conectados através de leitores de cartões. Numerosos ataques Autorun foram criados nestes últimos anos.

Com o Imunizador USB, você poderá evitar que qualquer drive flash formatado em NTFS, FAT32 ou FAT jamais possa executar malware automaticamente. Uma vez que um dispositivo USB esteja imunizado, o malware já não poderá configurá-lo para executar determinado aplicativo quando o dispositivo estiver conectado a um computador com Windows.

Para imunizar um dispositivo USB:

1. Conecte o flash drive ao seu computador.
2. Explore o seu computador para localizar o dispositivo de armazenamento removível e clique com o botão direito do mouse sobre o mesmo.
3. No menu contextual, aponte para o **Bitdefender** e selecione **Imunizar este drive**.



### Nota

Caso o drive já tenha sido imunizado, a mensagem **O dispositivo USB está protegido contra o malware baseado no autorun** aparecerá ao invés da opção Imunizar.

Para evitar que o seu computador execute malware de dispositivos USB não imunizados, desative a função de media autorun. Para mais informações, por favor consulte [“Usando o monitoramento automático de vulnerabilidade”](#) (p. 128).





## 5. OTIMIZAÇÃO DO SISTEMA

### 5.1. Ferramentas

O Bitdefender vem com uma seção de ferramentas que o ajuda a manter a integridade do seu sistema. As ferramentas de manutenção oferecidas são críticas para melhorias no desempenho do seu sistema e para uma gestão eficiente do espaço do seu disco rígido.

O Bitdefender fornece as seguintes ferramentas de Otimização para o PC:


- O **Otimizador em um clique** analisa e aumenta a velocidade do seu sistema ao realizar múltiplas tarefas em um único clique de botão.
- O **Otimizador de Inicialização** reduz o tempo de inicialização do seu sistema ao impedir que aplicações desnecessárias se executem na inicialização do PC.
- **Limpeza de Disco** identifica os arquivos e pastas maiores que não foram usados por muito tempo.

### Otimizando a velocidade do seu sistema com apenas um clique

Questões como falhas de disco rígido, arquivos de registro remanescentes e histórico do navegador, podem comprometer o desempenho do seu computador, e isso pode tornar-se irritante para você. Tudo isso pode ser solucionado em um único clique de botão.

O Otimizador de Um Clique permite que você identifique e remova arquivos inúteis ao executar uma série de tarefas de limpeza ao mesmo tempo.

Para iniciar o processo do Otimizador em um Clique:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão de ação **Otimizador em um Clique**.

#### a. **Analisando**

Espere o Bitdefender terminar de procurar por problemas no sistema.

- **Limpeza de Disco** - identifica arquivos e pastas que você não usa mais.



- Limpeza de Registro - identifica referências inválidas ou obsoletas no Registro do Windows.
- Limpeza de Privacidade - identifica arquivos temporários de Internet, cookies, cache e histórico do navegador.

O número de incidências encontradas é exibido. Clique no link **Ver detalhes** para revisá-los antes de proceder com o processo de limpeza. Clique em **OTIMIZAR** para continuar.

## b. Otimizando

Espera que o Bitdefender conclua a otimização do seu sistema.

## c. Questões

Aqui pode ver o resultado da operação.


Se desejar informações detalhadas sobre o processo de otimização, clique no botão **VER RELATÓRIO DETALHADO**.

## Otimizando o tempo de inicialização do seu PC.

A inicialização prolongada do sistema é um problema real, devido aos aplicativos que estão definidos para rodar sem necessidade. Esperar vários minutos para que um sistema inicialize pode custar-lhe tempo e produtividade.

A janela do Otimizador de Inicialização mostra quais aplicativos estão sendo executados durante a inicialização do sistema e permite que você gerencie o seu comportamento nesta etapa.

Para iniciar o processo do Otimizador de Inicialização:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão de ação **Otimizador de Inicialização**.

### a. Selecione os aplicativos

Você pode ver uma lista de aplicativos sendo executados na inicialização do sistema. Selecione aqueles que você quer desabilitar ou adiar durante a inicialização.

### b. Escolha da comunidade

Veja o que os outros usuários da Bitdefender decidiram fazer com o aplicativo que você selecionou.



## c. Tempo de inicialização do sistema

Verifique a barra no topo da janela para ver o tempo necessário tanto para o sistema como para os aplicativos selecionados serem executados durante a inicialização.

A reinicialização do sistema é necessária para ser capaz de obter informações sobre o tempo de inicialização do sistema e dos aplicativos.

## d. Estado da inicialização

- **Habilitar.** Selecione esta opção quando quiser que um aplicativo seja executado na inicialização do sistema. Essa opção é ativada por padrão.
- **Atraso.** Selecione essa opção para adiar a execução de um programa na inicialização do sistema. Isso significa que os aplicativos selecionados começarão com um atraso de cinco minutos após o usuário acessar o sistema. A funcionalidade do **Atraso** é pré-definida e não pode ser configurada pelo usuário.
- **Desabilitar.** Selecione esta opção para desabilitar a execução de um programa na inicialização do sistema.

## e. Resultados

Informações como o tempo estimado para a inicialização do sistema após adiar ou desabilitar programas são exibidas.

A reinicialização do sistema pode ser necessária para ver todas essas informações.

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



### Nota

Caso a sua assinatura expire ou você decida desinstalar o Bitdefender, os programas que você configurou para não serem executados na inicialização serão restaurados para a sua configuração padrão de inicialização.


## Otimizando seu disco

Arquivos e pastas desnecessários que ocupam espaço no seu disco podem tornar seu sistema lento. Portanto, é recomendável que você melhore a velocidade do sistema ao limpá-lo regularmente.



A Limpeza de Disco do Bitdefender o ajuda a liberar espaço em disco ao identificar arquivos e pastas grandes que você não usa mais.

Para começar a limpar seu sistema:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão de ação **Limpeza de Disco**.
3. Uma janela aparece com informações sobre o que a Limpeza de Disco pode fazer pelo seu sistema para liberar espaço. Clique em **CONTINUAR**.

#### a. Dispositivos e drives

Você pode ver uma lista dos discos disponíveis. Além dos discos do Windows, discos rígidos externos e dispositivos USB são verificados e exibidos na lista. Clique em **VISUALIZAR** para ter acesso às pastas pertencentes ao local selecionado. Clique em **VERIFICAR** na área do disco que você deseja limpar.

#### b. Verificando drive

O drive selecionado é analisado. Aguarde até o Bitdefender finalizar a busca por arquivos e pastas grandes.

#### c. Questões

Aqui você pode ver os resultados da operação divididos em pastas. No lado esquerdo da janela, um gráfico de pizza mostrando a quantidade de espaço em disco usado pode ser visto. Mova o mouse por cima dele para ver o nome dos seus arquivos e quanto de espaço eles ocupam.

Para navegar pelas pastas do local do sistema selecionado, selecione-os na parte direita da janela. Para visualizar o conteúdo de uma pasta em uma janela separada, selecione **Mostrar no Explorador de Arquivos**.

Arraste os arquivos que deseja excluir para a parte inferior da janela. Clique em **VISUALIZAR** caso deseje conferir novamente os arquivos que selecionou para excluir. Clique em **EXCLUIR PERMANENTEMENTE** para iniciar o processo de exclusão.

Confirme sua escolha.



## 5.2. Perfis

Atividades de trabalho diárias, assistir filmes ou jogar games podem causar lentidão no sistema, especialmente se eles estiverem sendo executados simultaneamente com os processos de atualização do Windows e tarefas de manutenção. Com o Bitdefender, você pode escolher e aplicar o seu perfil preferido; isso irá fazer ajustes no sistema para melhorar o desempenho de aplicativos específicos.

O Bitdefender fornece os seguintes perfis:

- Perfil de Trabalho
- Perfil de Filme
- Perfil de Jogo
- Perfil Wi-Fi Público
- Perfil Modo de Bateria

Caso você decida não usar os **Perfis**, um perfil padrão chamado **Padrão** será ativado e ele não fará qualquer otimização no seu sistema.

De acordo com sua atividade, as seguintes configurações do produto são aplicadas quando os perfis Trabalho, Filme ou Jogo são ativados:

- Todos os alertas e pop-ups do Bitdefender estão desativados.
- A Atualização Automática é adiada.
- As análises programadas são adiadas.
- O módulo Antispam é ativado.
- O **Consultor de Buscas** é desabilitado.
- As ofertas especiais e as notificações de produto estão desativadas.

De acordo com sua atividade, as seguintes configurações do sistema são aplicadas quando os perfis Trabalho, Filme ou Jogo são ativados:

- A Atualização Automática do Windows é adiada.
- Alertas e pop-ups do Windows são desabilitados.
- Programas em segundo plano desnecessários são suspensos.
- Os efeitos visuais são ajustados para o melhor desempenho.
- Tarefas de manutenção são adiadas.



- A configuração do plano de energia é ajustada.

Quando executado no perfil Wi-Fi Público, o Bitdefender Total Security é configurado para ajustar automaticamente as seguintes configurações:


- O Controle Ativo de Ameaças é ligado
- O Firewall do Bitdefender está ligado e as seguintes configurações são aplicadas ao seu adaptador sem fio:
  - Modo Sigiloso - Ligado
  - Genérico - Desligado
  - Tipo de rede - Pública
- As seguintes configurações da Proteção na Web são ativadas:
  - Analisar SSL
  - Proteção contra fraudes
  - Proteção contra phishing

## Perfil de Trabalho

A execução de várias tarefas no trabalho, tais como o envio de e-mails, ter uma videoconferência com seus colegas distantes ou trabalhar com aplicativos de design pode afetar o desempenho do sistema. O Perfil de Trabalho foi projetado para ajudá-lo a melhorar a sua eficiência no trabalho, desativando alguns dos serviços e tarefas de manutenção em segundo plano.

## Configurando o Perfil de Trabalho

Para configurar as ações a serem tomadas enquanto você está no Perfil de Trabalho:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Selecione a aba **PERFIS**.
3. Certifique-se de que a opção **Perfis** está ativada.
4. Clique no botão **CONFIGURAR** na área do Perfil de Trabalho.
5. Defina os ajustes de sistema que você quer que sejam aplicados selecionando as seguintes opções:




- Aumente o desempenho dos aplicativos de trabalho
  - Otimize as configurações do produto para perfil de Trabalho
  - Adie programas em segundo plano e tarefas de manutenção
  - Adiar as Atualizações Automáticas do Windows
6. Clique **Salvar** para salvar as alterações e fechar a janela.

## Adicionar aplicativos manualmente à lista do Perfil de Trabalho

Se o Bitdefender não entrar automaticamente no Perfil de Trabalho quando você abrir um determinado aplicativo de trabalho, você pode adicionar o aplicativo manualmente à **Lista de Aplicativos**.

Para adicionar aplicativos manualmente à Lista de aplicativos do Perfil de Trabalho:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Selecione a aba **PERFIS**.
3. Certifique-se de que a opção **Perfis** está ativada.
4. Clique no botão **CONFIGURAR** na área do Perfil de Trabalho.
5. Na janela **PERFIL DE TRABALHO**, clique no link **Lista de aplicações**.
6. Clique em **Adicionar** para adicionar um novo aplicativo à **Lista de aplicativos**.

Uma nova janela aparece. Vá até o arquivo executável do aplicativo, selecione-o e clique em **OK** para adicioná-lo à lista.


## Perfil de Filme

A exibição de conteúdo de vídeo de alta qualidade, como filmes de alta definição, exige recursos significativos do sistema. O Perfil de Filme ajusta as configurações de sistema e do produto para que você possa desfrutar de uma experiência cinematográfica agradável e sem interrupção.

## Configurando o Perfil de Filme

Para definir as ações a serem tomadas no Perfil de Filme:




1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Selecione a aba **PERFIS**.
3. Certifique-se de que a opção **Perfis** está ativada.
4. Clique no botão **CONFIGURAR** na área do Perfil de Filme.
5. Defina os ajustes de sistema que você quer que sejam aplicados selecionando as seguintes opções:
  - Aumente o desempenho dos reprodutores de vídeo
  - Otimize as configurações do produto para Perfil de filme
  - Adie programas em segundo plano e tarefas de manutenção
  - Adiar as Atualizações Automáticas do Windows
  - Ajustar configs do plano de energia para Modo Filme.
6. Clique **Salvar** para salvar as alterações e fechar a janela.

## Adicionando manualmente reprodutores de vídeo à lista do Perfil de Filme

Se o Bitdefender não entrar automaticamente no Perfil de Filme ao iniciar um determinado aplicativo de reprodução de vídeo, você pode adicionar manualmente o aplicativo à **Lista de reprodutores**.

Para adicionar manualmente reprodutores de vídeo à Lista de reprodutores no Perfil de Filme:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Selecione a aba **PERFIS**.
3. Certifique-se de que a opção **Perfis** está ativada.
4. Clique no botão **CONFIGURAR** na área do Perfil de Filme.
5. Na janela **PERFIL DE FILME**, clique no link **Lista de programas**.
6. Clique em **Adicionar** para adicionar um novo aplicativo à **Lista de reprodutores**.

Uma nova janela aparece. Vá até o arquivo executável do aplicativo, selecione-o e clique em **OK** para adicioná-lo à lista.






## Perfil de Jogo

Para desfrutar de uma experiência de jogo ininterrupta é importante reduzir carga do sistema e diminuir a lentidão. Usando heurísticas comportamentais, juntamente com uma lista de jogos conhecidos, o Bitdefender pode detectar automaticamente os jogos em execução e otimizar os recursos do sistema para que você possa aproveitar a sua pausa para jogo.

## Configurando o Perfil de Jogo


Para configurar as ações a serem tomadas enquanto você está no Perfil de Jogos:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Selecione a aba **PERFIS**.
3. Certifique-se de que a opção **Perfis** está ativada.
4. Clique no botão **CONFIGURAR** na área do Perfil de Jogos.
5. Defina os ajustes de sistema que você quer que sejam aplicados selecionando as seguintes opções:
  - Aumente o desempenho nos jogos
  - Otimize as configurações do produto para Perfil de jogo
  - Adie programas em segundo plano e tarefas de manutenção
  - Adiar as Atualizações Automáticas do Windows
  - Ajustar configs do plano de energia para Modo Jogo.
6. Clique **Salvar** para salvar as alterações e fechar a janela.

## Adicionando jogos manualmente à lista de Jogos

Se o Bitdefender não entrar automaticamente no Perfil de Jogo ao iniciar um determinado jogo ou aplicativo, você pode adicionar o aplicativo à **Lista de jogos** manualmente.

Para adicionar manualmente jogos à Lista de jogos no Perfil de Jogo:

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



3. Certifique-se de que a opção **Perfis** está ativada.
4. Clique no botão **CONFIGURAR** na área do Perfil de Jogos.
5. Na janela **PERFIL DE JOGOS**, clique no link **Lista de jogos**.
6. Clique em **Adicionar** para adicionar um novo jogo à **Lista de jogos**.


Uma nova janela aparece. Vá até o arquivo executável do jogo, selecione-o e clique em **OK** para adicioná-lo à lista.

## Perfil Wi-Fi Público

Enviar e-mails, digitar credenciais sensíveis ou fazer compras online enquanto conectado a uma rede sem fio não segura pode por seus dados pessoais em risco. O perfil Wi-Fi Público ajusta as configurações do produto para lhe dar a possibilidade de fazer pagamentos online e usar informações sensíveis em um ambiente protegido.

## Configurando o perfil Wi-Fi Público

Para configurar o Bitdefender para aplicar as configurações enquanto conectado a uma rede sem fio não segura:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Selecione a aba **PERFIS**.
3. Certifique-se de que a opção **Perfis** está ativada.
4. Clique no botão **CONFIGURAR** na área do perfil Wi-Fi Público.
5. Deixe marcada a caixa **Ajusta as configurações do produto para reforçar a proteção quando conectado a uma rede Wi-Fi pública não segura**.
6. Clique em **Guardar**.


## Perfil Modo de Bateria

O perfil Modo de Bateria é especialmente concebido para usuários de laptop e tablet. Sua finalidade é minimizar o impacto do sistema e do Bitdefender sobre o consumo de energia quando o nível de carga da bateria estiver mais baixo que o padrão ou o que você selecionou.

## Configurando o perfil Modo de Bateria

Para configurar o perfil Modo de Bateria:



1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Selecione a aba **PERFIS**.
3. Certifique-se de que a opção **Perfis** está ativada.
4. Clique no botão **CONFIGURAR** na área do perfil Modo de Bateria.
5. Escolha os ajustes de sistema que serão aplicados selecionando as seguintes opções:
  - Otimize as configurações do produto para o Modo de bateria.
  - Adie programas em segundo plano e tarefas de manutenção.
  - Adie as Atualizações Automáticas do Windows.
  - Ajuste as configurações do plano de energia para o Modo de bateria.
  - Desative os dispositivos externos e portas de rede.
6. Clique **Salvar** para salvar as alterações e fechar a janela.

Digite um valor válido na caixa de rotação, ou selecione um valor usando os botões para especificar quando o sistema deve começar a operar no Modo de Bateria. Por padrão, o modo é ativado quando o nível da bateria cai abaixo de 30%.

As seguintes configurações do produto são aplicadas quando o Bitdefender opera no perfil Modo de Bateria:

- A Atualização Automática do Bitdefender é adiada.
- As análises programadas são adiadas.
- O **Dispositivo de Segurança** é desligado.

O Bitdefender detecta quando o seu laptop está ligado na bateria e dependendo do nível de carga da bateria, ele automaticamente entra em Modo de Bateria. Da mesma forma, o Bitdefender sai automaticamente do Modo de Bateria ao detectar que o laptop está conectado com um cabo de energia.


## Otimização em Tempo Real

A Otimização em Tempo Real do Bitdefender é um plug-in que melhora o desempenho do seu sistema de forma silenciosa, em segundo plano, garantindo que você não seja interrompido enquanto está em um modo de perfil. Dependendo da carga do CPU, o plug-in monitora todos os processos,



focando naqueles que usam uma carga maior, para ajustá-los às suas necessidades.

Para ativar ou desativar a Otimização em Tempo Real:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Selecione a aba **PERFIS**.
3. Use o botão correspondente para ligar ou desligar a Otimização em Tempo Real.



## 6. RESOLUÇÃO DE PROBLEMAS

### 6.1. Resolvendo incidências comuns

Este capítulo apresenta alguns dos problemas que poderá encontrar ao utilizar o Bitdefender e as possíveis soluções. A maioria destes problemas pode ser resolvida com a configuração correcta das definições do produto.

- “O meu sistema parece estar lento” (p. 183)
- “A análise não inicia” (p. 185)
- “Já não consigo utilizar um aplicativo” (p. 188)
- “O que fazer quando o Bitdefender bloqueia um website ou um aplicativo online seguro” (p. 189)
- “O que fazer se o Bitdefender detectar uma aplicação segura como ransomware” (p. 190)
- “Como atualizar o Bitdefender numa ligação à Internet lenta” (p. 194)
- “Os Serviços do Bitdefender não estão respondendo” (p. 195)
- “O filtro antispam não funciona corretamente” (p. 196)
- “A funcionalidade Preenchimento Automático não funciona na minha Carteira” (p. 201)
- “A Remoção do Bitdefender falhou” (p. 202)
- “O meu sistema não reinicia após a instalação de Bitdefender” (p. 203)

Se não conseguir encontrar o seu problema aqui, ou se as soluções apresentadas não resolvem o seu problema, pode contactar os representantes do apoio técnico da Bitdefender como mostrado no capítulo “*Solicite Ajuda*” (p. 287).

### O meu sistema parece estar lento

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

Caso note uma diminuição de velocidade significativa, este problema pode ocorrer pelos seguintes motivos:

- **O Bitdefender não é o único programa de segurança instalada no sistema.**



Apesar de o Bitdefender procurar e remover os programas de segurança encontrados durante a instalação, é recomendado que remova todos os outros programas antivírus utilizados antes de instalar o Bitdefender. Para mais informações, por favor consulte **“Como posso remover outras soluções de segurança?”** (p. 81).

- **Não estão cumpridos os Requisitos Mínimos do Sistema para executar o Bitdefender.**

Se o seu computador não cumprir os Requisitos Mínimos do Sistema, ficará lento, especialmente se estiver executando múltiplos aplicativos ao mesmo tempo. Para mais informações, por favor consulte **“Requisitos mínimos do sistema”** (p. 3).

- **Você instalou aplicativos que não utiliza.**

Qualquer computador possui programas ou aplicativos que você não utiliza. E quaisquer programas indesejados são executados no plano de fundo, ocupando espaço no disco rígido e memória. Caso não utilize um programa, desinstale-o. Isso também se aplica a qualquer outro programa pré-instalado ou aplicativo de teste que tenha esquecido de remover.




### **Importante**

Caso suspeite que um programa ou aplicativo seja parte essencial de seu sistema operacional, não remova o mesmo e entre em contato com a Assistência ao Cliente Bitdefender para assistência.

- **Seu sistema pode estar infectado.**

A velocidade do seu sistema e o seu comportamento geral também podem ser afetados pelo malware. Spyware, víruses, Trojans e adware prejudicam o desempenho de seu sistema. Certifique-se de analisar o seu sistema periodicamente, pelo menos uma vez por semana. Recomendamos utilizar a Verificação de Sistema do Bitdefender pois a mesma verifica todos os tipos de malware que estejam ameaçando a segurança do seu sistema.

Para iniciar a Verificação do Sistema:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **ANTIVÍRUS**, selecione **Verificação do Sistema**.
4. Siga os passos do assistente.



## A análise não inicia

Este tipo de problema pode ter duas causas principais:

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

Neste caso:

1. Remover o Bitdefender totalmente do sistema:

- **No Windows 7:**

- a. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Programas e Recursos**.
- b. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
- c. Clique em **REMOVER** na janela que aparecer, depois escolha quais dados devem ser salvos para uma instalação posterior:
  - Arquivos em quarentena
  - Carteiras
  - Arquivos Cofre
- d. Clique em **CONTINUAR**.
- e. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

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

- a. No tela inicial do Windows, localize **Painel de Controle** (por exemplo, você pode começar digitando "Painel de Controle" diretamente na tela inicial) e depois clique no ícone.
- b. Clique em **Desinstalar um programa** ou **Programas e Recursos**.
- c. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
- d. Clique em **REMOVER** na janela que aparecer, depois escolha quais dados devem ser salvos para uma instalação posterior:
  - Arquivos em quarentena
  - Carteiras
  - Arquivos Cofre
- e. Clique em **CONTINUAR**.



f. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

● **No Windows 10:**

a. Clique em **Iniciar** e depois em Configurações.

b. Clique no ícone **Sistema** na área de Configurações e então selecione **Aplicativos instalados**.

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

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

e. Clique em **REMOVER** na janela que aparecer, depois escolha quais dados devem ser salvos para uma instalação posterior:

● Arquivos em quarentena

● Carteiras

● Arquivos Cofre

f. Clique em **CONTINUAR**.

g. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

2. Reinstale seu produto Bitdefender

● **O Bitdefender não é a única solução de segurança instalada no seu sistema.**

Neste caso:

1. Remover a outra solução de segurança. Para mais informações, por favor consulte [“Como posso remover outras soluções de segurança?”](#) (p. 81).

2. Remover o Bitdefender totalmente do sistema:

● **No Windows 7:**

a. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Programas e Recursos**.

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

c. Clique em **REMOVER** na janela que aparecer, depois escolha quais dados devem ser salvos para uma instalação posterior:

● Arquivos em quarentena





- Carteiras
- Arquivos Cofre
- d. Clique em **CONTINUAR**.
- e. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.
- **No Windows 8 e Windows 8.1:**
  - a. No tela inicial do Windows, localize **Painel de Controle** (por exemplo, você pode começar digitando "Painel de Controle" diretamente na tela inicial) e depois clique no ícone.
  - b. Clique em **Desinstalar um programa** ou **Programas e Recursos**.
  - c. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
  - d. Clique em **REMOVER** na janela que aparecer, depois escolha quais dados devem ser salvos para uma instalação posterior:
    - Arquivos em quarentena
    - Carteiras
    - Arquivos Cofre
  - e. Clique em **CONTINUAR**.
  - f. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.
- **No Windows 10:**
  - a. Clique em **Iniciar** e depois em Configurações.
  - b. Clique no ícone **Sistema** na área de Configurações e então selecione **Aplicativos instalados**.
  - c. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
  - d. Clique em **Desinstalar** novamente para confirmar sua escolha.
  - e. Clique em **REMOVER** na janela que aparecer, depois escolha quais dados devem ser salvos para uma instalação posterior:
    - Arquivos em quarentena
    - Carteiras
    - Arquivos Cofre



f. Clique em **CONTINUAR**.

g. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

3. Reinstale seu produto Bitdefender

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção *"Solicite Ajuda"* (p. 287).

## Já não consigo utilizar um aplicativo

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

Após instalar o Bitdefender você poderá se deparar com uma das seguintes situações:



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

Este tipo de situação ocorre quando o Controle Ativo de Ameaças detecta erroneamente que alguns aplicativos são maliciosos.

O Controle Ativo de Ameaças é um módulo do Bitdefender que monitora constantemente os aplicativos executados em seu sistema e reporta aqueles com comportamento potencialmente malicioso. Já que esta função é baseada em um sistema heurístico, pode haver casos em que aplicativos legítimos sejam reportados pelo Controle Ativo de Ameaças.

Quando essa situação ocorrer, você poderá excluir o aplicativo respectivo da monitoração do Controle de Ameaças Ativas.

Para adicionar o programa à lista de exclusões:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **ANTIVÍRUS**.
4. Selecione a aba **EXCLUSÕES**.



5. Clique no menu **Lista de processos excluídos da verificação** . Na janela que aparece, você pode gerenciar as exclusões de processos do Controle Ativo de Ameaças.
6. Adicionar exceções seguindo estes passos:
  - a. Clique no botão **ADD**.
  - b. Clique em **Explorar**, procure e selecione o aplicativo que quer excluir e depois clique em **OK**.
  - c. Mantenha a opção **Permitir** selecionada para prevenir que o Controle Ativo de Ameaças bloqueie o aplicativo.
  - d. Clicando **Adicionar**.



Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção *"Solicite Ajuda"* (p. 287).

## O que fazer quando o Bitdefender bloqueia um website ou um aplicativo online seguro

O Bitdefender oferece uma experiência de navegação de rede segura filtrando todo o tráfego da rede e bloqueando conteúdos maliciosos. No entanto, é possível que o Bitdefender considere um website ou um aplicativo online seguro como inseguro, o que fará que a análise de tráfego de HTTP do Bitdefender bloqueie-os incorretamente.

Se a mesma página ou aplicativo for bloqueado repetidamente, eles podem ser adicionados a uma lista segura para que não sejam analisados pelos mecanismos do Bitdefender, assegurando uma experiência de navegação da rede normal.

Para adicionar uma página web à **Lista branca**:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **PROTEÇÃO NA WEB**.
4. Clique no link **Lista branca**.
5. Forneça o endereço do website ou do aplicativo online bloqueado no campo correspondente e clique em **Adicionar**.



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

Apenas os websites e aplicativos que você confia completamente devem ser adicionados a essa lista. Esses serão excluídos da análise pelos seguintes mecanismos: malware, phishing e fraude.


Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção *"Solicite Ajuda"* (p. 287).

## O que fazer se o Bitdefender detectar uma aplicação segura como ransomware

Ransomware é um programa malicioso que tenta lucrar com usuários através do travamento de seus sistemas vulneráveis. Para mantê-lo protegido de situações desagradáveis, o Bitdefender lhe dá a possibilidade de resgatar arquivos pessoais.

Quando uma aplicação tenta modificar ou apagar um dos seus arquivos protegidos, ela será considerada insegura e o Bitdefender bloqueará sua funcionalidade.

Caso uma aplicação seja adicionada à lista de aplicações não confiáveis e você tiver certeza de que é seguro usá-la, siga esses passos:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **PROTEÇÃO CONTRA RANSOMWARE**, selecione **Aplicações bloqueadas**.
4. Clique em **Permitir** e procure a aplicação que você tem certeza de que é segura.
5. Clique em **OK** para adicionar a aplicação selecionada à lista confiável.


## Não consigo conectar-me à Internet

Poderá verificar que um programa ou navegador da rede já não consegue conectar-se à Internet ou acessar os serviços em rede após a instalação do Bitdefender.

Neste caso, a melhor solução é configurar o Bitdefender para permitir automaticamente conexões de e para o respectivo aplicativo de software.

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



2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **FIREWALL**.
4. Selecione a aba **REGRAS**.
5. Para adicionar uma regra de aplicação, clique no botão **ADICIONAR REGRA**.
6. Uma nova janela aparecerá para que você possa inserir as informações. Certifique-se de selecionar todos os tipos de rede disponíveis e na seção **Permissão** selecionar **Permitir**.

Feche o Bitdefender, abra o aplicativo de software e tente conectar-se à Internet novamente.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção *"Solicite Ajuda"* (p. 287).



## Não consigo acessar um dispositivo na minha rede

Dependendo da rede a que está conectado, a firewall do Bitdefender poderá bloquear a conexão entre o seu sistema e outro dispositivo (como outro computador ou uma impressora). Como resultado, já não poderá partilhar ou imprimir arquivos.

Neste caso, a melhor solução é configurar o Bitdefender para permitir automaticamente conexões de e para o respectivo dispositivo. Para cada conexão de rede você pode configurar uma zona confiável e especial.

Uma zona confiável é um dispositivo em que você confia plenamente. Todo o tráfego entre o seu computador e o dispositivo confiável é permitido. Para partilhar recursos com dispositivos específicos, tais como computadores ou impressoras, adicione-as como zonas confiáveis.

Para adicionar uma zona de confiança nos seus adaptadores de rede:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **FIREWALL**.
4. Selecione a aba **ADAPTADORES**.
5. Para adicionar uma zona, clique no link **Exceções de Rede**.
6. Digite o endereço de IP do computador ou da impressora que deseja adicionar no campo correspondente.



7. Na coluna **Adaptador**, selecione **Confiáveis**.
8. Na coluna **Permissão**, selecione **Permitir**.
9. Clique no botão + para adicionar a exceção, fechar a janela.

Se você ainda não consegue se conectar ao dispositivo, a incidência poderá não ser causada pelo Bitdefender.

Verifique a existência de outras causas potenciais, tais como as seguintes:

- A firewall no outro computador poderá bloquear a partilha de arquivos e impressoras com o seu computador.
- Se o Firewall do Windows for usado, pode ser configurado para compartilhar arquivos e impressoras da seguinte forma:
  - No **Windows 7**:
    1. Clique em **Iniciar**, vá ao **Painel de Controle** e selecione **Sistema e Segurança**.
    2. Vá ao **Firewall do Windows**, depois clique em **Permitir um programa por meio do Firewall do Windows**.
    3. Selecione a caixa de marcação **Compartilhar Arquivos e Impressoras**.
  - No **Windows 8 e Windows 8.1**:
    1. No tela inicial do Windows, localize **Painel de Controle** (por exemplo, você pode começar digitando "Painel de Controle" diretamente na tela inicial) e depois clique no ícone.
    2. Clique em **Sistema e Segurança**, acesse **Windows Firewall** e selecione **Permitir um aplicativo através do Windows Firewall**.
    3. Marque a caixa **Compartilhamento de arquivos e impressora** e depois clique em **OK**.
  - No **Windows 10**:
    1. Digite "Permitir um aplicativo através do Firewall do Windows" na caixa de pesquisa da barra de tarefas e clique no ícone correspondente.
    2. Clique em **Alterar configurações**.
    3. Na lista **Aplicativos e recursos permitidos**, marque a caixa **Compartilhamento de arquivos e impressora**, depois clique em **OK**.



- Se outro programa de firewall é usado, por favor consulte a sua documentação ou o arquivo de ajuda.
- Condições gerais que podem impedir ou uso ou a conexão com a impressora compartilhada:
  - Você pode precisar fazer logon em uma conta administrador do Windows para acessar a impressora compartilhada.
  - As permissões são definidas para a impressora compartilhada para permitir acesso apenas para usuários e computadores específicos. Se você está compartilhando a sua impressora, verifique as permissões definidas para a impressora para ver se o usuário do outro computador é permitido o acesso à impressora. Se você está tentando se conectar a uma impressora compartilhada, verifique com o usuário no outro computador, se você tem permissão para se conectar à impressora.
  - A impressora conectada ao seu computador ou a outro computador não está compartilhada.
  - A impressora compartilhada não é adicionada no computador.



## Nota

Para aprender como gerenciar o compartilhamento de impressora (compartilhar uma impressora, definir ou remover permissões para uma impressora, conectar-se a uma impressora da rede, ou a uma impressora compartilhada), vá para a Ajuda do Windows e Centro de Suporte (no menu Iniciar, clique **Ajuda e Suporte**).

- O acesso a uma impressora em rede pode ser restrito a computadores ou usuários específicos. Você deve verificar com o administrador da rede se possui ou não permissão para acessar a impressora.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção *"Solicite Ajuda"* (p. 287).




## A minha Internet está lenta

Esta situação poderá surgir depois de instalar o Bitdefender. Este problema poderá ser causado por erros na configuração da firewall do Bitdefender.

Para solucionar essa situação:

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



2. Clique no botão **VER MÓDULOS**.
3. Selecione o ícone  no canto superior direito do módulo **FIREWALL**.
4. Clique no botão correspondente para ativar ou desativar o **Firewall**.
5. Verifique se a sua ligação à Internet melhorou com a firewall do Bitdefender desativada.
  - Caso você ainda com uma conexão lenta à Internet, a incidência poderá não ser causada pelo Bitdefender. Você deve contatar o seu Provedor de Serviços de Internet para confirmar se a conexão está operacional. Se receber a confirmação do seu Fornecedor de Serviços de Internet que a ligação está operacional e o problema persistir, contacte a Bitdefender como indicado na secção "*Solicite Ajuda*" (p. 287).
  - Se a conexão com a internet melhorou após desativar o firewall do Bitdefender:
    - a. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
    - b. Clique no botão **VER MÓDULOS**.
    - c. Selecione o ícone  no canto superior direito do módulo **FIREWALL**.
    - d. Na aba **CONFIGURAÇÕES** clique no botão para desativar **Bloquear verificações de porta na rede**.
    - e. Acesse a aba **ADAPTADORES** e selecione sua conexão de Internet.
    - f. Na coluna **Tipo de Rede** selecione **Casa/Trabalho**.
    - g. Na coluna **Modo Sigiloso**, selecione **Ativar**. Configure a coluna **Genérico** como **Ativado**.
    - h. Feche o Bitdefender, reinicie o sistema e verifique a velocidade de conexão à Internet.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção "*Solicite Ajuda*" (p. 287).


## Como atualizar o Bitdefender numa ligação à Internet lenta

Se tiver uma ligação à Internet lenta (por exemplo, ligação telefónica), poderão ocorrer erros durante o processo de atualização.





Para manter seu sistema atualizado com as assinaturas de malware mais recentes do Bitdefender:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Selecione a aba **ATUALIZAR**.
3. Próximo a **Atualizar as regras de processamento**, selecione **Exibir antes de fazer download** do menu suspenso.
4. Volte à janela principal e clique no botão de ação **Atualizar** na interface do Bitdefender.
5. Selecione apenas **Atualização de assinaturas** e depois clique em **OK**.
6. O Bitdefender vai transferir e instalar apenas as atualizações das assinaturas de malware.

## Os Serviços do Bitdefender não estão respondendo

Este artigo ajuda você a solucionar o erro **Os Serviços do Bitdefender não estão respondendo**. Você pode encontrar esse erro da seguinte forma:

- O ícone do Bitdefender na **bandeja do sistema** está cinza e você recebe a informação de que os serviços do Bitdefender não estão respondendo.
- A janela do Bitdefender mostra que os serviços do Bitdefender não estão respondendo.

O erro pode ser causado por uma das seguintes condições:

- Erro temporário de comunicação entre os serviços do Bitdefender.
- Alguns dos serviços do Bitdefender estão parados.
- outras soluções de segurança sendo executadas em seu computador ao mesmo tempo com o Bitdefender.

Para solucionar este erro, tente estas soluções:

1. Espere um pouco e veja se alguma coisa muda. O erro pode ser temporário.
2. Reinicie o computador e aguarde alguns momentos até que o Bitdefender seja carregado. Abra o Bitdefender para verificar se o erro persiste. Reiniciar o computador normalmente resolve o problema.
3. Verifique se há alguma outra solução de segurança instalada, pois ela poderão afetar o funcionamento do Bitdefender. Se este for o caso,



recomendamos que você remova todas as outras soluções de segurança e então reinstale o Bitdefender.

Para mais informações, por favor consulte **“Como posso remover outras soluções de segurança?”** (p. 81).

Se o erro persistir, entre em contato com nossos representantes de suporte conforme descrito na seção **“Solicite Ajuda”** (p. 287).

## O filtro antispam não funciona corretamente

Este artigo ajuda você solucionar os seguintes problemas relacionados com as operações de filtragem do Bitdefender Antispam:

- Um número de mensagens de e-mail legítimas estão marcadas como [spam].
- Muitas mensagens spam não estão marcadas de acordo com o filtro antispam.
- O filtro antispam não detecta qualquer mensagem de Spam.

## Mensagens legítimas são marcadas como [spam]

Valida mensagens que estão marcadas como [spam] simplesmente porque elas parecem como spam para o filtro antispam Bitdefender. Normalmente, você pode resolver este problema ao configurar adequadamente o filtro antispam.

Bitdefender adiciona automaticamente os destinatários de suas mensagens de e-mail à sua lista de Amigos. As mensagens de e-mail recebidas de contatos na lista de Amigos, são consideradas legítimas. Elas não são verificadas pelo filtro antispam, e portanto, nunca são marcadas como [spam].

A configuração automática da lista de Amigos, não previne a detecção de erros que possam ocorrer nestas situações:

- Você recebe uma grande quantidade de e-mails com fins comerciais, como resultado de ter se registrado em vários sites. Neste caso, a solução é adicionar o endereço de e-mail de onde você recebe tais mensagens à lista de Amigos.
- Uma parte significativa de seus e-mails legítimos vem de pessoas das quais você nunca trocou e-mail antes, tal como clientes, potenciais sócios de negócios e outros. Outra solução é necessária neste caso.



Se estiver usando um cliente de e-mail com o qual o Bitdefender é compatível, **indique erros de detecção**.




## Nota

O Bitdefender integra-se aos e-mails mais comumente usados pelos clientes através de uma barra de ferramentas muito fácil de usar. Para uma lista completa de clientes de e-mail suportados, por favor vá para **“Clientes de e-mail e protocolos suportados”** (p. 111).


## Adicionar contatos à Lista de Amigos

Se você está usando um cliente de e-mail suportado, você pode facilmente adicionar os remetentes de mensagens legítimas à lista de Amigos. Siga esses passos:

1. Em seu cliente de e-mail, selecione uma mensagem de e-mail do remetente que você deseja adicionar à lista de Amigos.
2. Clique o botão  **Adicionar Amigo** à barra de ferramentas do antispam do Bitdefender.
3. Poderá lhe ser solicitado a acusar o recebimento do endereço adicionado à lista de Amigos. Selecione **Não mostre esta mensagem novamente** e clique **OK**.

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

Se você está usando um cliente de e-mail diferente, você pode adicionar contatos à lista de Amigos da interface do Bitdefender. Siga esses passos:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **ANTISPAM**, selecione **Gerenciar Amigos**.

Uma janela de confirmação aparecerá.

4. Digite o endereço de e-mail onde deseja sempre receber as mensagens de e-mail e depois clique em **Adicionar**. Pode adicionar quantos endereços de email desejar.
5. Clique em **OK** para guardar as alterações e fechar a janela.



## Indica os erros de detecção

Se você está usando um cliente de e-mail suportado, você pode facilmente corrigir o filtro antispam (indicando qual mensagem de e-mail não deve ser marcada como [spam]). Fazendo isto, a eficiência do filtro antispam melhorará consideravelmente. Siga esses passos:

1. Abra seu cliente de e-mail.
2. Vá para a pasta de lixo, aonde os spams são levados.
3. Selecione a mensagem legítima incorretamente marcada como [spam] pelo Bitdefender.
4. Clique o botão  **Adicionar Amigos** na barra de ferramentas do antispam do Bitdefender para adicionar o remetente à lista de Amigos. Você poderá ter que clicar **OK** para acusar recebimento. Você sempre receberá e-mails desse endereço, não importa o que a mensagem contenha.
5. Clique no botão  **Não Spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de e-mail do cliente). A mensagem de e-mail será removida para a pasta de Entrada.

## Muitas mensagens de spam não são detetadas

Se você está recebendo muitas mensagens que não estão marcadas como [spam], você precisa configurar o filtro antispam do Bitdefender para poder melhorar sua eficiência.

Tente as seguintes soluções:

1. Se estiver usando um cliente de e-mail com o qual o Bitdefender é compatível, **indique mensagens de spam não detectadas**.



### Nota


O Bitdefender integra-se aos e-mails mais comumente usados pelos clientes através de uma barra de ferramentas muito fácil de usar. Para uma lista completa de clientes de e-mail suportados, por favor vá para **“Clientes de e-mail e protocolos suportados”** (p. 111).

2. **Adicionar spammers à lista de Spammers**. As mensagens de e-mail recebidas destes endereços na lista de Spammers, são automaticamente marcados como [spam].




## Indica mensagens de spam não detectadas

Se você está usando um cliente de e-mail suportado, você pode facilmente indicar quais mensagens de e-mail foram detectadas como spam. Fazendo isto, a eficiência do filtro antispam melhorará consideravelmente. Siga esses passos:


1. Abra seu cliente de e-mail.
2. Vá para a Pasta de Entrada.
3. Selecione as mensagens spam não detectadas.
4. Clique no botão  **É Spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de e-mail do cliente). Elas são marcadas imediatamente como [spam] e movidas para a pasta lixo.

## Adicionar spammers à Lista de Spammers.

Se você está usando um cliente de e-mail suportado, você pode facilmente adicionar os remetentes das mensagens de spam, à lista de Spammers. Siga esses passos:

1. Abra seu cliente de e-mail.
2. Vá para a pasta de lixo, aonde os spams são levados.
3. Selecione as mensagens marcadas como [spam] pelo Bitdefender.
4. Clique o botão  **Adicionar Spammer** na barra de ferramentas do antispam do Bitdefender.
5. Lhe poderá ser solicitado acusar recebimento do endereço adicionado à lista de Spammers. Selecione **Não mostre esta mensagem novamente** e clique **OK**.

Caso esteja usando um cliente de e-mail diferente, você pode adicionar spammers manualmente à lista de Spammers da interface do Bitdefender. É conveniente fazer isto somente quando você recebe várias mensagens spam do mesmo endereço de e-mail. Siga esses passos:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **ANTISPAM**, selecione **Gerenciar Spammers**.




Uma janela de confirmação aparecerá.

4. Digite o endereço de e-mail do spammer e depois clique em **Adicionar**. Pode adicionar quantos endereços de email desejar.
5. Clique em **OK** para guardar as alterações e fechar a janela.

## O filtro antispam não detecta nenhuma mensagem spam

Se nenhuma mensagem de spam for marcada como [spam], poderá haver um problema com o filtro antispam do Bitdefender. Antes de resolver este problema, certifique-se de que não é causado por uma das seguintes condições:

- A proteção antispam poderá estar desligada. Para verificar o status de proteção antispam, clique no ícone  na barra lateral esquerda da interface do Bitdefender e depois selecione o link **VER MÓDULOS**. Clique na engrenagem do painel **ANTISPAM**, depois veja o lado superior da janela para conferir se o módulo está ativado.

Se o Antispam estiver desligado, é isso que está causando o problema. Clique no botão correspondente para ativar sua proteção antispam.

- A proteção Antispam do Bitdefender está disponível apenas para clientes de correio eletrônico configurado para receber mensagens de e-mail via protocolo POP3. Isso significa o seguinte:
  - E-mails recebidos através de serviços e-mail baseados em web (tais como Yahoo, Gmail, Hotmail ou outro) não são filtrados por envio de spam pelo Bitdefender.
  - Se o seu cliente de e-mail está configurado para receber mensagens de e-mail usando outro protocolo além de POP3 (por exemplo, IMAP4), o filtro Antispam do Bitdefender não os verifica por envio de spam.



### Nota

POP3 é um dos protocolos mais utilizados para fazer o download de mensagens de e-mail a partir de um servidor de correio. Se você não sabe o protocolo que o seu cliente de e-mail utiliza para importar mensagens de e-mail, pergunte à pessoa que configurou o seu cliente de e-mail.

- Bitdefender Total Security não verifica tráfego POP3 do Lotus Notes.



Uma possível solução é reparar ou reinstalar o produto. Contudo, você poderá contatar a Bitdefender para suporte, como descrito na seção *“Solicite Ajuda”* (p. 287).

## A funcionalidade Preenchimento Automático não funciona na minha Carteira

Você salvou suas credenciais online no Gerenciador de Senhas do seu Bitdefender e notou que o preenchimento automático não funciona. Normalmente, este problema surge quando a extensão da Carteira do Bitdefender não está instalada no seu navegador.

Para resolver esta situação, siga os seguintes passos:

### ● No Internet Explorer:

1. Abra o Internet Explorer.
2. Clique em Ferramentas.
3. Clique em Gerenciar Suplementos.
4. Clique em Barras de Ferramentas e Extensões.
5. Vá em **Carteira do Bitdefender** e clique em **Ativar**.

### ● No Mozilla Firefox:

1. Abrir o Mozilla Firefox.
2. Clique em Ferramentas.
3. Clique em Add-ons.
4. Clique em Extensões.
5. Vá em **Carteira do Bitdefender** e clique em **Ativar**.

### ● No Google Chrome:

1. Abrir o Google Chrome.
2. Acesse o ícone Menu.
3. Clique em Definições.
4. Clique em Extensões.
5. Vá em **Carteira do Bitdefender** e clique em **Ativar**.



## Nota

O add-on será ativado após você reiniciar seu navegador.

Agora verifique se o recurso de auto completar na Carteira está funcionando para suas contas online.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção *"Solicite Ajuda"* (p. 287).

## A Remoção do Bitdefender falhou

Caso queira remover o seu produto Bitdefender e observar que o processo demora ou o sistema trava, clique em **Cancelar** para abortar a ação. Caso não funcione, reinicie o sistema.

Se a remoção falhar, algumas chaves do registro e arquivos do Bitdefender poderão permanecer em seu sistema. Estes arquivos remanescentes poderão evitar uma nova instalação do Bitdefender. Elas também podem afetar o desempenho do sistema e sua estabilidade.

Para remover o Bitdefender completamente do seu sistema:

### ● No Windows 7:

1. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Programas e Recursos**.
2. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
3. Clique em **REMOVER** na janela que aparecer, depois escolha quais dados devem ser salvos para uma instalação posterior:
  - Arquivos em quarentena
  - Carteiras
  - Arquivos Cofre
4. Clique em **CONTINUAR**.
5. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

### ● No Windows 8 e Windows 8.1:

1. No tela inicial do Windows, localize **Painel de Controle** (por exemplo, você pode começar digitando "Painel de Controle" diretamente na tela inicial) e depois clique no ícone.





2. Clique em **Desinstalar um programa** ou **Programas e Recursos**.
  3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
  4. Clique em **REMOVER** na janela que aparecer, depois escolha quais dados devem ser salvos para uma instalação posterior:
    - Arquivos em quarentena
    - Carteiras
    - Arquivos Cofre
  5. Clique em **CONTINUAR**.
  6. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.
- No **Windows 10**:
1. Clique em **Iniciar** e depois em Configurações.
  2. Clique no ícone **Sistema** na área de Configurações e então selecione **Aplicativos instalados**.
  3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
  4. Clique em **Desinstalar** novamente para confirmar sua escolha.
  5. Clique em **REMOVER** na janela que aparecer, depois escolha quais dados devem ser salvos para uma instalação posterior:
    - Arquivos em quarentena
    - Carteiras
    - Arquivos Cofre
  6. Clique em **CONTINUAR**.
  7. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

## O meu sistema não reinicia após a instalação de Bitdefender

Se instalou o Bitdefender e não consegue reiniciar o seu sistema no modo normal, são vários os motivos para este tipo de problema.

Isto é muito provavelmente causado por uma instalação anterior de Bitdefender que não foi removida adequadamente ou por outra solução de segurança que ainda se encontra no sistema.



Eis como pode resolver cada situação:

● **Você tinha o Bitdefender anteriormente e não o removeu corretamente.**

Para resolver isto:

1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como fazer isto, consulte **“Como posso reiniciar no Modo de Segurança?”** (p. 82).

2. Remova Bitdefender do seu sistema:

● **No Windows 7:**

a. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Programas e Recursos**.

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

c. Clique em **REMOVER** na janela que aparecer, depois escolha quais dados devem ser salvos para uma instalação posterior:

● Arquivos em quarentena

● Carteiras

● Arquivos Cofre

d. Clique em **CONTINUAR**.

e. Aguarde até que o processo de desinstalação seja finalizado.

f. Reinicie seu sistema no modo normal.

● **No Windows 8 e Windows 8.1:**

a. No tela inicial do Windows, localize **Painel de Controle** (por exemplo, você pode começar digitando "Painel de Controle" diretamente na tela inicial) e depois clique no ícone.

b. Clique em **Desinstalar um programa** ou **Programas e Recursos**.

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

d. Clique em **REMOVER** na janela que aparecer, depois escolha quais dados devem ser salvos para uma instalação posterior:

● Arquivos em quarentena

● Carteiras

● Arquivos Cofre



- e. Clique em **CONTINUAR**.
- f. Aguarde até que o processo de desinstalação seja finalizado.
- g. Reinicie seu sistema no modo normal.

● **No Windows 10:**

- a. Clique em **Iniciar** e depois em Configurações.
- b. Clique no ícone **Sistema** na área de Configurações e então selecione **Aplicativos instalados**.
- c. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
- d. Clique em **Desinstalar** novamente para confirmar sua escolha.
- e. Clique em **REMOVER** na janela que aparecer, depois escolha quais dados devem ser salvos para uma instalação posterior:
  - Arquivos em quarentena
  - Carteiras
  - Arquivos Cofre
- f. Clique em **CONTINUAR**.
- g. Aguarde até que o processo de desinstalação seja finalizado.
- h. Reinicie seu sistema no modo normal.

3. Reinstale seu produto Bitdefender

● **Você tinha uma solução de segurança diferente anteriormente e não a eliminou corretamente.**

Para resolver isto:

1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como fazer isto, consulte **“Como posso reiniciar no Modo de Segurança?”** (p. 82).
2. Remova as demais soluções de segurança do seu sistema:

● **No Windows 7:**

- a. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Programas e Recursos**.
- b. Encontre o nome do programa que pretende remover e selecione **Remover**.



- c. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.
- **No Windows 8 e Windows 8.1:**
  - a. No tela inicial do Windows, localize **Painel de Controle** (por exemplo, você pode começar digitando "Painel de Controle" diretamente na tela inicial) e depois clique no ícone.
  - b. Clique em **Desinstalar um programa** ou **Programas e Recursos**.
  - c. Encontre o nome do programa que pretende remover e selecione **Remover**.
  - d. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.
- **No Windows 10:**
  - a. Clique em **Iniciar** e depois em Configurações.
  - b. Clique no ícone **Sistema** na área de Configurações e então selecione **Aplicativos instalados**.
  - c. Encontre o nome do programa que pretende remover e selecione **Desinstalar**.
  - d. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

Para desinstalar corretamente outro software, acesse o site do fornecedor e execute a ferramenta de desinstalação ou contate-o diretamente, para que lhe indiquem os procedimentos de desinstalação.

3. Reinicie o seu sistema no modo normal e reinstale o Bitdefender.

### **Já seguiu os passos acima e o problema não está resolvido.**

Para resolver isto:

1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como fazer isto, consulte "[Como posso reiniciar no Modo de Segurança?](#)" (p. 82).
2. Usar a opção de Restauração do Sistema do Windows para restaurar o computador para uma data anterior antes de instalar o produto Bitdefender.
3. Reinicie o sistema no modo normal e contate os nossos representantes do suporte conforme descrito na seção "[Solicite Ajuda](#)" (p. 287).



## 6.2. Remover malware do seu sistema

O malware pode afectar o seu sistema de várias formas e a actuação do Bitdefender depende do tipo de ataque por malware. Como os vírus alteram frequentemente o modo de ação, é difícil estabelecer um padrão com base no comportamento e nas ações.

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

- “Modo de Recuperação Bitdefender” (p. 207)
- “O que fazer se o Bitdefender encontrar vírus no seu computador?” (p. 210)
- “Como posso limpar um vírus num arquivo?” (p. 211)
- “Como posso limpar um vírus de um arquivo de correio eletrónico?” (p. 213)
- “O que fazer se eu suspeitar que um arquivo seja perigoso?” (p. 214)
- “O que são arquivos protegidos por senha no registro de análise?” (p. 214)
- “Quais são os itens ignorados no relatório de análise?” (p. 215)
- “O que são arquivos muito comprimidos no registro de análise?” (p. 215)
- “Por que é que o Bitdefender eliminou automaticamente um arquivo infectado?” (p. 215)

Se não conseguir encontrar o seu problema aqui, ou se as soluções apresentadas não resolvem o seu problema, pode contactar os representantes do apoio técnico da Bitdefender como mostrado no capítulo “*Solicite Ajuda*” (p. 287).

## Modo de Recuperação Bitdefender


**Modo do Recuperação** é uma característica do Bitdefender que lhe permite analisar e desinfetar todas as partições do disco rígido existentes fora do seu sistema operacional.

Quando o Bitdefender Total Security é instalado e o arquivo de Imagem de Resgate do Bitdefender baixado, o Modo de Resgate pode ser usado mesmo se você não conseguir iniciar o Windows.



## Baixando a Imagem de Resgate do Bitdefender

Para poder usar o Modo de Resgate, é necessário primeiro baixar seu arquivo de imagem da seguinte forma:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **ANTIVÍRUS**, selecione **Modo de Resgate**.
4. Clique em **SIM** na janela de confirmação que aparece para reiniciar seu computador.

Aguarde a Imagem de Resgate do Bitdefender ser obtida dos servidores Bitdefender. Assim que o processo de download for finalizado, o computador será reiniciado.


Um menu aparecerá para você selecionar um sistema operacional. Neste passo, você pode escolher iniciar seu sistema no Modo de Resgate ou no modo normal.

## Iniciar o seu sistema no Modo de Recuperação

Você pode entrar no Modo de Recuperação de duas formas:

Na **interface do Bitdefender**

Para entrar no Modo de Resgate diretamente do Bitdefender:

1. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
2. Clique no botão **VER MÓDULOS**.
3. No módulo **ANTIVÍRUS**, selecione **Modo de Resgate**.
4. Clique em **SIM** na janela de confirmação que aparece para reiniciar seu computador.
5. Depois que o computador se reiniciar, um menu aparecerá para você selecionar um sistema operacional. Escolha **Modo de Resgate do Bitdefender** para inicializar em um ambiente do Bitdefender onde você pode limpar sua partição do Windows.
6. Se notificado, pressione **Enter** e selecione a resolução de tela mais próxima da que você normalmente usa. Depois pressione novamente **Enter**.



O Modo de Resgate do Bitdefender carrega em alguns instantes.

Inicialize o seu computador diretamente no Modo de Recuperação

Se o Windows já não iniciar, você pode inicializar o seu computador diretamente no Modo de Recuperação do Bitdefender, seguindo os passos abaixo:

1. Inicie / reinicie o seu computador e comece a pressionar a tecla **espaços** do seu teclado antes de aparecer o logo do Windows.
2. Um menu aparecerá solicitando que você selecione um sistema operacional para iniciar. Pressione **TAB** para ir para a área de ferramentas. Escolha **Imagem de Recuperação Bitdefender** e prima a tecla **Enter** para inicializar num ambiente do Bitdefender onde poderá limpar a sua partição Windows.
3. Se notificado, pressione **Enter** e selecione a resolução de tela mais próxima da que você normalmente usa. Depois pressione novamente **Enter**.

O Modo de Recuperação do Bitdefender irá carregar dentro de alguns minutos.

## Analisar o seu sistema no Modo de Recuperação

Para verificar seu sistema no Modo de Resgate:

1. Entre no Modo de Recuperação, conforme descrito em **“Iniciar o seu sistema no Modo de Recuperação”** (p. 208).
2. O logo do Bitdefender surgirá e os motores antivírus começarão a ser copiados.
3. Uma janela de boas-vindas aparecerá. Clique em **Continuar**.
4. Iniciou-se uma atualização de assinaturas antivírus.
5. Após o fim da atualização, a janela do Verificador de Antivírus do Bitdefender aparecerá.
6. Clique em **Verificar agora**, selecione o alvo da verificação na janela que aparece e depois clique em **Abrir** para iniciar.

Recomenda-se que analise toda a partição do Windows.



## **Nota**

Ao trabalhar no Modo de Recuperação, você lida com nomes de partições do tipo do Linux. As partições do disco surgirão como sda1 provavelmente correspondendo à (C:) partição do Windows, sda2 correspondendo a (D:) e assim sucessivamente.

7. Aguarde o término da análise. Caso algum malware seja detectado, siga as instruções para remover a ameaça.
8. Para sair do Modo de Resgate, dê um clique duplo em uma área vazia da área de trabalho e selecione **Sair** no menu, depois escolha se deseja reiniciar ou desligar o computador.

## O que fazer se o Bitdefender encontrar vírus no seu computador?

Pode verificar se há um vírus no seu computador de uma das seguintes formas:

- O Bitdefender analisou o seu computador e encontrou itens infectados.
- Um alerta de vírus avisa que o Bitdefender bloqueou um ou vários vírus no seu computador.

Nestas situações, atualize o Bitdefender para se certificar que possui as assinaturas de malware mais recentes e realize uma Análise de Sistema.

Assim que a análise terminar, selecione a ação pretendida para os itens infectados (Desinfectar, Eliminar, Mover para a Quarentena).

## **Atenção**

Se suspeitar que o arquivo faz parte do sistema operativo do Windows ou que não é um arquivo infectado, não siga estes passos e contacte o Apoio ao Cliente do Bitdefender assim que possível.



Se não for possível efectuar a ação seleccionada e o relatório da análise indicar uma infecção que não foi possível eliminar, tem de remover o(s) arquivo(s) manualmente:

**O primeiro método pode ser utilizado no modo normal:**

1. Desative a proteção antivírus em tempo real do Bitdefender:





- a. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
  - b. Selecione o link **VER MÓDULOS**.
  - c. Selecione o ícone  no canto superior direito do módulo **ANTIVÍRUS**.
  - d. Clique no botão correspondente para desativar a **Verificação no acesso**.
2. Mostrar objetos ocultos no Windows. Para saber como fazer isto, consulte **“Como posso mostrar objetos ocultos no Windows?”** (p. 80).
  3. Procure a localização do arquivo infectado (veja no relatório da análise) e elimine-o.
  4. Active a proteção antivírus em tempo real do Bitdefender.

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

1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como fazer isto, consulte **“Como posso reiniciar no Modo de Segurança?”** (p. 82).
2. Mostrar objetos ocultos no Windows. Para saber como fazer isto, consulte **“Como posso mostrar objetos ocultos no Windows?”** (p. 80).
3. Procure a localização do arquivo infectado (veja no relatório da análise) e elimine-o.
4. Reinicie o seu sistema e inicie sessão no modo normal.

Se esta informação não foi útil, você pode contactar a Bitdefender para suporte, como descrito na seção **“Solicite Ajuda”** (p. 287).

## **Como posso limpar um vírus num arquivo?**

Um arquivo é um arquivo ou um conjunto de arquivos comprimidos num formato especial para reduzir o espaço no disco necessário para armazenar os arquivos.



Alguns destes formatos são formatos livres, possibilitando ao Bitdefender a opção de analisar o conteúdo e aplicar as ações adequadas para os remover.

Outros formatos de arquivo estão parcial ou totalmente fechados, mas o Bitdefender só pode detectar a presença de vírus no interior, mas não pode aplicar outras ações.



Se o Bitdefender avisar que foi detectado um vírus dentro de um arquivo e não estiver disponível uma ação, significa que não é possível remover o vírus devido a restrições nas definições de permissão do arquivo.

Pode limpar um vírus armazenado num arquivo da seguinte forma:

1. Identifique o arquivo que contém o vírus ao realizar uma Análise Completa do sistema.
2. Desative a proteção antivírus em tempo real do Bitdefender:
  - a. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
  - b. Selecione o link **VER MÓDULOS**.
  - c. Selecione o ícone  no canto superior direito do módulo **ANTIVÍRUS**.
  - d. Na aba **PROTEÇÃO**, clique no botão correspondente para desativar a **verificação no acesso**.
3. Vá à localização do arquivo e descompacte-o com uma aplicação de arquivo, como o WinZip.
4. Identifique e elimine o arquivo infectado.
5. Elimine o arquivo original de modo a garantir que a infecção é totalmente removida.
6. Comprima novamente os arquivos num novo arquivo com uma aplicação de arquivo, como o WinZip.
7. Ative a proteção antivírus em tempo real do Bitdefender e execute uma Verificação do sistema para garantir que não haja outra infecção no sistema.



## Nota

É importante observar que um vírus armazenado num arquivo não é uma ameaça imediata ao seu sistema, pois o vírus deve ser descompactado e executado para infectar o seu sistema.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção **"Solicite Ajuda"** (p. 287).





## Como posso limpar um vírus de um arquivo de correio eletrônico?

O Bitdefender também pode identificar vírus em bases de dados de correio eletrônico e arquivos de correio eletrônico armazenados no disco.

Por vezes, é necessário identificar a mensagem infectada com a informação fornecida no relatório da análise, e elimine-o manualmente.

Pode limpar um vírus armazenado num arquivo de correio eletrônico da seguinte forma:

1. Analisar a base de dados do correio eletrônico com o Bitdefender.
2. Desative a proteção antivírus em tempo real do Bitdefender:
  - a. Clique no ícone  na barra lateral esquerda da **interface do Bitdefender**.
  - b. Selecione o link **VER MÓDULOS**.
  - c. Selecione o ícone  no canto superior direito do módulo **ANTIVÍRUS**.
  - d. Clique no botão correspondente para desativar a **Verificação no acesso**.
3. Abra o relatório da análise e utilize a informação de identificação (Assunto, De, Para) das mensagens infectadas para localizá-las no cliente de correio eletrônico.
4. Elimine as mensagens infectadas. A maioria dos clientes de correio eletrônico move a mensagem eliminada para uma pasta de recuperação, a partir da qual pode ser recuperada. Deve certificar-se que a mensagem também é eliminada desta pasta de recuperação.
5. Compactar a pasta com a mensagem infectada.
  - No Microsoft Outlook 2007: No menu Arquivo, clique em Gestão de Arquivos de Dados. Selecione os arquivos das pastas (.pst) que pretende compactar e clique em Definições. Clique em Compactar Agora.
  - No Microsoft Outlook 2010 / 2013: No menu Arquivo, clique em informações, depois em configurações da conta (adicione ou remova contas ou modifique configurações de conexão existentes). Clique em Arquivo de Dados, selecione os arquivos das pastas (.pst) que pretende compactar e clique em Configurações. Clique em Compactar Agora.
6. Active a proteção antivírus em tempo real do Bitdefender.



Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção *"Solicite Ajuda"* (p. 287).

## O que fazer se eu suspeitar que um arquivo seja perigoso?

Você pode suspeitar que um arquivo do seu sistema é perigoso, embora o seu produto Bitdefender não o tenha detectado.

Para garantir que seu sistema esteja protegido:

1. Execute uma **Análise de Sistema** com o Bitdefender. Para saber como fazer isto, consulte *"Como posso analisar o meu sistema?"* (p. 59).
2. Se o resultado da análise parece estar limpo, mas você ainda tem dúvidas e quer verificar o arquivo, entre em contato com os representantes do suporte para que possamos ajudá-lo.

Para saber como fazer isto, consulte *"Solicite Ajuda"* (p. 287).

## O que são arquivos protegidos por senha no registro de análise?

Isto é apenas uma notificação que indica que o Bitdefender detectou que estes arquivos estão protegidos por senha ou por outra forma de encriptação.

Normalmente, os itens protegidos por senha são:

- Arquivos que pertencem a outras solução de segurança.
- Arquivos que pertencem ao sistema operativo.

Para analisar verdadeiramente os conteúdos, estes arquivos têm de ser extraídos ou de outra forma descodificados.

Se estes conteúdos pudessem ser extraídos, o verificador em tempo real do Bitdefender analisaria-os automaticamente para manter o seu computador protegido. Se pretende analisar esses arquivos com Bitdefender, terá de contactar o fabricante do produto para receber mais informações sobre esses arquivos.

Recomendamos que ignore estes arquivos pois não constituem uma ameaça ao seu sistema.



## Quais são os itens ignorados no relatório de análise?

Todos os arquivos que aparecem como Ignorados no relatório de análise estão limpos.

Para um melhor desempenho, o Bitdefender não analisa arquivos que não tenham sido alterados desde a última análise.

## O que são arquivos muito comprimidos no registro de análise?

Os itens sobre-comprimidos são elementos que não puderam ser extraídos pelo motor de análise ou elementos para os quais a descriptação levaria muito tempo, tornando o sistema instável.

Supercompactado significa que o Bitdefender não realizou a análise desse arquivo, pois a descompactação iria consumir muitos recursos do sistema. O conteúdo será analisado em acesso de tempo real, caso necessário.

## Por que é que o Bitdefender eliminou automaticamente um arquivo infectado?

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

Para determinados tipos de malware, a desinfecção não é possível porque o arquivo detectado é totalmente malicioso. Nestes casos, o arquivo infectado é eliminado do disco.

Este é, normalmente, o caso de arquivos de instalação que são transferidos de sítios de Internet suspeitos. Se se encontrar numa situação assim, transfira o arquivo de instalação do sítio de Internet do fabricante ou de outro sítio fiável.



## **ANTIVIRUS FOR MAC**



## 7. INSTALAÇÃO E REMOÇÃO

Este capítulo inclui os seguintes tópicos:

- *“Requisitos de Sistema”* (p. 217)
- *“Instalando o Bitdefender Antivirus for Mac”* (p. 217)
- *“Removendo o Bitdefender Antivirus for Mac”* (p. 224)

### 7.1. Requisitos de Sistema

Você somente pode instalar o Bitdefender Antivirus for Mac em computadores Macintosh com Intel e com OS X Mavericks (10.9.5), OS X Yosemite (10.10 ou superior), OS X El Capitan (10.11), OS X Sierra(10.12) instalados.

Seu Mac também deve atender a todos esses requisitos adicionais:

- Mínimo de 1 GB de Memória RAM
- Espaço mínimo de 600 MB disponível no disco rígido

É necessário ter conexão com a internet para registrar e atualizar o Bitdefender Antivirus for Mac.

#### Como descobrir a versão do seu OS X e informações de hardware do seu Mac

Clique no ícone da Apple no canto superior esquerdo da tela e escolha **Sobre este Mac**. Na janela que aparece, você pode ver a versão do seu sistema operacional e outras informações úteis. Clique em **Mais informações** para informações detalhadas de hardware.

### 7.2. Instalando o Bitdefender Antivirus for Mac

Você pode instalar o Bitdefender Antivirus for Mac desde:

- Bitdefender Central
- CD/DVD

#### 7.2.1. Instalar da Bitdefender Central

Você pode baixar o kit de instalação da sua Bitdefender Central. Uma vez que o processo de instalação estiver concluído, o Bitdefender Antivirus for Mac é ativado.



Para fazer download do Bitdefender Antivirus for Mac da sua conta Bitdefender Central, siga os seguintes passos:

1. Faça login como administrador.
2. Acesse: <https://central.bitdefender.com>.
3. Faça login na sua conta Bitdefender usando seu e-mail e senha.
4. Na janela **MEUS DISPOSITIVOS**, clique em **INSTALAR Bitdefender**.
5. Escolha uma das duas opções disponíveis:

● **DOWNLOAD**

Clique no botão e salve o arquivo de instalação.

● **Em outro dispositivo**

Selecione **OS X** para fazer download do seu produto Bitdefender e, em seguida, clique em **CONTINUAR**. Digite um endereço de e-mail no campo correspondente e clique em **ENVIAR**.

6. Execute o Bitdefender que você baixou.
7. Complete os passos de instalação. Para mais detalhes sobre este processo, acesse "*Processo de instalação*" (p. 220).

## 7.2.2. Instalar a partir do CD/DVD

1. Insira o CD/DVD de instalação na unidade e abra-o. Acesse o atalho para baixar o instalador.
2. Complete os passos de instalação. Para mais detalhes sobre este processo, acesse "*Processo de instalação*" (p. 220).
3. Faça login na sua conta **Bitdefender Central**:

**i** **Nota**

Se você já tem uma assinatura do Bitdefender Antivirus for Mac ativa, simplesmente faça login usando a conta Bitdefender com a qual a assinatura está associada e o produto será ativado.

Se sua conta Bitdefender não tem uma assinatura associada, ou se você ainda não tem uma conta, prossiga de acordo com sua situação:

**Já tenho uma conta Bitdefender**

Digite o endereço de e-mail e a senha da sua conta Bitdefender, e então clique em **ENTRAR**.





Se você esqueceu a senha da sua conta, ou simplesmente deseja criar uma nova, clique no link **Esqueci minha senha**. Digite seu endereço de e-mail e depois clique no botão **ESQUECI A SENHA**. Confira seu e-mail e siga as instruções fornecidas para definir uma nova senha para a sua conta Bitdefender.

**i** **Nota**  
Caso você já tenha uma conta MyBitdefender, pode usá-la para entrar na sua conta Bitdefender. Se você esqueceu sua senha, precisa ir primeiro em <https://my.bitdefender.com> para redefini-la. Depois, use as credenciais atualizadas para entrar na sua conta Bitdefender.

## Quero criar uma conta Bitdefender

Para criar uma conta Bitdefender, clique no link **Criar**. Digite a informação solicitada nos campos correspondentes, e então clique no botão **CRIAR CONTA**.

Leia os Termos de Serviço da Bitdefender antes de continuar.

Os dados que nos fornecer serão mantidos confidenciais.

Neste caso, o período de avaliação de 30 dias será ativado automaticamente. Antes do período de avaliação expirar, ative sua assinatura seguindo os passos de *"Ativar assinatura"* (p. 244).

**i** **Nota**  
Uma vez a conta criada, você pode usar o endereço de e-mail fornecido e a senha para fazer o login na sua conta em <https://central.bitdefender.com>.

## Quero executar o login usando minha conta do Microsoft, Facebook ou Google.

Para entrar com sua conta Microsoft, Facebook ou Google:

- Selecione o serviço que deseja usar. Você será redirecionado para a página de início de sessão daquele serviço.
- Siga as instruções fornecidas pelo serviço selecionado para ligar a sua conta ao Bitdefender.

**i** **Nota**  
O Bitdefender não tem acesso a qualquer informação confidencial como a senha da conta que você usa para efetuar o log in, ou a informações pessoais de seus amigos e contatos.



## 7.2.3. Processo de instalação

Para instalar o Bitdefender Antivirus for Mac:

1. Clique no arquivo baixado. O instalador será iniciado e você será guiado pelo processo de instalação.
2. Siga o assistente de instalação.

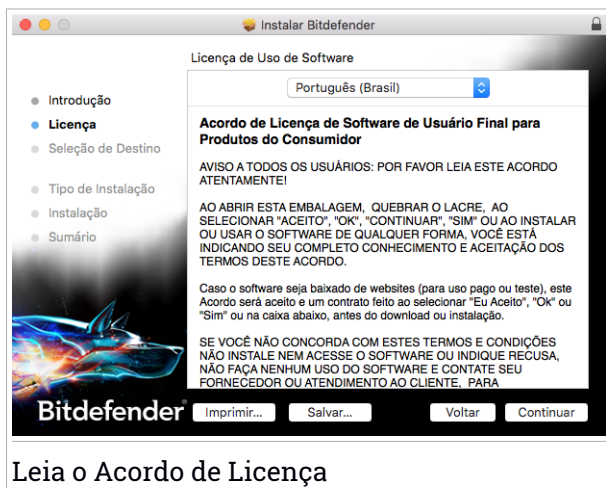
### Passo 1 - Janela de Boas-Vindas



Clique em **Continuar**.



## Passo 2 - Ler o Acordo de Licença



O Acordo de Licença é um acordo legal entre você e a Bitdefender para o uso do Bitdefender Antivirus for Mac. Você pode salvar o Acordo de Licença para revisá-lo mais tarde.

Por favor, leia o Acordo de Licença cuidadosamente. Para continuar a instalação do software, você precisa concordar com os termos do acordo de licença do software. Clique em **Continuar** e depois em **Concordar**.



### Importante

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



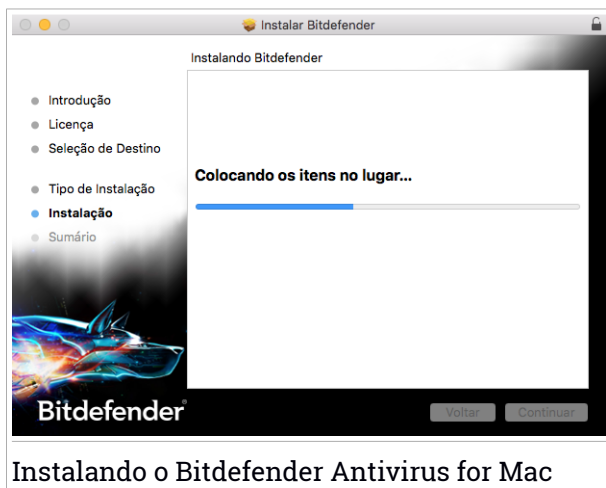
## Passo 3 - Iniciar instalação



O Bitdefender Antivirus for Mac será instalado em Macintosh HD/Biblioteca/Bitdefender. O caminho da instalação não pode ser modificado. Clique em **Instalar** para iniciar a instalação.

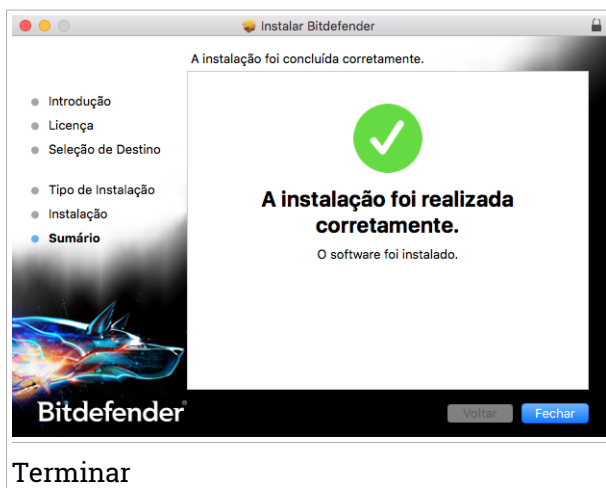


## Passo 4 - Instalando o Bitdefender Antivirus for Mac



Aguarde a instalação ser concluída e clique em **Continuar**.

## Passo 5 - Terminar



Clique em **Fechar** para fechar a janela do instalador.  
O processo de instalação agora está completo.



Na primeira instalação do Bitdefender Antivirus for Mac, o assistente da Proteção da Máquina do Tempo aparecerá. Para mais informações, acesse "*Proteção da Máquina do Tempo*" (p. 230).

## 7.3. Removendo o Bitdefender Antivirus for Mac

Por ser um aplicativo complexo, o Bitdefender Antivirus for Mac não pode ser removido da forma convencional, ou seja, arrastando o ícone do aplicativo da pasta Aplicativos para a Lixeira.

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

1. Abra uma janela do **Finder**, vá para a pasta Aplicativos e escolha Utilitários.
2. Dê um clique duplo no aplicativo Desinstalador Bitdefender para Mac para abri-lo.
3. Clique no botão **Desinstalar** e aguarde o processo ser concluído.
4. Clique em **Fechar** para finalizar.



### Importante

Caso haja um erro, você pode entrar em contato com o Atendimento ao Consumidor da Bitdefender, como descrito em "*Solicite Ajuda*" (p. 287).



## 8. INTRODUÇÃO

Este capítulo inclui os seguintes tópicos:

- “*Sobre o Bitdefender Antivirus for Mac*” (p. 225)
- “*Abrindo o Bitdefender Antivirus for Mac*” (p. 225)
- “*Janela principal do aplicativo*” (p. 225)
- “*Ícone do aplicativo no Dock*” (p. 227)

### 8.1. Sobre o Bitdefender Antivirus for Mac


O Bitdefender Antivirus for Mac é um verificador antivírus poderoso, que pode detectar e remover todos os tipos de software maliciosos (“malware”), incluindo:

- adware
- Vírus
- Spyware
- Cavalos de Troia
- keyloggers
- worms

Este aplicativo detecta e remove não só malware para Mac, mas também malware para Windows, prevenindo, assim, que você envie arquivos infectados para sua família, amigos e colegas usando PCs.

### 8.2. Abrindo o Bitdefender Antivirus for Mac

Você pode abrir o Bitdefender Antivirus for Mac de diversas formas.

- Clique no ícone do Bitdefender Antivirus for Mac no Launchpad.
- Clique no ícone  na barra de menu e escolha **Abrir Janela Principal**.
- Abra uma janela do Finder, vá em Aplicativos e dê um clique duplo no ícone Bitdefender Antivirus for Mac.

### 8.3. Janela principal do aplicativo

Na janela principal do aplicativo, você pode conferir o status de segurança do seu computador, realizar varreduras no sistema, tornar sua navegação na web mais segura, ou fazer login em conta Bitdefender.



Janela principal do aplicativo

A opção **Autopilot**, localizada na parte direita superior da janela principal, monitora continuamente os aplicativos executados no computador, à procura de ações típicas de malware, e previne que novas ameaças de malware entrem no seu sistema.

Por motivos de segurança, é recomendável deixar o Autopilot ligado. Se o Autopilot estiver desligado, você não estará protegido automaticamente contra ameaças de malware.

A barra de status no topo da janela o informa sobre o status de segurança do sistema usando mensagens explícitas e cores sugestivas. Se o Bitdefender Antivirus for Mac não tiver alertas, a barra de status é verde. Quando um problema de segurança é detectado, a barra de status muda para amarelo. Clique no botão **Visualizar incidências** para visualizar os problemas que afetam a segurança do seu sistema. Para informações detalhadas sobre problemas e como repará-los, acesse *"Reparando Incidências"* (p. 232).

Abaixo da barra de status, três botões de verificação estão disponíveis para ajudá-lo a verificar seu Mac:

- **Verificação Rápida** - procura por malware nos locais mais vulneráveis no seu sistema (por exemplo, as pastas que contêm os documentos, downloads, downloads de e-mail e arquivos temporários de cada usuário).





- **Verificação Completa** - realiza uma busca completa por malware em todo o sistema. Todas as montagens conectadas também serão verificadas.
- **Verificação Personalizada** - ajuda a procurar por malware em arquivos, pastas ou volumes específicos.

Para mais informações, acesse "[Verificando seu Mac](#)" (p. 229).

Além dos botões de verificação, há mais opções disponíveis:

- **Proteção na Web** - filtra todo o tráfego na web e bloqueia qualquer conteúdo malicioso para tornar sua experiência na web mais segura. Para mais informações, acesse "[Proteção da Internet](#)" (p. 262).
- **Ir para conta Bitdefender** - clique no link **Ir para sua conta** na parte inferior direita da interface principal para acessar sua conta Bitdefender. Para mais informações, acesse "[Bitdefender Central](#)" (p. 243).
- **Número de dias restantes** - exibe o tempo restante antes da sua assinatura expirar. Quando a data de expiração chegar, clique no link para acessar a página da web onde você poderá renovar sua assinatura.
- **Comprar** - redireciona-o para a página da Bitdefender, onde é possível conferir as ofertas disponíveis ou comprar uma assinatura.
- **Feedback** - abre uma nova janela no seu e-mail de cliente padrão para entrar em contato conosco.

## 8.4. Ícone do aplicativo no Dock

O ícone do Bitdefender Antivirus for Mac pode ser visto no Dock assim que você abrir o aplicativo. O ícone no Dock lhe proporciona uma forma fácil de procurar por malware em arquivos e pastas. Basta arrastar e soltar o arquivo ou pasta no ícone do Dock e a verificação iniciará imediatamente.





## 9. PROTEGENDO CONTRA SOFTWARES MALICIOSOS

Este capítulo inclui os seguintes tópicos:

- “*Melhores Práticas*” (p. 228)
- “*Verificando seu Mac*” (p. 229)
- “*Ligando ou desligando o Autopilot*” (p. 230)
- “*Proteção da Máquina do Tempo*” (p. 230)
- “*Assistente de Análise*” (p. 232)
- “*Reparando Incidências*” (p. 232)
- “*Proteção da Internet*” (p. 262)
- “*ATUALIZAÇÕES*” (p. 235)

### 9.1. Melhores Práticas

Para manter seu sistema livre de malware e evitar infecções acidentais de outros sistemas, siga estas práticas:

- Mantenha o **Autopilot** ligado para permitir que os arquivos do sistema sejam verificados pelo Bitdefender Antivirus for Mac.
- Mantenha seu Bitdefender Antivirus for Mac atualizado com as assinaturas de malware e atualizações de produto mais recentes, enquanto o **Autopilot** está ativado.
- Confira e repare os problemas relatados pelo Bitdefender Antivirus for Mac regularmente. Para informações detalhadas, acesse “*Reparando Incidências*” (p. 232).
- Confira o registro detalhado de eventos em relação à atividade do Bitdefender Antivirus for Mac no seu computador. Sempre que algo relevante para a segurança do seu sistema ou dados acontecer, uma nova mensagem será adicionada ao histórico do Bitdefender. Para mais detalhes, acesse “*Histórico*” (p. 240).
- É recomendável que você também siga estas práticas:
  - Crie o hábito de verificar arquivos que você baixar de uma memória de armazenamento externa (como um pen-drive ou CD), especialmente quando desconhecer a fonte.



- Se você tem um arquivo DMG, monte-o e verifique seu conteúdo (os arquivos dentro do volume/imagem montada).

A forma mais fácil de verificar um arquivo, pasta ou volume é arrastar e soltar na janela ou ícone do Bitdefender Antivirus for Mac no Dock.

Nenhuma outra configuração ou ação é necessária. No entanto, se você quiser, é possível ajustar as configurações e preferências do aplicativo para melhor atender suas necessidades. Para mais informações, acesse "*Configurando Preferências*" (p. 237).

## 9.2. Verificando seu Mac

Além do recurso de **Autopilot**, que continuamente monitora as aplicações em execução no computador à procura de ações típicas de malware e previne que novas ameaças de malware entrem no seu sistema, você pode verificar seu Mac ou arquivos específicos sempre que quiser.

A forma mais fácil de verificar um arquivo, pasta ou volume é arrastar e soltar na janela ou ícone do Bitdefender Antivirus for Mac no Dock. O assistente de verificação aparecerá e o guiará pelo processo de verificação.

Você também pode iniciar uma verificação da seguinte forma:

1. Abra o Bitdefender Antivirus for Mac.
2. Clique em um dos três botões para iniciar a verificação desejada.
  - **Verificação Rápida** - procura por malware nos locais mais vulneráveis no seu sistema (por exemplo, as pastas que contêm os documentos, downloads, downloads de e-mail e arquivos temporários de cada usuário).
  - **Verificação Completa** - realiza uma busca completa por malware em todo o sistema. Todas as montagens conectadas também serão verificadas.



### Nota

Dependendo do tamanho do seu disco rígido, verificar todo seu sistema pode demorar (até uma hora ou mais). Para um melhor desempenho, é recomendável não executar essa tarefa enquanto executa outras tarefas intensivas (como edição de vídeos).


Se preferir, você pode escolher não verificar volumes montados específicos adicionando-os à lista **Exclusões** na janela de Preferências.



- **Verificação Personalizada** - ajuda a procurar por malware em arquivos, pastas ou volumes específicos.

## 9.3. Ligando ou desligando o Autopilot

Para ligar ou desligar o Autopilot, siga qualquer um dos seguintes passos:

- Abra o Bitdefender Antivirus for Mac e clique no botão para ligar ou desligar o Autopilot.
- Clique no ícone  na barra de menu e escolha **DESLIGAR Autopilot**.



### Atenção

Recomendamos que desative o Autopilot pelo menor tempo possível. Se o Autopilot estiver desligado, você não estará protegido automaticamente contra ameaças de malware.

## 9.4. Proteção da Máquina do Tempo

A Proteção da Máquina do Tempo da Bitdefender funciona como uma camada de segurança adicional para o seu drive de backup, incluindo todos os arquivos nele armazenados, através do bloqueio do acesso de qualquer fonte externa. Caso os arquivos do seu drive da Máquina do Tempo sejam encriptados por ransomware, você poderá recuperá-los sem pagar pelo resgate.

## Assistente da Proteção da Máquina do Tempo

O assistente da Proteção da Máquina do Tempo da Bitdefender aparecerá assim que o Bitdefender Antivirus for Mac for instalado pela primeira vez no seu Macintosh.



Você precisa configurar o aplicativo do sistema de backup da Máquina do Tempo antes de habilitar a proteção do Bitdefender.

Se o recurso Máquina do Tempo não estiver habilitado na sua máquina:

1. Clique na opção **Ir para Máquina do Tempo**.

A janela **Máquina do Tempo** em Preferências do Sistema aparecerá.

2. Ative o recurso, e então selecione o local para armazenar os arquivos de backup.

Se precisar de mais informações sobre como ativar a aplicação Máquina do Tempo no seu sistema, clique no link **Descobrir como configurar o Máquina do Tempo** no assistente.

Para habilitar a Proteção da Máquina do Tempo do Bitdefender para os seus backups:

1. Clique na opção **Habilitar proteção**.  
Uma janela de confirmação aparecerá.
2. Clique em **Fechar**.

## Ativar ou desativar a Proteção da Máquina do Tempo

Ativar ou desativar a Proteção da Máquina do Tempo

1. Abra o Bitdefender Antivirus for Mac.
2. Clique em Bitdefender Antivirus for Mac na barra de menu e escolha **Preferências**.



3. Selecione a aba **Proteção**.
4. Selecione ou desmarque a caixa de seleção **Proteção da Máquina do Tempo**.

## 9.5. Assistente de Análise

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



Informações em tempo real sobre as ameaças detectadas e resolvidas são exibidas durante cada verificação.

Espre que o Bitdefender Antivirus for Mac termine a análise.



### Nota

O processo de análise pode demorar algum tempo, dependendo da complexidade da mesma.

## 9.6. Reparando Incidências

O Bitdefender Antivirus for Mac automaticamente detecta e o informa sobre uma série de problemas que podem afetar a segurança do seu sistema e dados. Dessa forma, você 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 detectados incluem:

- As novas assinaturas de malware e atualizações do produto não foram baixados dos nossos servidores porque o **Autopilot** está desabilitado.
- Ameaças não resolvidas foram detectadas no seu sistema.
- O **Autopilot** está desligado.

Para verificar e reparar os problemas detectados:

1. Abra o Bitdefender Antivirus for Mac.
2. Se o Bitdefender não tiver alertas, a barra de status é verde. Quando um problema de segurança é detectado, a barra de status muda para amarelo.
3. Confira a descrição para mais informações.
4. Quando um problema é detectado, clique no botão **Visualizar incidências** para ver informações sobre o que está afetando a segurança do seu sistema. Você pode escolher ações na janela que aparece.

Nome da infecção	Caminho para o arquivo infectado	Ação tomada
MAC.OSX.Trojan...	/Users/Shared/malware/CoinThief/StealthBit.app/Contents/...	
Mac.OSX.iWorm.F	/Users/Shared/malware/iWorm/Install.app/Contents/MacOS/0	
Mac.OSX.iWorm.D	/Users/Shared/malware/iWorm/JavaW	
MAC.OSX.Backd...	/Users/Shared/malware/Janicab/RecentNews.?fdp.app/Cont...	
MAC.OSX.Backd...	/Users/Shared/malware/Janicab/RecentNews.?fdp.app/Cont...	
MAC.OSX.Trojan...	/Users/Shared/malware/Janicab/RecentNews.?fdp.app/Cont...	
MAC.OSX.Backd...	/Users/Shared/malware/Janicab/RecentNews.?fdp.app/Cont...	

Revelar no Finder    Adicionar a Excluídas

Fechar

Janela de ameaças não resolvidas

A lista de ameaças não resolvidas é atualizada após cada verificação de sistema.

Você pode escolher as seguintes ações para ameaças não resolvidas:

- Revelar no Finder. Escolha essa ação para remover as infecções manualmente.



- **Adicionar às Exclusões.** Essa ação não está disponível para malware encontrado dentro de arquivos.

## 9.7. Proteção da Internet

O Bitdefender Antivirus for Mac usa as extensões do TrafficLight para tornar sua experiência de navegação na web completamente segura. As extensões do TrafficLight interceptam, processam e filtram todo o tráfego na web, bloqueando qualquer conteúdo malicioso.

As extensões trabalham e se integram com os seguintes navegadores de internet: Mozilla Firefox, Google Chrome e Safari.

Uma variedade de recursos está disponível para protegê-lo de todas as formas de ameaças que você pode encontrar enquanto navega na internet:

- **Filtro Avançado de Phishing** - previne que você acesse websites usados para ataques de phishing.
- **Filtro de Malware** - bloqueia qualquer malware que você encontre enquanto navega na internet.
- **Analizador de Resultados de Busca** - proporciona alertas antecipados de websites de risco nos seus resultados de busca.
- **Filtro Antifraude** - proporciona proteção contra websites fraudulentos enquanto você navega na internet.
- **Notificação de Rastreador** - detecta rastreadores em páginas visitadas enquanto protege sua privacidade online.

## Habilitando extensões do TrafficLight

Para habilitar as extensões do TrafficLight, siga estes passos:

1. Abra o Bitdefender Antivirus for Mac.
2. Clique em **Reparar Agora** para ativar a proteção na web.
3. O Bitdefender Antivirus for Mac detectará qual navegador você tem instalado no seu sistema. Para instalar a extensão do TrafficLight no seu navegador, clique em **Obter Extensão**.
4. Você será redirecionado para este site:  
<http://bitdefender.com/solutions/trafficlight.html>
5. Selecione **DOWNLOAD GRÁTIS**.





6. Siga estes passos para instalar a extensão do TrafficLight correspondente ao seu navegador.

## Classificação de página e alertas

Dependendo de como o TrafficLight classifica a página que você está visualizando, um dos seguintes ícones é exibido nessa área:



Esta página é segura. Você pode continuar seu trabalho.



Esta página pode ter conteúdo perigoso. Tenha cautela caso decida visitá-la.



Você deve sair desta página imediatamente. Alternativamente, você pode escolher uma das opções disponíveis:

- Sair da página clicando em **Voltar à segurança**.
- Seguir para o site, apesar do alerta, clicando em **Entendo os riscos, continuar mesmo assim**.

## 9.8. ATUALIZAÇÕES

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

Mantenha o **Autopilot** ligado para permitir que as atualizações de assinaturas de malware e do produto sejam baixados automaticamente no seu sistema. Se alguma atualização for detectada, esta será automaticamente baixada e instalada em seu computador.

As atualizações de assinaturas de malware são executadas na hora, ou seja, os arquivos que precisam ser atualizados são substituídos progressivamente. Desta forma, a atualização não afetará o funcionamento do produto e, ao mesmo tempo, exclui qualquer possibilidade de vulnerabilidade.

- Se o Bitdefender Antivirus for Mac estiver atualizado, pode detectar as ameaças mais recentes descobertas e limpar os arquivos infectados.
- Se o Bitdefender Antivirus for Mac não estiver atualizado, não poderá detectar e remover os malware mais recentes descobertos pelos laboratórios da Bitdefender.



## 9.8.1. Solicitando uma Atualização

Você pode solicitar uma atualização manualmente sempre que quiser.

Uma conexão com a internet ativa é necessária para verificar atualizações disponíveis e baixá-las.

Para solicitar uma atualização manualmente:

1. Abra o Bitdefender Antivirus for Mac.
2. Clique no botão **Ações** na barra de menu.
3. Escolha **Atualizar Banco de Dados de Vírus**.

Alternativamente, você pode solicitar uma atualização manualmente ao pressionar CMD + U.

Você pode ver o progresso de atualização e arquivos baixados.

## 9.8.2. Obtendo atualizações via servidor proxy

O Bitdefender Antivirus for Mac só pode ser atualizado por meio de servidores proxy que não requerem autenticação. Você não precisa modificar quaisquer configurações do programa.

Se você se conectar à internet por meio de um servidor proxy que requer autenticação, é necessário mudar para uma conexão direta regularmente para obter atualizações de assinaturas de malware.

## 9.8.3. Atualizar para uma nova versão

Ocasionalmente, lançamos atualizações do produto para adicionar novos recursos e melhorias ou reparar problemas. Essas atualizações podem requerer uma reinicialização do sistema para iniciar a instalação de arquivos novos. Por padrão, se uma atualização requer a reinicialização do sistema, o Bitdefender Antivirus for Mac continuará trabalhando com os arquivos anteriores até você reiniciar o sistema. Neste caso, o processo de atualização não interferirá com o trabalho do usuário.

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




## 10. CONFIGURANDO PREFERÊNCIAS

Este capítulo inclui os seguintes tópicos:

- “*Acessando as preferências*” (p. 237)
- “*Info da conta*” (p. 237)
- “*Preferências de proteção*” (p. 237)
- “*Exclusões de Análise*” (p. 239)
- “*Histórico*” (p. 240)
- “*Quarentena*” (p. 241)

### 10.1. Acessando as preferências

Para abrir a janela de preferências do Bitdefender Antivirus for Mac:

1. Abra o Bitdefender Antivirus for Mac.
2. Faça uma das seguintes:
  - Clique em Bitdefender Antivirus for Mac na barra de menu e escolha **Preferências**.
  - Clique no ícone  na barra de menu e escolha **Preferências**.
  - Pressione Command-Vírgula(,).

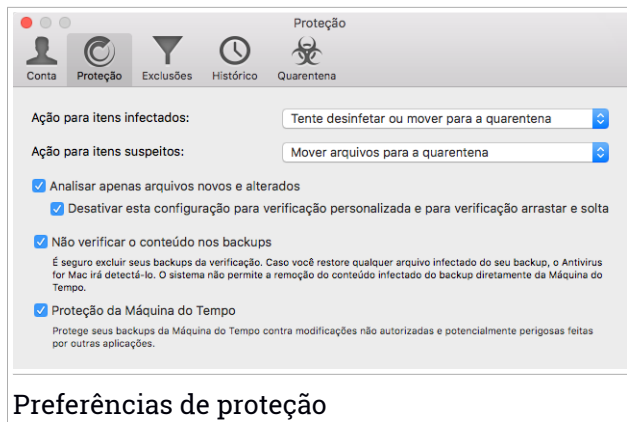
### 10.2. Info da conta

A janela de informações da conta contém detalhes sobre sua assinatura e sua conta Bitdefender.

Sempre que desejar fazer login com outra conta Bitdefender, clique no botão **Trocar de conta**, digite seu novo endereço de e-mail e senha na janela do aplicativo conta Bitdefender, e então clique em **ENTRAR**.

### 10.3. Preferências de proteção

A janela de preferências de proteção lhe permite configurar a abordagem geral da verificação. Você pode configurar as ações para arquivos infectados e suspeitos detectados e outras configurações gerais.



- **Ação para itens infectados.** Quando detecta um vírus ou outro malware, o Bitdefender Antivirus for Mac irá tentar remover automaticamente o código de malware do arquivo e reconstruir o arquivo original. Esta operação é designada por desinfecção. Os arquivos que não podem ser desinfetados são movidos para a **quarentena** para conter a infecção.

Embora não seja recomendado, você pode configurar o aplicativo para não tomar nenhuma ação com arquivos infectados. Arquivos infectados são apenas incluídos no registro.

O Autopilot garante uma boa proteção contra malware com um impacto mínimo no desempenho do sistema. Se há ameaças não resolvidas, você pode vê-las e decidir o que fazer com elas.



- **Ação para itens suspeitos.** Os arquivos são detectados como suspeitos pela análise heurística. Não foi possível desinfetar os arquivos suspeitos por não estar disponível uma rotina de desinfecção.



Por padrão, os arquivos suspeitos são movidos para a quarentena. Quando o vírus está na quarentena não pode prejudicar de nenhuma maneira, porque não pode ser executado ou lido.

Se preferir, pode escolher ignorar arquivos suspeitos. Arquivos infectados são apenas incluídos no registro.

- **Analisar apenas arquivos novos e alterados.** Selecione esta caixa para configurar o Bitdefender Antivirus for Mac para verificar somente arquivos que não foram verificados antes ou que foram modificados desde a última verificação.

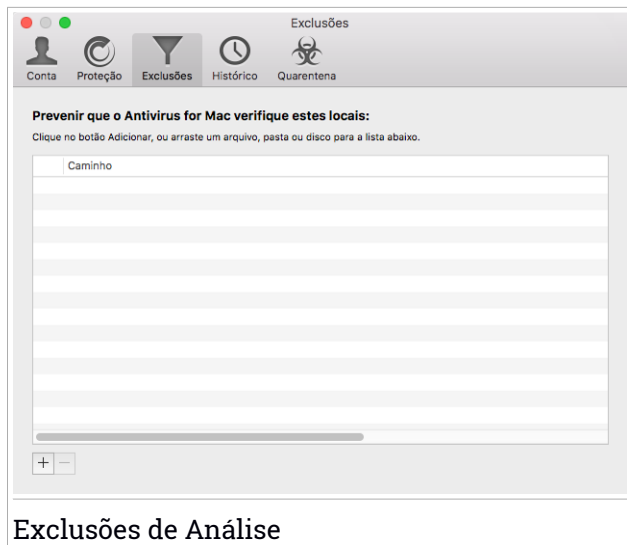
Você pode escolher não aplicar essa configuração para a verificação arrastando e soltando ao selecionar a caixa correspondente.

- **Não verificar o conteúdo nos backups.** Selecione esta caixa para excluir os arquivos de backup da verificação. Se os arquivos infectados forem restaurados em um momento posterior, o Bitdefender Antivirus for Mac os detectará automaticamente e tomará a ação necessária.
- **Proteção da Máquina do Tempo.** Selecione esta caixa de verificação para proteger os arquivos armazenados na Máquina do Tempo. Caso os arquivos do seu drive da Máquina do Tempo sejam encriptados por ransomware, você poderá recuperá-los sem pagar pelo resgate.

## 10.4. Exclusões de Análise

Se quiser, você pode configurar o Bitdefender Antivirus for Mac para não verificar arquivos, pastas ou até mesmo um volume inteiro específicos. Por exemplo, você pode desejar excluir da verificação:

- Arquivos que são erroneamente identificados como infectados (conhecidos como falsos positivos)
- Arquivos que causam erros de verificação
- Volumes de backup



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

Há duas formas de configurar uma exclusão de verificação:

- Arraste e solte um arquivo, pasta ou volume na lista de exclusões.
- Clique no botão com o sinal de mais (+), localizado abaixo da lista de exclusões. Depois, escolha o arquivo, pasta ou volume a ser excluído da verificação.

Para remover uma exclusão de verificação, selecione-a na lista e clique no botão com um sinal de menos (-), localizado na lista de exclusões.

## 10.5. Histórico

O Bitdefender mantém um registro detalhado dos eventos relacionados com a sua atividade no seu computador. Sempre que ocorre algo relevante à segurança do seu sistema ou dados, uma nova mensagem é adicionada ao Histórico do Bitdefender Antivirus for Mac, de forma similar a um novo e-mail que aparece na sua Caixa de Entrada.

Os eventos são uma ferramenta importante na monitoração e gestão da proteção do seu Bitdefender. Por exemplo, você pode facilmente verificar se a atualização foi realizada com sucesso, se foi encontrado malware no



seu computador, se um aplicativo não autorizado tentou acessar seu drive da Máquina do Tempo, etc.

Detalhes sobre a atividade do produto são exibidos.

Data	Ação	Detalhes
23/09/2016, 13:06	Autopilot - LIGAR	
23/09/2016, 13:06	Autopilot - DESLIGAR	
23/09/2016, 13:06	Locais personalizados - ver...	
23/09/2016, 13:06	Locais personalizados - ver...	Infecções encontradas
23/09/2016, 13:06	EICAR-Test-File (not a virus...	nenhuma ação foi definida em Preferências: /
23/09/2016, 13:06	Locais personalizados - ver...	Infecções encontradas
23/09/2016, 13:06	EICAR-Test-File (not a virus...	nenhuma ação foi definida em Preferências: /
23/09/2016, 13:06	EICAR-Test-File (not a virus...	nenhuma ação foi definida em Preferências: /
23/09/2016, 13:05	Locais personalizados - ver...	
23/09/2016, 13:05	VBS.Netlog.D em quarentena	/Users/tester/Desktop/infected/AllQuar/2. Inf

## Histórico

Quando você quiser deletar esse histórico, clique no botão **Limpar Histórico**.

O botão **Copiar** possibilita copiar essas informações na área de transferência.

## 10.6. Quarentena

O Bitdefender Antivirus for Mac permite isolar os arquivos infectados ou suspeitos em uma área segura, chamada quarentena. Quando o vírus está na quarentena não pode prejudicar de nenhuma maneira, porque não pode ser executado ou lido.



Nome da Ameaça	Caminho original
VBS.Netlog.D	/Users/tester/Desktop/infected/AllQuar/2. Infectat Nedezinfectabil.txt
VBS.Netlog.D	/Users/tester/Desktop/infected/AllQuar/10. Infectat Nedezinfectabil.emlx

Restaurar Excluir Número de itens: 2

Status:	Infectados
Dono:	tester
Usuário:	root
Data:	23/09/2016, 13:06

### Arquivos em quarentena

A seção de Quarentena mostra todos os arquivos atualmente isolados na pasta da Quarentena.

Para deletar um arquivo da quarentena, selecione-o e clique em **Deletar**. Se pretende restaurar um arquivo da quarentena para a respectiva localização original, selecione-o e clique em **Restaurar**.





## 11. BITDEFENDER CENTRAL

Este capítulo inclui os seguintes tópicos:

- “*Sobre Bitdefender Central*” (p. 243)
- “*Minhas assinaturas*” (p. 279)
- “*Meus dispositivos*” (p. 277)

### 11.1. Sobre Bitdefender Central

Bitdefender Central é a plataforma virtual onde você tem acesso às funções e serviços online do produto, e pode realizar remotamente tarefas importantes nos dispositivos em que o Bitdefender estiver instalado. Você pode acessar sua conta Bitdefender de qualquer computador ou dispositivo móvel conectado à Internet visitando <https://central.bitdefender.com>. Uma vez que você tenha obtido acesso, você pode realizar as seguintes ações:

- Fazer download e instalar o Bitdefender nos sistemas operacionais Windows, OS X e Android. Os produtos disponíveis para download são:
  - Bitdefender Antivirus for Mac
  - A linha de produtos Windows da Bitdefender
  - Bitdefender Mobile Security
  - Bitdefender Consultor Parental
- Controlar e renovar suas assinaturas do Bitdefender.
- Adicionar novos dispositivos à sua rede e controlar suas funções de onde quer que você esteja.

### 11.2. Acessando a Bitdefender Central

Há várias formas de acessar a Bitdefender Central. Dependendo da tarefa que você quiser realizar, você pode utilizar qualquer uma das seguintes opções:

- Na interface principal do Bitdefender Antivirus for Mac:
  1. Clique no link **Ir para sua conta** na parte inferior direita da tela.
- No seu navegador da Internet:
  1. Abrir um navegador em qualquer dispositivo com acesso à Internet.



2. Acesse: <https://central.bitdefender.com>.
3. Faça login na sua conta usando seu e-mail e senha.

## 11.3. Minhas assinaturas


A plataforma da Bitdefender Central possibilita que você controle facilmente as assinaturas de todos os seus dispositivos.

### 11.3.1. Ativar assinatura

Uma assinatura pode ser ativada durante o processo de instalação utilizando sua conta Bitdefender. Junto com o processo de ativação, a validade da assinatura inicia sua contagem regressiva.

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

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


1. Acesse **Bitdefender Central**.
2. Clique no ícone  localizado no canto superior esquerdo da janela e depois selecione o painel **Minhas Assinaturas**.
3. Clique no botão **CÓDIGO DE ATIVAÇÃO** e então digite o código no campo correspondente.
4. Clique em **ENVIAR**.

A assinatura está ativada agora.

Para começar a instalar o produto nos seus dispositivos, acesse "*Instalar da Bitdefender Central*" (p. 217).

### 11.3.2. Comprar assinatura

Você pode comprar uma assinatura diretamente da sua conta Bitdefender seguindo os seguintes passos:

1. Acesse **Bitdefender Central**.
2. Clique no ícone  localizado no canto superior esquerdo da janela e depois selecione o painel **Minhas Assinaturas**.



3. Clique no link **Comprar Agora**. Você será redirecionado para uma página da web de onde poderá fazer a compra.


Assim que finalizar o processo, a disponibilidade da assinatura está visível no canto inferior direito da interface principal do produto.

## 11.4. Meus dispositivos


A seção **Meus Dispositivos** em sua conta Bitdefender permite que você instale, controle e realize ações remotas em seu Bitdefender em qualquer dispositivo, desde que esteja ligado e conectado à Internet. Os cartões de dispositivos exibem o nome do dispositivo, o estado de sua proteção e tempo disponível da assinatura.

### 11.4.1. Personalize seu dispositivo

Para identificar facilmente seus dispositivos, você pode personalizar o nome de cada dispositivo:


1. Acesse **Bitdefender Central**.
2. Na janela **MEUS DISPOSITIVOS**, clique no ícone  no cartão de dispositivo desejado e então selecione **Configurações**.
3. Mude o nome do dispositivo como desejar, depois selecione **SALVAR**.


Você pode criar e atribuir um proprietário a cada um de seus dispositivos para uma melhor gestão:

1. Acesse **Bitdefender Central**.
2. Na janela **MEUS DISPOSITIVOS**, clique no ícone  no cartão de dispositivo desejado, e então selecione **Perfil**.
3. Clique **Adicionar proprietário** e preencha os campos correspondentes. Defina o Sexo, Data de nascimento e selecione até uma Foto de perfil.
4. Clique em **ADICIONAR** para salvar o perfil.
5. Selecione o proprietário desejado na lista **Proprietário do dispositivo** e clique em **ATRIBUIR**.



## 11.4.2. Ações remotas

Para atualizar o Bitdefender remotamente no seu dispositivo, clique no ícone  no cartão de dispositivo desejado e então selecione **Atualizar**.

Para habilitar o recurso Autopilot remotamente no seu dispositivo, clique no ícone  no cartão de dispositivo desejado e então selecione **Configurações**. Clique no botão correspondente para habilitar o Autopilot.

Quando você clicar no cartão de dispositivo, as abas a seguir aparecerão:

- **PAINEL**. Nesta janela você pode verificar o estado da proteção dos seus produtos Bitdefender e o número de dias restantes em sua assinatura. O estado da proteção pode estar verde, quando não houver problemas afetando seu dispositivo, ou vermelho quando o dispositivo estiver em risco. Quando houver problemas afetando seu produto, clique em **Visualizar incidências** para descobrir mais detalhes.
- **Proteção**. Desta janela você pode executar uma Verificação Rápida ou Completa em seus dispositivos remotamente. Clique no botão **VERIFICAR** para iniciar o processo. Você também pode conferir quando a última verificação foi realizada no dispositivo e acessar um relatório da última verificação, contendo as informações mais importantes. Para mais informações sobre esses dois processos de verificação, acesse "[Verificando seu Mac](#)" (p. 229).



## 12. PERGUNTAS MAIS FREQUENTES

### Como posso experimentar o Bitdefender Antivirus for Mac antes de fazer a assinatura?

Você é um novo cliente Bitdefender e gostaria de experimentar nosso produto antes de comprá-lo. O período de avaliação é de 30 dias e você pode continuar usando o produto instalado somente se comprar uma assinatura Bitdefender. Para avaliar o Bitdefender Antivirus for Mac, você precisa:

1. Criar uma conta Bitdefender seguindo os seguintes passos:

- Acesse: <https://central.bitdefender.com>.
- Digite a informação solicitada nos campos correspondentes, e então clique no botão **CRIAR CONTA**.

Os dados que nos fornecer serão mantidos confidenciais.

2. Faça o download do Bitdefender Antivirus for Mac da seguinte forma:

- Na janela **MEUS DISPOSITIVOS**, clique em **INSTALAR Bitdefender**.
- Escolha uma das duas opções disponíveis:

- **DOWNLOAD**

Clique no botão e salve o arquivo de instalação.

- **Em outro dispositivo**

Selecione **OS X** para fazer download do seu produto Bitdefender e, em seguida, clique em **CONTINUAR**. Digite um endereço de e-mail no campo correspondente e clique em **ENVIAR**.

- Execute o Bitdefender que você baixou.


### Tenho um código de ativação. Como posso adicionar sua validade à minha assinatura?

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

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

1. Acesse [Bitdefender Central](#).



2. Clique no ícone  localizado no canto superior esquerdo da janela e depois selecione o painel **Minhas Assinaturas**.
3. Clique no botão **CÓDIGO DE ATIVAÇÃO** e então digite o código no campo correspondente.
4. Clique novamente no botão **CÓDIGO DE ATIVAÇÃO**.

A extensão agora está visível na sua conta Bitdefender e no seu produto Bitdefender Antivirus for Mac instalado, na parte inferior direita da tela.

## O registro de verificação indica que ainda há itens não resolvidos. Como removê-los?

Os itens não resolvidos no registro de verificação podem ser:

- arquivos de acesso restrito (xar, rar, etc.)

**Solução:** Use a opção **Revelar no Finder** para encontrar o arquivo e deletá-lo manualmente. Não se esqueça de esvaziar a Lixeira.

- caixas de correio restritas (Thunderbird, etc.)

**Solução:** Use o aplicativo para remover a entrada contendo o arquivo infectado.

- Conteúdo nos backups

**Solução:** Habilite a opção **Não verificar o conteúdo nos backups** nas Preferências de Proteção ou selecione **Adicionar às exclusões** para os arquivos detectados.

Se os arquivos infectados forem restaurados em um momento posterior, o Bitdefender Antivirus for Mac os detectará automaticamente e tomará a ação necessária.



### Nota


Arquivos de acesso restrito significam que o Bitdefender Antivirus for Mac só pode abri-los, mas não pode modificá-los.

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

O Bitdefender mantém um log de todas as ações importantes, mudanças de status e outras mensagens críticas relacionadas à sua atividade. Para acessar essas informações, abra a janela de preferências do Bitdefender Antivirus for Mac:

1. Abra o Bitdefender Antivirus for Mac.



2. Faça uma das seguintes:
  - Clique em Bitdefender Antivirus for Mac na barra de menu e escolha **Preferências**.
  - Clique no ícone  na barra de menu e escolha **Preferências**.
  - Pressione Command-Vírgula(,).
3. Escolha a aba **Histórico**.

Detalhes sobre a atividade do produto são exibidos.

## **Posso atualizar o Bitdefender Antivirus for Mac por meio de um servidor proxy?**

O Bitdefender Antivirus for Mac só pode ser atualizado por meio de servidores proxy que não requerem autenticação. Você não precisa modificar quaisquer configurações do programa.

Se você se conectar à internet por meio de um servidor proxy que requer autenticação, é necessário mudar para uma conexão direta regularmente para obter atualizações de assinaturas de malware.

## **Como eu posso remover o Bitdefender Antivirus for Mac?**

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

1. Abra uma janela do **Finder**, vá para a pasta Aplicativos e escolha Utilitários.
2. Dê um clique-duplo no aplicativo Desinstalador Bitdefender.
3. Clique em **Desinstalar** para continuar.
4. Espere o processo ser concluído, depois clique em **Fechar** para finalizar.





### **Importante**

Caso haja um erro, você pode entrar em contato com o Atendimento ao Consumidor da Bitdefender, como descrito em *"Solicite Ajuda"* (p. 287).

## **Como removo as extensões do TrafficLight do meu navegador?**

- Para remover as extensões do TrafficLight do Mozilla Firefox, siga estes passos:
  1. Abra o seu navegador Mozilla Firefox.
  2. Vá em **Ferramentas** e selecione **Add-ons**.



3. Selecione **Extensões** na coluna à esquerda.
  4. Selecione a extensão e clique em **Remover**.
  5. Reinicie o navegador para completar o processo de remoção.
- Para remover as extensões do TrafficLight do Google Chrome, siga estes passos:
    1. Abra o seu navegador Google Chrome.
    2. Clique em  na barra de ferramentas do navegador.
    3. Vá em **Ferramentas** e selecione **Extensões**.
    4. Selecione a extensão e clique em **Remover**.
    5. Clique em **Desinstalar** para confirmar o processo de remoção.
  - Para remover o Bitdefender TrafficLight do Safari, siga estes passos:
    1. Abra o seu navegador Safari.
    2. Clique em  na barra de ferramentas do navegador e clique em **Preferências**.
    3. Selecione a aba **Extensões** e encontre a extensão **Bitdefender TrafficLight no Safari** na lista.
    4. Selecione a extensão e clique em **Desinstalar**.
    5. Clique em **Desinstalar** para confirmar o processo de remoção.





## **MOBILE SECURITY PARA ANDROID**



## 13. RECURSOS DE PROTEÇÃO

O Bitdefender Mobile Security & Antivirus protege seu dispositivo Android com os seguintes recursos:

- Verificador de Malware
- Consultor de Privacidade
- Segurança na Web
- Anti-Roubo, incluindo:
  - Localização Remota
  - Bloqueio remoto do aparelho
  - Apagamento remoto do aparelho
  - Alertas do aparelho remoto
- Bloqueio de Aplicativo
- Relatórios
- WearON

Você pode usar os recursos do produto por 14 dias, sem nenhum custo. Quando o período expirar, você precisará comprar a versão completa para proteger seu dispositivo móvel.



## 14. INTRODUÇÃO


### Requerimentos do Aparelho

O Bitdefender Mobile Security & Antivirus funciona em qualquer dispositivo com Android 4.0 ou superior. É necessária uma conexão ativa à Internet para a varredura de malware nas nuvens.

### Instalando o Bitdefender Mobile Security & Antivirus

#### ● Da Bitdefender Central

##### ● Android

1. Acesse: <https://central.bitdefender.com>.
2. Entre na sua conta Bitdefender.
3. Pressione o ícone  no canto superior esquerdo da tela, e então selecione **Meus dispositivos**.
4. Na janela **MEUS DISPOSITIVOS**, pressione o ícone +.
5. Selecione **Bitdefender Mobile Security** na lista e pressione **IR A GOOGLE PLAY**.
6. Pressione **INSTALAR** na tela do Google Play.

##### ● No Windows, Mac OS X, iOS

1. Acesse: <https://central.bitdefender.com>.
2. Entre na sua conta Bitdefender.
3. Na janela **MEUS DISPOSITIVOS**, pressione **INSTALAR O Bitdefender**.
4. Selecione o link **Em outro dispositivo**.
5. Escolha **Android**.
6. Selecione **Bitdefender Mobile Security** na lista e pressione **CONTINUAR**.
7. Digite um endereço de e-mail no campo correspondente e pressione **ENVIAR**.
8. Acesse sua conta de e-mail no seu dispositivo Android e pressione o botão **OBTENHA NO Google Play**.



Você será redirecionado para o aplicativo do **Google Play**.

9. Pressione **INSTALAR** na tela do Google Play.

## ● Do Google Play

Busque por Bitdefender Mobile Security & Antivirus para localizar e instalar o aplicativo.

Alternativamente, escaneie o código QR:



## Entre na sua conta Bitdefender

Para usar o Bitdefender Mobile Security & Antivirus, você precisa vincular seu dispositivo a uma conta Bitdefender ou conta Google acessando a conta dentro do aplicativo. Na primeira vez que abrir o aplicativo, será pedido que você acesse uma conta.

Se você instalou o Bitdefender Mobile Security & Antivirus desde sua conta Bitdefender, o aplicativo tentará fazer login automaticamente com essa conta.

Para vincular seu dispositivo a uma conta Bitdefender:

1. Abra o Bitdefender Mobile Security & Antivirus.
2. Pressione **USAR CONTA DA CENTRAL** e digite o endereço de e-mail e senha da sua conta Bitdefender.



### Nota

Caso não possua uma conta, selecione o link correspondente. Para entrar utilizando uma conta do Google, pressione a opção **CONTA DO GOOGLE**.

3. Pressione **ENTRAR**.



## Ativação do Bitdefender Mobile Security & Antivirus

Para obter a proteção do Bitdefender Mobile Security & Antivirus, você deve ativar seu produto com uma assinatura, que especificará por quanto tempo você poderá utilizar o produto. Assim que esse período acabar, o aplicativo para de realizar suas funções e proteger seu dispositivo.

Para ativar o Bitdefender Mobile Security & Antivirus:

1. Abra o Bitdefender Mobile Security & Antivirus.
2. O aplicativo exibe informações sobre o status da assinatura atual.  
Pressione **EU POSSUO UM CÓDIGO**.
3. Digite um código de ativação no campo correspondente, depois pressione **ATIVAR**.

Para estender uma assinatura disponível:

1. Abra o Bitdefender Mobile Security & Antivirus.
2. Pressione o botão **Menu** e selecione **Informações da Conta** na lista de opções.
3. Na seção **Estender assinatura**, digite um código de ativação e pressione **ATIVAR**.

Você também pode estender sua assinatura atual acessando as ofertas listadas.

## Painel

Toque no ícone do Bitdefender Mobile Security & Antivirus na gaveta de aplicativos do seu aparelho para abrir a interface do aplicativo.

O Painel de Controle apresenta informações sobre o status de segurança de seu dispositivo e permite o fácil controle de todas as funções de segurança.

Quando houver um processo em andamento ou uma função solicitar uma ação sua, um cartão com mais informações e ações possíveis será exibido no Painel de Controle.

Você pode acessar as funções do Bitdefender Mobile Security & Antivirus e navegar facilmente de uma seção a outra utilizando o botão **Menu** localizado no canto superior esquerdo da tela:



## **Verificador de Malware**

Permite que você inicie uma varredura sob demanda e habilita ou desabilita o Armazenamento da Varredura. Para mais informações, por favor consulte "[Verificador de Malware](#)" (p. 257)

## **Consultor de Privacidade**

Oferece a você informações sobre os aplicativos de Android instalados no seu dispositivo e suas ações em segundo plano. Para mais informações, por favor consulte "[Consultor de Privacidade](#)" (p. 260)

## **Segurança na Web**

Permite que você ative ou desative o recurso de segurança web. Para mais informações, por favor consulte "[Proteção da Internet](#)" (p. 262)

## **Anti-Roubo**

Permite que você ative ou desative as características Anti-Roubo e configure os ajustes Anti-Roubo. Para mais informações, por favor consulte "[Recursos Anti-Roubo](#)" (p. 264)

## **Bloqueio de Aplicativo**

Permite que você proteja seus aplicativos instalados, através da configuração de um código de acesso PIN. Para mais informações, por favor consulte "[Bloqueio de Aplicativo](#)" (p. 270)

## **Relatórios**

Mantém um registro de todas as ações importantes, mudanças de status e outras mensagens críticas relacionadas à atividade do seu dispositivo. Para mais informações, por favor consulte "[Relatórios](#)" (p. 275)

## **WearON**

Comunica-se com seu smartwatch para ajudá-lo a encontrar seu telefone, caso você o tenha perdido ou esqueceu onde o deixou. Para mais informações, por favor consulte "[WearON](#)" (p. 276)



## 15. VERIFICADOR DE MALWARE

Bitdefender protege o seu aparelho e dados contra aplicativos maliciosos usando a verificação na instalação e verificação sob demanda.



### Nota

Assegure-se que o seu dispositivo está conectado à Internet. Se seu dispositivo não estiver conectado à Internet, o processo de varredura não será iniciado.

### ● Verificação na Instalação

Sempre que instalar um aplicativo, o Bitdefender Mobile Security & Antivirus verifica automaticamente se o mesmo utiliza tecnologia nas nuvens. O mesmo processo de verificação se inicia toda vez que aplicativos instalados são atualizados.

Este tipo de varredura é realizada através do recurso Autopiloto. Autopilot é um verificador inteligente que confere todos os aplicativos que você instala ou atualiza, e impede que vírus se alastrem.

Caso o aplicativo seja considerado malicioso, aparecerá um alerta solicitando que você desinstale-o. Pressione **Desinstalar** para acessar a tela de desinstalação do aplicativo.

### ● Verificação solicitada

Sempre que você quiser saber se os aplicativos instalados em seu dispositivo são seguros para utilização, você pode realizar uma verificação.

Para iniciar uma verificação, simplesmente pressione o botão **INICIAR VERIFICAÇÃO** do cartão Verificador de Malware disponível no Painel de Controle.

Você também pode realizar uma verificação seguindo estes passos:

1. Abra o Bitdefender Mobile Security & Antivirus.
2. Pressione o botão **Menu** e selecione **Verificador de Malware** na lista de opções.
3. Pressione **INICIAR ANÁLISE**.



### Nota

Permissões adicionais são necessárias no Android 6 para a função Verificador de Malware. Após pressionar o botão **INICIAR VERIFICAÇÃO**, selecione **Permitir** para as seguintes opções:



- Permitir que o **Antivírus** faça e administre ligações?
- Permitir que o **Antivírus** acesse fotos, mídias e arquivos no seu dispositivo?

O processo de verificação será exibido e você poderá interrompê-lo a qualquer momento.



## Verificação de Malware

O Bitdefender Mobile Security & Antivirus já vem configurado para verificar o armazenamento interno de seu dispositivo, incluindo qualquer cartão SD conectado. Desta forma, quaisquer aplicativos perigosos que possam estar no cartão podem ser detectados antes que possam causar danos.

Para habilitar ou desabilitar a Verificação de Memória:


1. Abra o Bitdefender Mobile Security & Antivirus.





2. Pressione o botão **Menu** e selecione **Verificador de Malware** na lista de opções.

3. Toque no botão correspondente.

Você também pode habilitar ou desabilitar a verificação de memória na área de **Configurações** pressionando o botão , depois o botão correspondente.

Caso sejam detectados quaisquer aplicativos maliciosos, serão exibidas informações sobre eles e você poderá removê-los tocando o botão **DESINSTALAR**.

O cartão do Verificador de Malware exibe o estado de seu dispositivo. Quando ele está seguro, o cartão fica verde. Quando o dispositivo necessitar de verificação ou de alguma ação sua, o cartão ficará vermelho.




## 16. CONSULTOR DE PRIVACIDADE

O Consultor de Privacidade confia nas informações verificadas da Nuvem para oferecer constantemente informações atualizadas sobre seus aplicativos de Android.

A maioria dos aplicativos é legítima, mas também há aplicativos que podem rastrear sua localização, acessar e compartilhar suas informações pessoais. O Consultor de Privacidade fornece os fatos, mas finalmente é você quem decide se um aplicativo é seguro para uso ou não.

Use o Consultor de Privacidade para descobrir mais informações sobre aplicativos que:

- acessam ou fazem upload de seus contatos para sua própria nuvem
- podem descobrir sua verdadeira identidade
- podem ser negligentes, enviando suas senhas pela Internet e colocando suas contas em risco
- podem fazer uso e upload da ID exclusiva do seu Dispositivo para analisar o que você faz
- coletam dados de relatórios e análises estatísticos para monitorá-lo
- rastreiam sua localização
- exibem anúncios
- podem custar-lhe dinheiro

Pressione o ícone de filtro  para ver uma lista das dicas mais importantes.

As informações a seguir estão disponíveis nessa lista:

- quais aplicativos são vírus
- quais aplicativos enviam sua identidade a estranhos
- quais aplicativos contêm anúncios muito invasivos
- quais aplicativos enviam seus dados particulares para estranhos
- quais aplicativos podem custar-lhe dinheiro
- quais aplicativos enviam dados não criptografados
- quais aplicativos rastreiam sua localização



- quais aplicativos têm acesso à informação sigilosa

## Grau de Privacidade

Calculando o Grau de Privacidade para cada usuário, o Consultor de Privacidade fornece uma visão precisa e personalizada de quão vulnerável você é, para que você possa avaliar e tomar as medidas apropriadas para cada aplicativo instalado. Você deve ter cuidado quando seu grau de privacidade estiver baixo.

Se você tenha dúvidas sobre as permissões necessárias para um determinado aplicativo, tente obter mais informações sobre o mesmo antes de decidir se deve ou não continuar usando tal aplicativo.



## 17. SEGURANÇA NA WEB

A Segurança na Web usa os serviços em nuvem do Bitdefender para verificar as páginas da web que você acessa com o navegador padrão do Android, Google Chrome, Firefox, Opera, Opera Mini, Dolphin, e navegadores internos de aplicativos, como Facebook ou Facebook Messenger. Uma lista completa com os navegadores suportados está disponível na seção Segurança na Web.

Caso uma URL aponte para um website conhecido por phishing ou fraude, ou para conteúdo malicioso como spyware ou vírus, a página web fica temporariamente bloqueada e um alerta é exibido.

Você poderá então optar por ignorar o alerta e prosseguir à página web ou retornar a uma página segura.



### Nota

Permissões adicionais são necessárias no Android 6 para a função Segurança na Web.

Habilite a permissão para registrar como serviço de Acessibilidade e pressione **LIGAR** quando solicitado. Toque em **Antivírus** e ative o botão, depois confirme que você concorda com o acesso às permissões do seu dispositivo.





## 18. RECURSOS ANTI-ROUBO

Bitdefender pode ajudá-lo a localizar seu dispositivo e impedir que seus dados pessoais caiam em mãos erradas.

Tudo o que você precisa fazer é ativar o Antifurto no dispositivo e, quando necessário, acessar a **Bitdefender Central** de qualquer navegador da web, em qualquer lugar.

Mesmo que você não possa acessar a Internet, você ainda pode proteger seu dispositivo e seus dados enviando **comandos via SMS** de qualquer telefone celular para o seu smartphone através de mensagens de texto normais.

Bitdefender Mobile Security & Antivirus oferece os seguintes recursos Anti-Roubo:

### Localização Remota

Visualize a localização atual do seu aparelho no Google Maps. A localização é atualizada a cada 5 segundos, para que você possa rastreá-lo se estivesse em movimento.

A precisão da localização depende de como o Bitdefender é capaz de determiná-la:

- Caso o GPS esteja ativado no aparelho, sua localização pode ser determinada dentro de dois metros, desde que esteja ao alcance dos satélites GPS (ou seja, fora de um edifício).
- Se o aparelho estiver dentro de casa, sua localização pode ser determinada em dezenas de metros caso o Wi-Fi esteja ativado e existam redes sem fio disponíveis no alcance.
- Caso contrário, a localização será determinada utilizando somente informações a partir da rede móvel, que pode oferecer uma precisão não melhor que várias centenas de metros.

### Mostrar IP

Exibe o último endereço de IP para o dispositivo selecionado. Pressione **MOSTRAR IP** para torná-lo visível.

### Apagamento Remoto

Remova todos os dados pessoais de seu aparelho roubado.



## Bloqueio Remoto

Bloqueia a tela do seu aparelho e define uma senha para desbloquear o mesmo.

## Enviar alerta ao aparelho (Scream)

Envie uma mensagem remotamente para ser exibida na tela do aparelho ou emitir um som alto no alto-falante do aparelho.

Caso você venha a perder seu aparelho, você pode informar a quem achou como o aparelho pode ser devolvido, exibindo uma mensagem na tela do aparelho.

Caso tenha perdido seu aparelho e exista a possibilidade dele não estar longe de você (por exemplo, em algum lugar em casa ou no escritório), que melhor maneira de encontrá-lo do que fazê-lo tocar um som alto? O som será reproduzido mesmo se o aparelho estiver no modo silencioso.

## Ativando Anti-Roubo

Para ativar a função Antifurto, basta completar o processo de configuração do cartão Antifurto disponível no Painel de Controle.

Você também pode ativar a função Antifurto seguindo estas instruções:

1. Abra o Bitdefender Mobile Security & Antivirus.
2. Pressione o botão **Menu** e selecione **Antifurto** na lista de opções.
3. Pressione **ATIVAR**.
4. O seguinte procedimento será iniciado para ajudá-lo na ativação desta função:



### Nota

Permissões adicionais são necessárias no Android 6 para a função Anti-Roubo. Para ativá-lo, siga os seguintes passos:

- Pressione **Ativar Antifurto**, então pressione **LIGAR**.
- Habilite as permissões nas seguintes opções:
  - a. Permitir que o **Antivírus** envie e visualize mensagens SMS?
  - b. Permitir que o **Antivírus** acesse a localização deste dispositivo?
  - c. Permitir que o **Antivírus** acesse seus contatos?

### a. Conceder privilégios de administrador



Esses privilégios são essenciais à operação da função Antifurto, e devem ser concedidas antes de continuar.

## b. Definir senha numérica para o aplicativo

Para garantir que quaisquer mudanças feitas nas configurações da função Antifurto passem por sua autorização, um código PIN deve ser definido. Sempre que for feita uma tentativa de modificar as configurações Anti-Roubo, o PIN deverá ser inserido antes que as mudanças sejam aplicadas. De forma alternativa, em dispositivos que suportam autenticação por leitura de digital, uma confirmação por digital pode ser usada em vez do código PIN configurado.



### Nota

O mesmo código PIN é usado pelo Bloqueio de Aplicativo para proteger seus aplicativos instalados.

## c. Ativar a função Tirar Foto

Sempre que alguém tentar acessar seus aplicativos instalados enquanto a opção Tirar Foto estiver ligada, o Bitdefender tirará uma foto da pessoa. Para mais detalhes sobre esta função, por favor acesse **"Tirar foto"** (p. 272).

## d. Configurar número de confiança para o Antifurto

Selecione a aba **CONTROLE DE SMS**, digite um número telefônico de confiança ou selecione um da lista de contatos, e depois pressione **SALVAR NÚMERO**. O número confiável deve conter um código de país e pode ser o número de alguém que você conhece ou o número de outro telefone que você usa.

Quando um cartão SIM diferente for inserido em seu dispositivo, o Bitdefender Mobile Security & Antivirus automaticamente enviará uma mensagem de texto ao número confiável com o novo número de telefone.

Dessa forma, você pode enviar comandos ao seu telefone por SMS mesmo que o SIM seja trocado e seu número mude.



### Importante

Esta não é uma etapa obrigatória, mas é recomendável que você defina um número de confiança durante a instalação inicial. O comando





Limpeza funciona apenas quando enviado de um número de confiança pré-definido.

Uma vez que o Anti-Roubo é ativado, você pode ativar ou desativar os recursos de controle Web ou controle via SMS individualmente na tela Anti-Roubo pressionando os ícones correspondentes.



## Usando os recursos Anti-Roubo de Bitdefender Central (Controle Web)



### Nota

Todas as funções de Antifurto necessitam que a opção **Dados em segundo plano** esteja ativa nas configurações de Dados do seu dispositivo.

Para acessar as funções do Antifurto na sua conta Bitdefender:

1. Acesse **Bitdefender Central**.
2. Pressione o ícone  no canto superior esquerdo da tela, e então selecione **Meus dispositivos**.
3. Na janela **MEUS DISPOSITIVOS**, selecione o cartão de dispositivo desejado.
4. Selecione a aba **Antifurto**.
5. No último campo da janela, pressione o ícone  e depois o botão com a função correspondente que deseja usar:

**Localizar** - exibe a localização do seu dispositivo no Google Maps.



**Alerta** - digite uma mensagem para ser exibida na tela do seu dispositivo e/ou para fazer com que seu dispositivo emita um alarme sonoro.



**Bloquear** - bloquear seu dispositivo e definir um PIN para desbloqueá-lo.



**Limpar** - apagar todos os dados do seu dispositivo.



### Importante

Após apagar um dispositivo, todos os recursos Anti-Roubo deixam de funcionar.



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

## Usando os recursos Anti-Roubo através de comandos via SMS (Controle via SMS)

Uma vez que os comandos por SMS são ativados, você pode enviar os seguintes comandos de seu smartphone via SMS de qualquer outro telefone celular:

- **LOCATE** - enviar uma mensagem contendo a localização do dispositivo ao número de telefone do qual o comando foi enviado. A mensagem contém um link do Google Maps que pode ser aberto no navegador do telefone celular.
- **SCREAM** - tocar um som alto no alto-falante do dispositivo.
- **LOCK** - bloqueie a tela do dispositivo com o código PIN que você definiu.
- **WIPE** - apagar todos os dados do seu dispositivo.



### Importante

O comando Limpeza funciona apenas quando enviado de um número de confiança pré-definido.

- **CALLME** - discar o número de telefone do qual o comando foi enviado com o alto-falante ativado. Assim, você poderá escutar silenciosamente a pessoa que estiver com seu telefone.
- **HELP** - enviar uma mensagem contendo todos os comandos disponíveis ao número de telefone do qual o comando foi enviado.
- **SIM Change** - o número de confiança que você configurou receberá um SMS com o novo número de telefone assim que seu SIM for substituído por um novo. Para configurar o número de telefone do seu amigo, pressione a opção **Número de confiança**. Digite o número dele incluindo o código do país, ou escolha seu cartão da lista de contatos.

Todos os comandos por SMS devem ser enviados usando o seguinte formato:

**bd-<PIN> <command>**



### Nota

Os símbolos indicam variáveis e não devem aparecer no comando.



Por exemplo, se você definiu o PIN de segurança como 123456 e deseja receber uma mensagem com a localização do seu telefone, mande a seguinte mensagem de texto para seu número de telefone:

**BD-123456 LOCATE**



## 19. BLOQUEIO DE APLICATIVO

Aplicativos instalados, como e-mails, fotos ou mensagens, podem conter dados pessoais que você gostaria que permanecessem privados, limitando o acesso a eles de forma seletiva.

O App Lock ajuda você a bloquear o acesso indesejado aos aplicativos, através da configuração de um código de acesso PIN de segurança. O código PIN deve ter no mínimo 4 dígitos e no máximo 8, e será solicitado todas as vezes que você desejar acessar os aplicativos restritos.

De forma alternativa, em dispositivos que suportam autenticação por leitura de digital, uma confirmação por digital pode ser usada em vez do código PIN configurado.

### Ativando o Bloqueio de Aplicativo

Para restringir acesso a aplicativos específicos, configure o Bloqueio de Aplicativo pelo cartão exibido no Painel de Controle após a ativação da função Antifurto.

Você também pode ativar o Bloqueio de Aplicativo seguindo estas instruções:

1. Abra o Bitdefender Mobile Security & Antivirus.
2. Pressione o botão **Menu** e selecione **Bloqueio de Aplicativo** na lista de opções.
3. Pressione **ATIVAR** e permita o acesso aos dados de uso para o Bitdefender selecionando a caixa correspondente.



#### Nota

Permissões adicionais são necessárias no Android 6 para a função Tirar Foto.

Para habilitá-la, permita que o **Antivírus** tire fotos e grave vídeos.

4. Volte para o aplicativo, configure o código de acesso e pressione **DEFINIR PIN**.



#### Nota

Esta etapa somente será necessária se você não tiver configurado o PIN na função Antifurto.



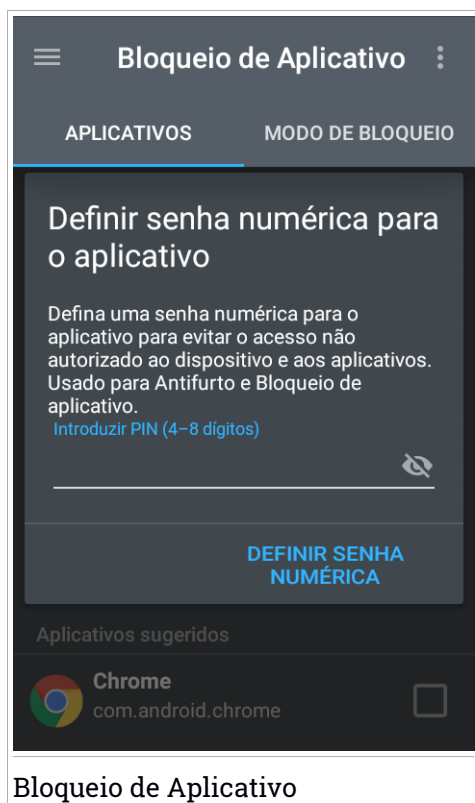
5. Permite que a opção Tirar Foto pegue qualquer intruso que tente acessar seus dados pessoais.
6. Selecione os aplicativos que você gostaria de proteger.

Usar o PIN ou digital errada cinco vezes seguidas ativará uma pausa de 30 segundos. Dessa forma, qualquer tentativa de acessar os aplicativos protegidos será bloqueada.



## Nota

O mesmo código PIN é usado pelo Antifurto para ajudá-lo a localizar seu dispositivo.






## Modo de bloqueio

Daqui você pode escolher quando a função Bloqueio de Aplicativo deve proteger os aplicativos instalados no seu dispositivo.

Você pode escolher uma das seguintes opções:

- **Bloquear sempre** - o código PIN ou digital que você configurou deverá ser usado sempre que você tentar acessar os aplicativos bloqueados.
- **Desbloquear até a tela apagar** - o acesso aos seus aplicativos será válido até a tela apagar.
- **Permitir uma saída rápida** - você pode sair e acessar novamente seus aplicativos desbloqueados dentro de 30 segundos.
- **Ativar desbloqueio inteligente** - quando ativado e conectado a uma rede definida como confiável, as outras configurações ficam indisponíveis. Isso significa que nenhuma confirmação por PIN ou digital é necessária quando aplicativos bloqueados são acessados.

## Ajustes do Bloqueio de Aplicativo

Pressione o botão  no menu de recursos do Bloqueio de Aplicativo, e então selecione **Configurações** para uma configuração mais avançada do seu Bloqueio de Aplicativo.

Em **Configurações** do Bloqueio de Aplicativo você pode fazer o seguinte:

- Ativar o Snap Photo quando três tentativas erradas de desbloqueio forem realizadas.
- Bloquear notificações para aplicativos recentemente instalados.
- Mudar seu código PIN.

## Tirar foto

Com o Snap Photo da Bitdefender você pode pegar seus amigos ou parentes em flagrante. Assim você pode educá-los a não bisbilhotar seus arquivos pessoais ou os aplicativos que você usa.

A função funciona facilmente: uma foto é tirada com a câmera frontal sempre que a confirmação por código PIN ou digital que você definiu para proteger seus aplicativos for inserida incorretamente três vezes seguidas. A foto será




salva com informação sobre o dia, hora e motivo, e poderá ser visualizada quando você abrir o Bitdefender Mobile Security & Antivirus e acessar o recurso Bloqueio de Aplicativo.



## Nota


Este recurso somente está disponível para telefones que têm uma câmera frontal.

Para configurar o recurso Snap Photo:

1. Abra o Bitdefender Mobile Security & Antivirus.
2. Pressione o botão **Menu** e selecione **Bloqueio de Aplicativo** na lista de opções.
3. Pressione o botão  no menu do recurso Bloqueio de Aplicativo, e então selecione **Configurações**.
4. Habilite o botão de **Tirar foto quando 3 tentativas erradas de desbloqueio forem realizadas**.

As fotos tiradas quando o PIN incorreto é inserido são exibidas no menu de Bloqueio de Aplicativo e podem ser visualizadas em tela cheia.

De forma alternativa, eles podem ser vistos na sua conta Bitdefender:

1. Acesse: <https://central.bitdefender.com>.
2. Acesse sua conta.
3. Pressione o ícone  no canto superior esquerdo da tela, e então selecione **Meus dispositivos**.
4. Selecione o seu dispositivo na janela **MEUS DISPOSITIVOS** e depois a aba **Antifurto**.

As fotos são exibidas.

Apenas as 3 fotos mais recentes são salvas.

## Desbloqueio Inteligente

Um método fácil para que a função Bloqueio de Aplicativo pare de pedir uma confirmação por PIN ou digital sempre que você acessa os aplicativos protegidos é a ativação do Desbloqueio Inteligente.




Com o Desbloqueio Inteligente, você pode definir as redes Wi-Fi de confiança às quais você normalmente conecta de forma que as configurações do Bloqueio de Aplicativo sejam desabilitadas quando você estiver conectado a elas.

Para ativar a função Desbloqueio Inteligente:

1. Abra o Bitdefender Mobile Security & Antivirus.
2. Pressione o botão **Menu** e selecione **Bloqueio de Aplicativo** na lista de opções.
3. Selecione a aba **MODO DE BLOQUEIO** e ative o botão correspondente.

A rede sem fio que você está conectado é exibida.

Para definir a conexão WiFi que você está usando como confiável, pressione o ícone .



## Nota

Esta configuração somente estará disponível se o recurso Desbloqueio Inteligente estiver habilitado.

Quando você mudar de opinião, desabilite o recurso, e as redes WiFi que você configurou como confiáveis serão tratadas como não-confiáveis.





## 20. RELATÓRIOS

O recurso Relatórios mantém um registro detalhado de eventos relacionados à atividade de análise do seu dispositivo.

Sempre que acontecer algo relevante à segurança do seu dispositivo, uma nova mensagem será adicionada a Relatórios.

Para acessar a seção Relatórios:


1. Abra o Bitdefender Mobile Security & Antivirus.
2. Pressione o botão **Menu** e selecione **Relatórios** na lista de opções.

As seguintes abas estão disponíveis na janela Relatórios:

- **RELATÓRIOS SEMANAIS** - aqui você tem acesso ao status de segurança e às tarefas executadas da semana atual e anterior. O relatório semanal é gerado todo domingo e você receberá uma notificação informando sobre sua disponibilidade.

Toda semana uma nova dica será exibida nesta seção, então lembre-se de conferir regularmente para obter o máximo que seu aplicativo pode oferecer.

- **REGISTRO DE ATIVIDADES** - aqui você poderá acessar informações detalhadas sobre as atividades do seu aplicativo Bitdefender Mobile Security & Antivirus desde quando foi instalado no seu dispositivo Android.

Para apagar o registro de atividade disponível, pressione o botão  no canto superior direito da tela e depois selecione **Limpar registro de atividades**.



## 21. WEARON

Com WearON do Bitdefender, você pode encontrar facilmente seu smartphone, esteja ele na sala de reunião do escritório ou sob uma almofada no sofá. O dispositivo pode ser encontrado mesmo se o modo silencioso estiver ativado.

Mantenha esse recurso ativado para garantir que você sempre terá seu smartphone por perto.



### Nota

O recurso funciona com Android 4.3 e Android Wear.

## Ativando o WearON

Para usar o WearON, você só precisa conectar seu smartwatch ao aplicativo do Bitdefender Mobile Security & Antivirus e ativar o recurso com o seguinte comando de voz:

**Start:**<Where is my phone>

O **Bitdefender WearON** tem dois comandos:

### 1. Alerta de Telefone

Com o recurso Alerta de Telefone você encontra rapidamente seu smartphone, sempre que se afastar muito dele.

Se estiver com seu smartwatch, ele detecta automaticamente o aplicativo no seu telefone e vibra sempre que você ficar menos de dez metros de distância do seu aparelho.

Para habilitar esse recurso, abra o Bitdefender Mobile Security & Antivirus, toque em **Configurações Globais** no menu e selecione o botão correspondente na seção WearON.

### 2. Grito

Encontrar seu telefone nunca foi tão fácil. Quando esquecer onde deixou seu telefone, toque no comando Grito no seu relógio para fazer seu telefone tocar.



## 22. BITDEFENDER CENTRAL

Bitdefender Central é a plataforma virtual onde você tem acesso às funções e serviços online do produto, e pode realizar remotamente tarefas importantes nos dispositivos em que o Bitdefender estiver instalado. Você pode acessar sua conta Bitdefender de qualquer computador ou dispositivo móvel conectado à Internet visitando <https://central.bitdefender.com>. Uma vez que você tenha obtido acesso, você pode realizar as seguintes ações:

- Fazer download e instalar o Bitdefender nos sistemas operacionais Windows, OS X e Android. Os produtos disponíveis para download são:
  - Bitdefender Mobile Security & Antivirus
  - O Antivírus Bitdefender para Mac
  - A linha de produtos Windows da Bitdefender
- Controlar e renovar suas assinaturas do Bitdefender.
- Adicionar novos dispositivos à sua rede e controlar suas funções de onde quer que você esteja.

### Acessar sua conta Bitdefender

Para acessar sua conta Bitdefender, basta:

1. Abrir um navegador em qualquer dispositivo com acesso à Internet.
2. Acesse: <https://central.bitdefender.com>.
3. Entre na sua conta usando seu endereço de e-mail e senha.



### Meus dispositivos

A seção **MEUS DISPOSITIVOS** em sua conta Bitdefender permite que você instale, controle e realize ações remotas em seu Bitdefender em qualquer dispositivo, desde que esteja ligado e conectado à Internet. Os cartões de dispositivos exibem o nome do dispositivo, o estado de sua proteção e tempo disponível da assinatura.



Para identificar facilmente seus dispositivos, você pode personalizar o nome de cada dispositivo:

1. Acesse **Bitdefender Central**.



2. Pressione o ícone  no canto superior esquerdo da tela, e então selecione **Meus dispositivos**.
3. Na janela **MEUS DISPOSITIVOS**, pressione o ícone  no cartão de dispositivo desejado e selecione **Configurações**.
4. Altere o nome do dispositivo no campo correspondente, e então selecione **Salvar**.

Você pode criar e atribuir um proprietário a cada um de seus dispositivos para uma melhor gestão:

1. Acesse **Bitdefender Central**.
2. Pressione o ícone  no canto superior esquerdo da tela, e então selecione **Meus dispositivos**.
3. Na janela **MEUS DISPOSITIVOS**, pressione o ícone  no cartão de dispositivo desejado e selecione **Perfil**.
4. Pressione **Adicionar proprietário** e preencha os campos correspondentes. Defina o sexo, data de nascimento e você pode até selecionar uma foto de perfil.
5. Pressione **ADICIONAR** para salvar o perfil.
6. Selecione o proprietário desejado na lista **Proprietário do dispositivo** e pressione **ATRIBUIR**.

Para mais ações remotas e informações sobre seu produto Bitdefender em um dispositivo específico, selecione o cartão de dispositivo desejado.

Quando você selecionar o cartão de dispositivo, as abas a seguir aparecerão:

- **PAINEL**. Nesta janela você pode verificar o estado da proteção dos seus produtos Bitdefender e o número de dias restantes em sua assinatura. O estado da proteção pode estar verde, quando não houver problemas afetando seu dispositivo, ou vermelho quando o dispositivo estiver em risco. Quando houver problemas afetando seu produto, pressione **Visualizar incidências** para descobrir mais detalhes. Daqui você poderá resolver manualmente os problemas que afetam a segurança de seus dispositivos.
- **Proteção**. Desta janela você pode executar uma Verificação remota em seu dispositivo. Pressione no botão **VERIFICAR** para iniciar o processo. Você também pode conferir quando a última verificação foi realizada no



dispositivo e acessar um relatório da última verificação, contendo as informações mais importantes.


- **Anti-theft.** Caso tenha perdido seu dispositivo, você pode localizá-lo e realizar ações remotas com a função Antifurto. Toque em **LOCALIZAR** para descobrir a localização de seu dispositivo. A última localização conhecida será exibida, com a hora e a data. Para mais detalhes sobre esta função, por favor acesse "*Recursos Anti-Roubo*" (p. 264).

## Minhas assinaturas

A plataforma da Bitdefender Central possibilita que você controle facilmente as assinaturas de todos os seus dispositivos.

## Verificar assinaturas disponíveis

Para verificar suas assinaturas disponíveis:

1. Acesse **Bitdefender Central**.
2. Pressione o ícone  no canto superior esquerdo da tela, e então selecione **Minhas Assinaturas**.

Aqui você pode acessar informações sobre a disponibilidade das assinaturas que você possui e o número de dispositivos utilizando cada uma delas.


Você pode adicionar um novo dispositivo a uma assinatura ou renová-la selecionando um cartão de assinatura.

## Adicionar novo dispositivo

Caso sua assinatura cubra mais de um dispositivo, você pode adicionar um novo dispositivo e instalar seu Bitdefender Mobile Security & Antivirus nele, como descrito em "*Instalando o Bitdefender Mobile Security & Antivirus*" (p. 253).

## Renove assinatura

Se lhe restam menos de 30 dias de assinatura e você desabilitou a renovação automática, é possível renová-la manualmente seguindo os seguintes passos:

1. Acesse **Bitdefender Central**.
2. Pressione o ícone  no canto superior esquerdo da tela, e então selecione **Minhas Assinaturas**.



3. Selecione o cartão de assinatura desejado.

4. Pressione **RENOVAR** para continuar.

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



## 23. PERGUNTAS MAIS FREQUENTES

### **Por que o Bitdefender Mobile Security & Antivirus requer conexão de Internet?**

O aplicativo precisa se comunicar com os servidores do Bitdefender para determinar o status de segurança dos aplicativos que ele analisa e das páginas web que você está visitando, e também para receber comandos da sua conta Bitdefender quando usar o recurso Antifurto.

### **Para que o Bitdefender Mobile Security & Antivirus precisa de cada permissão?**

- Acesso à Internet -> utilizado para comunicação nas nuvens.
- Analisar status do telefone e identidade -> utilizado para detectar se o aparelho está conectado à Internet e para extrair determinadas informações do dispositivo necessárias para criar uma ID exclusiva ao comunicar-se com Bitdefender nuvem.
- Ler e escrever marcadores do navegador -> o módulo Web Security apaga sites maliciosos do seu histórico de navegação.
- Ler o registro de dados -> o Bitdefender Mobile Security & Antivirus detecta traços de atividade de malware dos registros Android.
- Leitura/escrita de SMS, contatos, dados da conta e de armazenamento externo -> Necessário para o recurso de apagamento remoto.
- Localização -> Necessária para localização remota.
- Câmera -> necessária para tirar foto.
- Armazenamento -> usado para permitir que o Verificador de Malware verifique o cartão SD.



### **Onde posso encontrar os detalhes sobre a atividade do aplicativo?**

O Bitdefender Mobile Security & Antivirus mantém um log de todas as ações importantes, mudanças de status e outras mensagens críticas relacionadas à sua atividade. Para acessar essa informação, abra o Bitdefender Mobile Security & Antivirus e pressione o botão do **Menu**, e então selecione **Relatórios** na lista de opções.

### **Esqueci o código PIN que defini para proteger meu aplicativo. What do I do?**

1. Acesse [Bitdefender Central](#).



2. Pressione o ícone  no canto superior esquerdo da tela, e então selecione **Meus dispositivos**.
3. Na janela **MEUS DISPOSITIVOS**, selecione o ícone  no cartão de dispositivo desejado e depois selecione **Configurações**.
4. Recupere o PIN no campo **PIN de Aplicativo**.

## **Como o Bitdefender Mobile Security & Antivirus irá influenciar no desempenho do meu dispositivo e na autonomia da minha bateria?**



O impacto é muito baixo. O aplicativo somente roda quando é essencial – inclusive durante a instalação e quando você navega pela interface do aplicativo - ou quando deseja realizar uma verificação de segurança. O Bitdefender Mobile Security & Antivirus não roda em plano de fundo quando você liga para amigos, envia mensagens ou joga.

## **Como posso desligar a função Bloqueio de Aplicativo?**

Não há uma opção para desligar a função Bloqueio de Aplicativo, mas você pode desativá-la facilmente ao desmarcar as caixas próximas aos aplicativos selecionados depois que validar o PIN ou digital que definiu.

## **Como posso definir outra rede sem fio como confiável?**

Se deseja definir outra rede sem fio como confiável:

1. Abra o Bitdefender Mobile Security & Antivirus.
2. Pressione o botão **Menu** e selecione **Bloqueio de Aplicativo** na lista de opções.
3. Selecione a aba **MODO DE BLOQUEIO** e selecione o ícone .
4. Valide o PIN ou digital para confirmar sua escolha.
5. Clique no ícone  ao lado da rede que você deseja definir como confiável.

## **O que o Consultor de Privacidade me diz sobre os aplicativos que eu instalo?**

O Consultor de Privacidade lhe diz o que cada aplicativo é capaz de fazer em seu dispositivo. A mesma diz se um aplicativo pode acessar seus dados privados, enviar mensagens, conectar à internet ou realizar qualquer outra função que possa representar riscos à sua segurança.

## **Posso remover um aplicativo que eu considero uma ameaça para a minha privacidade?**





Você pode remover manualmente um aplicativo usando o Consultor de Privacidade. Para isso, toque no aplicativo desejado, então pressione o botão **DESINSTALAR APLICATIVO**. Confirme sua escolha e aguarde a conclusão do processo de desinstalação.

## Como eu desativo as notificações do Consultor de Privacidade?

Se deseja parar de receber notificações do Consultor de Privacidade:

1. Abra o Bitdefender Mobile Security & Antivirus.
2. Pressione o botão do **Menu** e selecione **Configurações** na lista de opções.
3. Na seção **Consultor de Privacidade**, pressione a chave correspondente.

## Em que idiomas o Bitdefender Mobile Security & Antivirus está disponível?

O Bitdefender Mobile Security & Antivirus está disponível atualmente nos seguintes idiomas:

- Brasileiro
- Holandês
- Inglês
- Francês
- Alemão
- Grego
- Italiano
- Japonês
- Coreano
- Polonês
- Português
- Romeno
- Russo
- Espanhol
- Tailandês
- Turco
- Vietnamita

Outros idiomas serão adicionados em versões futuras. Para alterar o idioma da interface do Bitdefender Mobile Security & Antivirus, acesse as configurações do seu aparelho **Idioma & teclado** e defina o idioma que deseja usar no aparelho.

## Posso modificar a conta Bitdefender associada ao meu aparelho?



Sim, você pode alterar facilmente a conta Bitdefender vinculada ao seu dispositivo seguindo esses passos:

1. Abra o Bitdefender Mobile Security & Antivirus.
2. Pressione o botão **Menu** e selecione **Informações da Conta** na lista de opções.
3. Pressione **SAIR** e confirme sua escolha.
4. Pressione **USAR CONTA DA CENTRAL** e digite o endereço de e-mail e senha da sua nova conta Bitdefender.

## O que é o Administrador de Aparelho?

O Administrador de Aparelhos é um recurso para Android que concede ao Bitdefender Mobile Security & Antivirus as permissões necessárias para a realização de certas tarefas de forma remota. Sem esses privilégios, o bloqueio remoto não funcionaria e o apagamento do aparelho não seria capaz de remover seus dados completamente. Se deseja remover o aplicativo, certifique-se de revogar esses privilégios antes de tentar desinstalar em **Configurações > Segurança > Selecionar administradores do dispositivo**.

## Para que serve o número de confiança?

Se o seu telefone chegar às mãos de uma pessoa sem a intenção de devolvê-lo ao seu legítimo proprietário, é provável que o SIM card seja trocado rapidamente. Sempre que o Bitdefender Mobile Security & Antivirus detectar que o SIM card no seu telefone foi alterado, ele mandará automaticamente uma mensagem de texto contendo o novo número de telefone para o número que você definiu. Dessa forma, você pode enviar comandos ao seu telefone por SMS mesmo que o SIM seja trocado e seu número mude. Pode ser o número de alguém que você conhece e confia ou o número de outro telefone que você usa.

## O número de confiança pode ser alterado depois de definido?

Para definir um número confiável diferente:

1. Abra o Bitdefender Mobile Security & Antivirus.
2. Pressione o botão do **Menu** e selecione **Configurações** na lista de opções.
3. Na seção **Antifurto**, pressione **Número confiável**.

O PIN será solicitado para que você possa alterar o número confiável.

## Quanto custará para enviar comandos por SMS?



Comandos por SMS são enviados como mensagens de texto normais e, portanto, são cobrados como tais por sua operadora. O Bitdefender não cobra nenhuma taxa adicional.

## **Como solucionar o erro "Nenhum Token Google" que aparece ao fazer login no Bitdefender Mobile Security & Antivirus.**

Esse erro ocorre quando o dispositivo não está associado com alguma conta Google, ou o mesmo está associado, porém um problema temporário está prevenindo ele de conectar ao Google. Tente uma das seguintes soluções:

- Vá para as Configurações > do Android; Aplicativos > Gerenciar Aplicativos > Bitdefender Mobile Security & Antivirus e aperte **Limpar data**. Tente fazer o log in novamente.
- Certifique-se que seu dispositivo está associado com uma conta Google.  
Para checar isso, vá para Configurações > Conta & sincronize e veja se a conta Google está listada sob **Manage Accounts**. Adicione sua conta se a mesma não estiver listada, reinicie seu dispositivo e então tente log in no Bitdefender Mobile Security & Antivirus.
- Reinicie seu dispositivo e depois tente entrar novamente.



**CONTATE-NOS**



## 24. SOLICITE AJUDA

A Bitdefender fornece aos seus clientes um nível de suporte rápido e eficaz. Se encontrar algum problema ou se tiver alguma questão sobre o nosso produto Bitdefender, pode utilizar vários recursos em linha para encontrar uma solução ou resposta. Ou, se preferir você poderá contatar a equipe de Suporte ao Cliente Bitdefender. Os nossos técnicos de suporte responderão imediatamente às suas questões e proporcionarão a ajuda que precisar.

A seção *"Resolvendo incidências comuns"* (p. 183) fornece as informações necessárias em relação às incidências mais frequentes que poderá encontrar ao utilizar este produto.

Caso não encontre uma resposta para a sua pergunta no material fornecido, acesse <https://www.bitdefender.com/support/contact-us.html> e entre em contato com nossos representantes de suporte.

Você também pode conferir nosso *"Recursos online"* (p. 288) para mais sugestões ou informações sobre todos os produtos Bitdefender.



## 25. RECURSOS ONLINE

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

- Centro de Suporte Bitdefender:

<https://www.bitdefender.com/support/consumer.html>

- Fórum de Suporte Bitdefender:

<https://forum.bitdefender.com>

- o portal de segurança informática HOTforSecurity:

<https://www.hotforsecurity.com>

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

### 25.1. Centro de Suporte Bitdefender

O Centro de Suporte do Bitdefender é um repositório de informação online sobre os produtos Bitdefender. Armazena, num formato facilmente acessível, relatórios sobre os resultados do suporte técnico em curso e atividades de correção de falhas do suporte e equipas de desenvolvimento do Bitdefender, além de artigos mais gerais sobre prevenção de vírus, gestão de soluções do Bitdefender com explicações detalhadas e muitos outros artigos.

O Centro de Suporte da Bitdefender está aberto ao público e é acessado com frequência. A informação extensiva que ele contém é mais um meio de proporcionar aos clientes do Bitdefender as informações técnicas e o conhecimento de que necessitam. Todos os pedidos de informação válidos ou relatórios de falhas oriundos de clientes do Bitdefender são eventualmente direcionados para o Centro de Apoio do Bitdefender, como relatórios de correção de falhas, fichas de resolução de problemas ou artigos informativos como suplemento dos arquivos de ajuda.

O Centro de Suporte da Bitdefender encontra-se disponível a qualquer hora

<https://www.bitdefender.com/support/consumer.html>.

### 25.2. Fórum de Suporte Bitdefender

O Fórum de Suporte do Bitdefender proporciona aos utilizadores do Bitdefender uma forma fácil de obter ajuda e ajudar os outros.



Se o seu produto Bitdefender não estiver a funcionar correctamente, se não conseguir remover certos vírus do seu computador ou se tiver alguma questão sobre a forma como opera, coloque o seu problema ou a sua questão no fórum.

Os técnicos de suporte Bitdefender supervisionam o fórum à espera de novas mensagens para fornecer ajuda. Você também pode receber uma resposta ou solução de um usuário mais experiente do Bitdefender.

Antes de publicar o seu problema ou questão, por favor pesquise o fórum por um tópico semelhante ou relacionado.

O Fórum de Suporte do Bitdefender está disponível em <https://forum.bitdefender.com>, em 5 idiomas diferentes: inglês, alemão, francês, espanhol e romeno. Clique na hiperligação **Protecção Casa & Casa/Escritório** para acessar à secção dedicada aos produtos de consumidor.

## 25.3. Portal HOTforSecurity

HOTforSecurity é uma fonte rica de informações sobre segurança de computadores. Aqui você pode conhecer as várias ameaças as quais seu computador fica exposto quando conectado à Internet (malware, phishing, spam, cibercriminosos).

Os novos artigos são publicados regularmente para o manter atualizado sobre as últimas ameaças descobertas, as actuais tendências de segurança e outras informações sobre a indústria de segurança informática.

A página web do HOTforSecurity é <https://www.hotforsecurity.com>.



## 26. INFORMAÇÃO SOBRE CONTATO

A comunicação eficiente é a chave para um negócio de sucesso. Nos últimos 16 anos a BITDEFENDER estabeleceu uma reputação indiscutível, excedendo as expectativas dos clientes e parceiros, sempre buscando uma melhor comunicação. Por favor, não hesite em nos contactar sobre quaisquer assuntos ou dúvidas que você possa ter.

### 26.1. Endereços da Rede

Departamento de Vendas: [sales@bitdefender.com](mailto:sales@bitdefender.com)

Centro de Suporte: <https://www.bitdefender.com/support/consumer.html>

Documentação: [documentation@bitdefender.com](mailto:documentation@bitdefender.com)

Distribuidores locais: <https://www.bitdefender.com/partners>

Programa de parcerias: [partners@bitdefender.com](mailto:partners@bitdefender.com)

Relações com a mídia: [pr@bitdefender.com](mailto:pr@bitdefender.com)

Carreiras: [jobs@bitdefender.com](mailto:jobs@bitdefender.com)

Apresentação de Vírus: [virus\\_submission@bitdefender.com](mailto:virus_submission@bitdefender.com)

Envio de spam: [spam\\_submission@bitdefender.com](mailto:spam_submission@bitdefender.com)

Relato de abuso: [abuse@bitdefender.com](mailto:abuse@bitdefender.com)

Site Web: <https://www.bitdefender.com>

### 26.2. Distribuidores locais

Os distribuidores locais Bitdefender estão preparados para responder a quaisquer dúvidas relacionadas com as suas áreas de operação, quer sejam comerciais ou assuntos gerais.

Para encontrar um distribuidor Bitdefender no seu país:

1. Vá para <https://www.bitdefender.com/partners/partner-locator.html>.
2. Escolha seu país e cidade utilizando as opções correspondentes.
3. Caso não encontre um distribuidor Bitdefender no seu país, não hesite em contactar-nos pelo e-mail [sales@bitdefender.com](mailto:sales@bitdefender.com). Por favor, escreva a sua mensagem em inglês para podermos responder imediatamente.

### 26.3. Escritórios Bitdefender

Os escritórios Bitdefender estão preparados para responder a quaisquer dúvidas relacionadas com as suas áreas de operação, quer sejam comerciais ou assuntos gerais. Seus endereços respectivos estão listados abaixo.





## E.U.A

### **Bitdefender, LLC**

6301 NW 5th Way, Suite 4300

Fort Lauderdale, Florida 33309

Telefone (escritório&vendas): 1-954-776-6262

Vendas: [sales@bitdefender.com](mailto:sales@bitdefender.com)

Suporte Técnico: <https://www.bitdefender.com/support/consumer.html>

Página da Web <https://www.bitdefender.com>

## Alemanha

### **Bitdefender GmbH**

TechnoPark Schwerte

Lohbachstrasse 12

D - 58239 Schwerte

Escritório: +49 2304 9 45 - 162

Fax: +49 2304 9 45 - 169

Vendas: [vertrieb@bitdefender.de](mailto:vertrieb@bitdefender.de)

Suporte Técnico: <https://www.bitdefender.de/support/consumer.html>

Página da Web <https://www.bitdefender.de>

## Espanha

### **Bitdefender España, S.L.U.**

C/Bailén, 7, 3-D

08010 Barcelona

Fax: +34 93 217 91 28

Fone: +34 902 19 07 65

Vendas: [comercial@bitdefender.es](mailto:comercial@bitdefender.es)

Suporte Técnico: <https://www.bitdefender.es/support/consumer.html>

Website: <https://www.bitdefender.es>

## Romênia

### **BITDEFENDER SRL**

Complex DV24, Building A, 24 Delea Veche Street, Sector 2

Bucharest

Fax: +40 21 2641799

Telefone de Vendas: +40 21 2063470

E-mail de vendas: [sales@bitdefender.ro](mailto:sales@bitdefender.ro)



Suporte Técnico: <https://www.bitdefender.ro/support/consumer.html>  
Website: <https://www.bitdefender.ro>

## Emirados Arabes

### **Dubai Internet City**

Building 17, Office # 160

Dubai, UAE

Telefone de Vendas: 00971-4-4588935 / 00971-4-4589186

E-mail de vendas: [mena-sales@bitdefender.com](mailto:mena-sales@bitdefender.com)

Suporte Técnico: <https://www.bitdefender.com/support/consumer.html>

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



## Glossário

### **ActiveX**

ActiveX é um modelo para escrever programas para que outros programas e o sistema operacional possam buscá-los. A tecnologia ActiveX é usada com o Microsoft Internet Explorer para fazer páginas da Web interativas que se parecem e se comportam como programas de computador, melhor que páginas estáticas. Com o ActiveX, usuários podem perguntar ou responder questões, apertar botões e interagir de outras formas com a página. Controles ActiveX são também escritos usando Visual Basic.

O ActiveX é notável para uma completa falta de controles de segurança; especialistas em segurança de computador desencorajam seu uso pela Internet.

### **Adware**

O Adware é sempre combinado com um programa host sem custo enquanto o usuário concordar em aceitar o adware. Não existem implicações neste tipo de instalação, pois o usuário concordou com o propósito do aplicativo.

No entanto, propagandas do tipo “pop-up” podem se tornar uma inconveniência, e em alguns casos afetar a performance do seu sistema. Além disso, a informação que alguns destes programas coleta pode causar problemas de privacidade a usuários que não estão totalmente cientes do funcionamento do programa.

### **Ameaça persistente avançada**

A ameaça persistente avançada (APA) explora as vulnerabilidades dos sistemas para roubar informações importantes e fornecê-las à fonte. Grandes grupos como organizações, empresas ou governos são os alvos deste malware.

O objetivo de uma ameaça persistente avançada é permanecer não detectada por um longo período, sendo capaz de monitorar e coletar informações importantes sem danificar as máquinas atacadas. O método usado para injetar o vírus na rede é através de um arquivo PDF ou documento do Office que pareça inofensivo, de forma que todo usuário possa abrir esses arquivos.



## **Área de Notificação**

Introduzido com o Windows 95, a bandeja 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 acessar aos detalhes e controles.

## **Arquivo**

Um disco, fita ou diretório que contém arquivos que podem ter sido gravados como backup.

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

## **Arquivo de relatório**

Um arquivo que lista as ações que ocorreram. Por exemplo Bitdefender mantém um arquivo de relatório com uma lista dos caminhos verificados, as pastas, o número de arquivos e arquivos comprimidos verificados, quantos arquivos infectados e suspeitos foram encontrados.

## **Assinatura**

Acordo de compra que dá ao usuário o direito de usar um produto ou serviço específico em um número específico de dispositivos e por um período de tempo determinado. Uma assinatura expirada pode ser automaticamente renovada usando a informação fornecida pelo usuário na primeira compra.

## **Assinatura de vírus**

É um padrão binário de vírus, utilizado pelo programa antivírus para detectar e eliminar os vírus.

## **Atualizar**

Uma nova versão do programa ou driver do produto projetado para substituir uma versão antiga do mesmo produto. Além disso, as rotinas de instalação verificam se uma versão mais antiga está instalada no seu computador; caso contrário, você não poderá instalar a atualização.

O Bitdefender possui um módulo de atualização que permita a você verificar manualmente por atualizações ou deixa que ele automaticamente atualize o produto.



## **Backdoor**

Um furo na segurança do sistema deixado deliberadamente pelos desenvolvedores ou mantenedores. A motivação para tais furos não pe sempre sinistra, alguns sistemas operacionais, por exemplo, saem com contas privilegiadas para uso em campo para serviço dos técnicos ou programa de manutenção dos programadores do fabricante.

## **Caminho**

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

A rota entre dois pontos quaisquer, com os canais de comunicação entre dois computadores.

## **Cliente de e-mail**

É um aplicativo que lhe permite enviar e receber e-mails.

## **Código de ativação**

É um código exclusivo que pode ser comprado no varejo e usado 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 determinados dispositivos e também pode ser usado para estender uma assinatura com a condição de ser gerada para o mesmo produto ou serviço.

## **Cookie**

Dentro da indústria da Internet, os cookies são descritos como pequenos arquivos de texto que contém informações sobre computadores individuais que podem sendo analisados e usados pelos anunciantes para rastrear gostos e interesses on-line. Nesse contexto, a tecnologia de cookies ainda está em desenvolvimento e a intenção é direcionar os anúncios diretamente aos seus interesses. É uma faca de dois gumes para muitos, porque por um lado é eficiente e pertinente porque só veja anúncios que interessam. E por outro lado, envolve “rastrear” e “seguir” a onde você vai e onde está clicando. Consequentemente, existe um debate sobre a privacidade e muitas pessoas se sentem ofendidas pelo fato de serem vistas como um número SKU (você sabe, o código de barras na parte traseira das embalagens que são lidas no caixa do supermercado). Embora esse ponto de vista possa ser extremo, em alguns casos é preciso.



## **Download**

Copiar dados (geralmente um arquivo inteiro) de uma fonte principal para um periférico. O termo é muitas vezes usado para descrever o processo de copiar um arquivo de um serviço on-line para seu próprio computador. Download também pode se referir a copiar um arquivo de um servidor de rede para um computador na rede.

## **E-mail**

Correio eletrônico. Um serviço que envia mensagens para computadores em redes locais ou mundiais.

## **Eventos**

Uma ação ou ocorrência detectada por um programa. Eventos podem ser ações de usuários, tais como clicar com botão do mouse ou pressionar uma tecla, ou ocorrências do sistema, como falta de memória.

## **Extensão do arquivo**

É a parte do arquivo, após o ponto final, indica o tipo de dados que estão armazenados no arquivo.

Muitos sistemas operacionais usam extensões de arquivos, ex. Unix, VMS, MS-DOS. Eles são usualmente de uma a três letras e / ou números (alguns sistemas operacionais antigos não suportam mais que três). Exemplos: "c" para códigos em C, "ps" para PostScript, "txt" para texto.

## **Falso positivo**

Ocorre quando a verificação identifica um arquivo infectado quando de fato não está.

## **Heurística**

Um método baseado em regras para identificar novos vírus. Esse método de verificação não se baseia em definições de vírus específicas. A vantagem da verificação heurística é que ela não é enganada por uma nova variante do vírus. Entretanto ela pode relatar um código suspeito em um programa normal, gerando assim um chamado "falso positivo".

## **IP**

Um protocolo roteável no conjunto do protocolo TCP/IP que é responsável pelo endereçamento IP, roteamento, e fragmentação e montagem dos pacotes IP.



## **Itens para inicializar**

Qualquer arquivo colocado nessa pasta será executado quando o computador iniciar. Por exemplo, uma tela de boas-vindas, um arquivo de som, um aviso de calendário ou um aplicativo pode ser um item de inicialização. Normalmente um pseudônimo deste arquivo é colocado nesta pasta, em vez do arquivo em si.

## **Java applet**

Um programa em Java que é projetado para ser executado somente em uma página web. Para usar um aplicativo em uma página web, você deve especificar o nome do aplicativo e o tamanho (comprimento e largura em pixels) que o aplicativo pode utilizar. Quando a página da web é acessada, o navegador descarrega-a de um servidor e executa na máquina do usuário (o cliente). Os aplicativos diferem dos programas em que eles são comandados por um protocolo estrito de segurança.

Por exemplo, mesmo que um aplicativo funcione em um cliente, eles não podem ler ou escrever dados na máquina do cliente. Adicionalmente, os aplicativos são mais restringidos de modo que só podem ler e escrever dados nos domínios aos quais servem.

## **Keylogger**

Um keylogger é um aplicativo que registra tudo o que é digitado.

Os keyloggers não são por natureza maliciosos. Podem ser usados com objetivos legítimos, tais como monitorar a atividade de funcionários ou crianças. No entanto, são cada vez mais usados por cibercriminosos com objetivos maliciosos (por exemplo, para recolher dados privados, tais como credenciais de acesso e CPF).

## **Linha de comando**

Na interface de linha de comando, os usuários digitam os comando em um espaço fornecido diretamente na tela usando comandos da linguagem.

## **Memória**

Áreas internas de armazenamento do computador. O termo memória identifica o armazenamento de dados que vem em forma de chips e a armazenagem de palavra é utilizada para memória que existe em fitas ou discos. Todo computador vem com uma certa quantidade de memória física, geralmente referida com memória RAM.



## **Não heurística**

Esse método de verificação confia em definições de vírus específicas. A vantagem da verificação não heurística é que ela não pode ser enganada por algo que pode parecer um vírus, e não gera falsos alarmes.

## **Navegador**

Termo simplificado para navegador da web, um programa utilizado para localizar e exibir páginas da Internet. Navegadores populares incluem o Microsoft Internet Explorer, Mozilla Firefox e Google Chrome. Estes são navegadores gráficos, o que significa que podem exibir tanto gráficos como texto. Em adição, os navegadores mais modernos podem apresentar informações multimídia, como som e vídeo, através de plug-ins para alguns formatos.

## **Phishing**

O ato de enviar e-mail a um usuário declarando falsamente ser uma empresa legítima em uma tentativa de enganar o usuário a entregar informações que serão usadas para roubo de identidade. O e-mail direciona o usuário a uma página web onde é solicitado a fornecer informações pessoais, tais como senhas, cartão de crédito, cadastros e contas em bancos, que a empresa legítima em questão já possui. A página web, no entanto, é falsa e existe apenas para roubar informação do usuário.

## **Photon**

Photon é uma tecnologia inovadora não-intrusiva da Bitdefender, projetado para minimizar o impacto da proteção antivírus no desempenho. Ao monitorar a atividade do seu PC em segundo plano, ele cria padrões de uso que ajudam a otimizar processos de inicialização e análise.

## **Porta**

Uma interface no computador na qual você pode conectar um dispositivo. Computadores pessoais possuem vários tipos de portas. Internamente, existem vários tipos de portas conectando unidades de disco, monitores e teclados. Externamente, os computadores pessoais possuem portas conectando modems, impressoras, mouse e outros dispositivos periféricos.





Em redes TCP/IP e UDP, um ponto final a uma conexão lógica. A número da porta identifica que tipo de porta é. Por exemplo, porta 80 é usada para tráfego HTTP.

## **Pote de mel**

Um sistema de computador chamariz estabelecido para atrair hackers, destinado a estudar a forma como agem e identificar os métodos que usam para coletar informações do sistema. As empresas e corporações estão mais interessadas em implementar e usar potes de mel para melhorar seu estado geral de segurança.

## **Programas comprimidos**

Um arquivo em formato compactado. Muitos sistemas operacionais e programas contêm comandos que permitem a você compactar um arquivo para ocupar menos memória. Por exemplo: suponha que você tenha um texto que contém dez caracteres de espaço consecutivos. Normalmente, isso requereria dez bytes de armazenamento.

Entretanto, um programa que compacta arquivos substituiria os caracteres de espaço por um caractere especial série-espaço seguido do número de espaços que estão sendo substituídos. Neste caso, os dez espaços exigiriam apenas dois bytes. Esta é apenas uma técnica de compactação - existem muitas mais.

## **Ransomware**

Ransomware é um programa malicioso que tenta lucrar com usuários através do travamento de seus sistemas vulneráveis. CryptoLocker, CryptoWall e TeslaWall são apenas algumas variantes que perseguem sistemas pessoais de usuários.

A infecção pode ser espalhada acessando um e-mail indesejado, baixando anexos de e-mail ou instalando aplicativos, sem que o usuário saiba o que está acontecendo em seu sistema. Usuários frequentes e empresas são alvos de hackers de ransomware.

## **Rootkit**

Um rootkit é um pacote de ferramentas de software que proporcionam um nível de acesso de administrador a um sistema. O termo foi usado em primeiro lugar nos sistemas operativos UNIX e referia-se a ferramentas recompiladas que proporcionavam aos intrusos direitos de



administração, permitindo-lhes ocultar a sua presença de forma a não serem vistos pelos administradores do sistema.

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

Os rootkits não são maliciosos por natureza. Por exemplo, os sistemas e mesmo algumas aplicações ocultam arquivos críticos usando rootkits. No entanto, eles são essencialmente utilizados para ocultar malware ou para esconder a presença de um intruso no sistema. Quando combinados com o malware, os rootkits são uma grande ameaça à integridade e segurança de um sistema. Eles podem monitorar tráfego, criar backdoors no sistema, alterar arquivos e relatórios e evitam ser detectados.

## **Script**

Outro termo para um arquivo de macro ou arquivo de comandos, um script é uma lista de comandos que podem ser executados sem a interação do usuário.

## **Setor de Boot**

O setor de boot é um setor no começo de cada disco que identifica a arquitetura do disco (tamanho do setor, tamanho do cluster, e assim por diante). Para inicializar os discos, o setor de boot também contém um programa que carrega o sistema operacional.

## **Spam**

Lixo eletrônico em forma de mensagens. Normalmente conhecido como e-mail não solicitado.

## **Spyware**

Qualquer software que coleta informações do usuário através da conexão de Internet sem o seu consentimento, normalmente para propósitos de propaganda. Aplicativos spyware são tipicamente distribuídos de forma oculta juntamente com programas freeware ou shareware que podem ser baixados da Internet; no entanto, deve ser notado que a maioria dos programas shareware e freeware não apresentam spyware. Uma vez instalado, o spyware monitora a atividade do usuário na Internet e transmite essa informação de forma oculta para outra pessoa. O spyware



pode coletar também endereços de e-mail e até mesmo número de cartões de crédito e senhas.

A similaridade do spyware com o cavalo de tróia é que o usuário instala algo que não deseja instalando algum outro produto. Um modo comum de se tornar uma vítima de spyware é baixar alguns programas de compartilhamento de arquivos (peer-to-peer) que estão disponíveis hoje em dia.

Deixando de lado as questões de ética e privacidade, o spyware prejudica o usuário consumindo memória do computador e conexão com a Internet quando manda a informação de volta a sua base usando a conexão de Internet do usuário. Porque o spyware usa a memória e os recursos do sistema, os aplicativos sendo executados podem levar o sistema ao colapso ou instabilidade geral.

## **TCP/IP**

Transmission Control Protocol/Internet Protocol - Um conjunto de protocolos de uma rede de trabalho amplamente utilizado na Internet que permite comunicações em redes de computadores interconectadas com várias arquiteturas de hardware e diversos sistemas operacionais. O TCP/IP inclui padrões de como os computadores se comunicam e convenções para conectar redes e direcionar o tráfego.

## **Trojan**

Um programa destrutivo que oculta um aplicativo benigna. Diferente dos vírus, os trojans não se replicam, mas podem ser tão destrutivos quanto eles. Um dos tipos mais traiçoeiros de vírus do tipo Cavalo de Troia é um programa que promete remover vírus do seu computador, mas em vez disso, introduz vírus nele.

O termo vem da história de Ilíada de Homero, na qual os gregos deram um cavalo de madeira gigante seus inimigos, os Troianos como uma oferta de paz. Mas depois dos troianos arrastarem o cavalo para dentro dos muros da cidade, os soldados Gregos saíram furtivamente da barriga do cavalo e abriram os portões da cidade, permitindo que seus compatriotas derrubassem e capturassem Tróia.

## **Unidade de disco**

É uma máquina que lê e escreve dados em um disco.

Uma unidade de disco rígido lê e escreve em um disco rígido.



Uma unidade de disquete acessa disquetes.

Os discos rígidos podem ser internos (armazenado dentro do computador) ou externos (armazenado em uma caixa separada que está conectada ao computador).

## **Virtual Private Network (VPN)**

É uma tecnologia que ativa uma conexão direta temporária e criptografada para uma certa rede sobre uma rede menos segura. Dessa forma, enviar e receber dados é seguro e criptografado, difícil de virar alvo de espões. Uma prova de segurança é a autenticação, que pode ser feita somente com o uso de um nome de usuário e senha.

## **Vírus**

Um programa ou uma parte do código que é carregado no seu computador sem o seu conhecimento e é executado contra a sua vontade. A maioria dos vírus pode também se duplicar. Todos os vírus de computador são feitos pelo homem. É fácil criar um simples vírus que pode se reproduzir repetidamente. Mesmo um simples vírus é perigoso, porque pode rapidamente usar toda memória disponível e fazer o sistema parar. O tipo de vírus mais perigoso é aquele que é capaz de transmitir-se através de uma rede ou contornando sistemas de segurança.

## **Vírus de boot**

Um vírus que infecta o setor de boot do disco rígido ou de um disquete. Uma tentativa de inicialização com um disquete infectado com vírus de boot fará com que o vírus se torne ativo na memória. Toda vez que você reiniciar seu sistema daquele ponto em diante, você terá um vírus ativo na memória.

## **Vírus de macro**

Um tipo de vírus de computador que é codificado como uma macro dentro de um documento. Muitos aplicativos, como Microsoft Word e Excel, suportam poderosas linguagens de macro.

Essas aplicações permitem a você colocar uma macro em um documento, e mandam a macro ser executada cada vez que o documento é aberto.

**Vírus polimórfico**

Um vírus que muda sua forma cada vez que um arquivo é infectado. Como não têm nenhum padrão binário consistente, tais vírus são duros de identificar.

**Worm**

Um programa que se propaga pela rede, se reproduzindo enquanto avança. Ele não pode se anexar a outros programas.