Bitdefender®
SMALL OFFICE SECURITY

GUIA DO USUÁRIO

Mac iOS

Bitdefender Small Office Security
Guia do Usuário

Data de Publicação 12/18/2019

Aviso Legal

Bitdefender

Índice

Apresentação do Bitdefender Small Office Security

A assinatura do Bitdefender Small Office Security está orientada para pequenos negócios que possuam entre 5 e 20 dispositivos Windows, macOS, Android e iOS e busquem melhorar a segurança, prevenir a perda de dados e impedir que ataques de hackers e malware explorem as vulnerabilidades de sua rede.

A gestão de todos os dispositivos conectados pode ser feita usando a plataforma da Bitdefender Central desde que o administrador esteja logado com as credenciais usadas para ativar a assinatura adquirida. Para acessar a Bitdefender Central no Windows e macOS, vá a https://central.bitdefender.com, e no iOS e Android instale o aplicativo especificado, que pode ser baixado na loja de aplicativos associada a cada plataforma.

Para impedir que usuários façam mudanças nos recursos e configurações que podem afetar a segurança da rede, o administrador pode definir uma senha na conta do Bitdefender. Esta opção está disponível para o produto Bitdefender Total Security, que pode ser instalado em dispositivos com Windows.

A área de Atividade na Bitdefender Central oferece uma vista geral dos dispositivos conectados e seus status de proteção. Caso sejam identificadas ameaças, o administrador pode realizar uma verificação ao mesmo tempo em todos os dispositivos afetados.

Caso você já tenha uma conta Bitdefender com uma assinatura ativa para outro produto ou pacote, para ativar a assinatura do Bitdefender Small Office Security você ainda precisará criar uma nova conta usando outro endereço de e-mail. Uma assinatura pode ser ativada durante o processo de instalação de um dos produtos incluídos no pacote, ou na Bitdefender Central conforme descrito em "*Ativar assinatura*" (p. 32). A partir do processo de ativação, a validade da sua assinatura começa a contar.

Este guia foi elaborado para os quatro produtos incluídos no Bitdefender Small Office Security:

- "Total Security para PC" (p. 1)

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

- "Antivirus para Mac" (p. 193)

  Aprenda a usar o produto nos seus Macs.

- “Mobile Security para iOS” (p. 238)

  Aprenda a usar o produto nos seus smartphones e tablets iOS.
- “Mobile Security para Android” (p. 257)

  Aprenda a usar o produto nos seus smartphones e tablets Android.
- “Contate-nos” (p. 299)

  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, 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.

1.2.1. Requisitos mínimos do sistema

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

1.2.2. Requisitos de sistema recomendados

- 2,5 GB de espaço disponível em disco rígido (pelo menos 800 MB no drive do sistema)
- Intel CORE Duo (2 GHz) ou processador equivalente
- 2 GB de memória (RAM)

1.2.3. Requisitos de Software

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

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

- Google Chrome 34 e superior
- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 e 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**, e clique em **INSTALAR PROTEÇÃO**.
3. Escolha uma das duas opções disponíveis:
   - **Proteja este dispositivo**
     a. Selecione essa opção, e a seguir, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique no botão correspondente.
     b. Guarde o arquivo de instalação.
   - **Proteja outros dispositivos**
     a. Selecione essa opção, e a seguir, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique no botão correspondente.
     b. Pressione **ENVIAR LINK DE DOWNLOAD**.
     c. Digite um endereço de email no campo correspondente e clique em **ENVIAR EMAIL**.

Observe que o link de download gerado será válido apenas durante as próximas 24 horas. Se o link expirar, você precisará gerar um novo seguindo os mesmos passos.

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

4. 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 uma solução de segurança incompatível ou uma versão antiga do Bitdefender, você 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 das soluções de segurança detectadas.

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

Antes de completar o processo de instalação, você deve concordar com o Acordo de Assinatura. Por favor, leia o cordo de Assinatura com calma, já que ele contém os termos e condições segundo 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.

Duas tarefas adicionais podem ser realizadas neste passo.

- Mantenha a opção **Enviar relatórios de produto** 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.

Clique no botão **INSTALAR** para iniciar o processo de instalação do seu Bitdefender.

Passo 2 - Instalação em progresso

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

As áreas críticas do seu sistema são analisadas em busca de ameaças, as últimas versões dos arquivos do aplicativo são baixadas e instaladas, e os serviços do Bitdefender são iniciados. Este passo pode demorar alguns minutos. Clique em **PULAR VERIFICAÇÃO** se deseja verificar seu sistema depois. Para mais informações sobre executar uma verificação do sistema, acesse "*Executando uma Análise do Sistema*" (p. 74).

Passo 3 - Instalação concluída

Seu produto Bitdefender foi instalado com sucesso.

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

Passo 4 - 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

Depois que você instala o Bitdefender Total Security, seu computador fica protegido contra todos os tipos de ameaças (como malware, spyware, ransomware, exploits, botnets e cavalos de troia) e ameaças da internet (como hackers, phishing e spam).

O aplicativo usa a tecnologia Photon para melhorar a velocidade e o desempenho do processo de análise da ameaça. 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.

Conectar-se a redes sem fio públicas de aeroportos, shoppings, cafés ou hotéis sem proteção pode ser perigoso para o seu dispositivo e seus dados. Principalmente porque fraudadores podem estar assistindo suas atividades e encontrar o melhor momento para roubar seus dados pessoais, e também porque todos podem ver seu endereço IP, tornando sua máquina uma vítima de ciberataques futuros. Para evitar tais situações inoportunas, instale e use o aplicativo "*VPN*" (p. 137).

Você pode manter um registro das suas senhas e contas online ao armazená-las em uma "*Proteção do Gerenciador de Senhas para suas credenciais*" (p. 128) carteira. Com uma única senha-mestre você pode proteger sua privacidade de invasores que podem tentar deixá-lo sem dinheiro.

"*Proteção da Webcam*" (p. 114)previne que aplicativos não confiáveis acessem sua câmera, evitando qualquer tentativa de ser hackeada. Com base na escolha dos usuários do Bitdefender, o acesso de aplicativos populares à sua webcam será permitido ou bloqueado.

Para protegê-lo de potenciais bisbilhoteiros e espiões quando seu dispositivo estiver conectado a uma rede sem fio insegura, o Bitdefender analisa seu nível de proteção e, quando necessário, faz recomendações para reforçar a segurança das suas atividades online. Para instruções sobre como manter seus dados pessoais seguros, acesse o "*Consultor de Segurança Wi-Fi*" (p. 110).

Seus arquivos pessoais, fotos ou filmes armazenados localmente e na nuvem, agora podem ficar longe da ameaça mais perigosa da atualidade: o ransomware. Para informações sobre como proteger arquivos pessoais, acesse "*Safe Files*" (p. 118).

Agora arquivos criptografados por ransomware podem ser recuperados sem que você precise gastar dinheiro para qualquer resgate exigido. Para informações sobre como recuperar tais arquivos criptografados, veja "*Remediação de ransomware*" (p. 121).

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. 154).

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, acesse "*Notificações*" (p. 9).

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, acesse "*Bitdefender Central*" (p. 26).

A seção "*Como*" (p. 40) 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. 162) seção de possíveis soluções para os problemas mais comuns.

2.1.1. 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**.
  3. Clique em **Bitdefender Total Security** ou, mais rápido, clique duas vezes no ícone do Bitdefender na barra de sistema.
- No **Windows 8 e Windows 8.1**:

Localize o Bitdefender 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 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 na área de notificação.

Para mais informações sobre a janela e ícone do Bitdefender na bandeja do sistema, consulte *"Interface Bitdefender"* (p. 13).

2.1.2. 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 alguma ameaça ou vulnerabilidade fori encontrada no seu computador, etc. Adicionalmente, pode tomar outras ações se necessário ou alterar ações tomadas pelo Bitdefender.

Para acessar as notificações, clique em **Notificações** no menu de navegação 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.

2.1.3. 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. Consequentemente, 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 em **Configurações** no menu de navegação na 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 ativar um perfil manualmente, ligue o botão correspondente. Somente um perfil pode ser ativado manualmente por vez.

Para mais informações sobre Perfis, por favor, acesse "*Perfis*" (p. 154).

2.1.4. 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 em **Configurações** no menu de navegação na interface do Bitdefender.
2. Na janela **Geral**, ative a **Proteção por Senha**.
3. Digite 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 em **Configurações** no menu de navegação na interface do Bitdefender.
2. Na janela **Geral**, desative a **Proteção por Senha**.
3. Digite a senha, depois clique em **OK**.

> **Nota**
> Para alterar a senha do seu produto, clique em **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.

2.1.5. Relatórios do produto

Os relatórios do produto contêm informações sobre como você utiliza o produto Bitdefender instalado. Esta informação é essencial para melhorar o produto e pode ajudar-nos a oferecer-lhe uma experiência melhor no futuro.

Saiba que esses relatórios não contêm dados confidenciais, como seu nome ou endereço IP, e que não serão usados para fins comerciais.

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

1. Clique em **Configurações** no menu de navegação na interface do Bitdefender.
2. Selecione a aba **Avançado**.
3. Desligue **Relatórios do produto**.

2.1.6. Notificações de ofertas especiais

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.

Para ativar ou desativar notificações de ofertas especiais:

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

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

2.1.7. Interface de Verificação Antimalware

O Bitdefender se integra com a Microsoft Interface de Verificação Antimalware (AMSI), uma forma de ajudá-lo a permanecer protegido contra malware de script dinâmico e vias não tradicionais de ciberataque. A AMSI é um padrão genérico de interface que permite que aplicativos e serviços se integrem com produtos Bitdefender.

Ligue ou desligue a Integração com Interface de Verificação Antimalware:

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

A integração com a opção de Interface de Verificação Antimalware vem habilitada de fábrica e está disponível somente no Windows 10.

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 o ícone do ângulo direito para continuar sendo guiado, ou **Pular guia** para fechar o assistente.

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

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

No menu de navegação ao lado esquerdo, você pode acessar as seções da sua conta Bitdefender, a área de configurações, notificações e as sessões

do Bitdefender para configurações detalhadas e tarefas administrativas avançadas. E você também pode nos contatar para obter suporte caso tenha perguntas ou algo inesperado apareça.

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

2.2.1. Ícone da bandeja do sistema

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

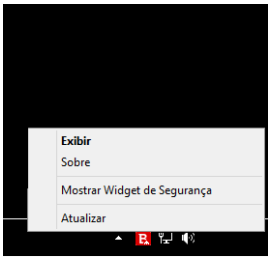
Nota

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 Bitdefendermais rapidamente.

- **Exibir** - abre a janela principal do Bitdefender.
- **Informação** - abre uma janela na qual você poderá consultar informação sobre o Bitdefender, onde procurar ajuda se acontecer algo inesperado, onde acessar e visualizar o Acordo de Assinatura, os Componentes de Terceiros e a Política de Privacidade.
- **Ocultar / Exibir Dispositivo Segurança** - ativa / desativa Dispositivo Segurança.



Ícone da área de notificação

- **Atualizar agora** - realiza uma atualização imediata. Você pode acompanhar o status de atualizações no painel de Atualizações na janela do Bitdefender.

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:

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

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.

2.2.2. Menu de navegação

No lado esquerdo da interface do Bitdefender está o menu de navegação, que lhe permite acessar rapidamente os recursos e ferramentas do Bitdefender que você precisa para utilizar seu produto. As abas disponíveis nesta área são:

- **Painel**. Daqui, você pode reparar problemas de segurança rapidamente, ver recomendações de acordo com as necessidades e uso do seu dispositivo, realizar ações rápidas e instalar o Bitdefender em outros dispositivos.

- **Proteção**. Aqui, você pode executar e configurar verificações antivírus, acessar as configurações do firewall, proteger arquivos e aplicativos contra ataques de ransomware, recuperar dados criptografados por ransomware e configurar a proteção enquanto você navega na internet.
- **Privacidade**. Daqui, você pode criar gerenciadores de senhas para suas contas online, proteger o acesso à sua webcam contra espiões, fazer pagamentos online em um ambiente online, abrir o aplicativo do VPN e proteger seus filhos ao visualizar e restringir sua atividade online.
- **Utilidades**. Daqui você pode melhorar a velocidade do sistema e configurar a função Antifurto para os seus dispositivos.
- **Notificações**. É possível acessar daqui as notificações geradas.
- **Minha conta**. Daqui, você pode acessar sua conta Bitdefender para verificar suas assinaturas e realizar tarefas de segurança nos dispositivos que você gerencia. Detalhes sobre a conta Bitdefender e assinatura em uso também estão disponíveis.
- **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.

2.2.3. Painel Geral

A janela do painel 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 alguns cliques de distância.

A janela é organizada em três áreas principais:

Área de status de segurança

Aqui é onde você pode conferir o status de segurança do seu computador.

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

Ações rápidas
: Aqui você pode executar diferentes tarefas para manter seu sistema protegido e funcionando na melhor velocidade possível. Você também pode instalar o Bitdefender em outros dispositivos, desde que sua assinatura tenha disponibilidade.

Área de status de segurança

O Bitdefenderutiliza um sistema de rastreio de problemas para detectar e lheinformar sobre os problemas que podem afetar a segurança do seu computador edados. As incidências detectadas incluem definições de proteção importantes que estão desligadas e outras condições que podem representar um risco à segurança.

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

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

Autopilot

Para lhe oferecer uma operação efetiva e proteção reforçada enquanto realiza diferentes atividades, o Bitdefender Autopilot agirá como o seu consultor de segurança pessoal. Dependendo da atividade que você realizar, seja trabalhar, fazer pagamentos online, assistir a filmes ou jogar jogos, o Bitdefender Autopilot fornecerá recomendações contextuais com base no uso e necessidades do seu dispositivo. As recomendações propostas também podem estar relacionadas às ações que você precisa executar para manter seu produto funcionando na capacidade máxima.

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

Desligando as notificações do Autopilot

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

Para desligar as notificações do Autopilot:

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

Ações rápidas

Com as ações rápidas você pode iniciar rapidamente tarefas que você considera importantes para manter seu sistema protegido e funcionando na melhor velocidade possível.

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

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

As tarefas que você pode adicionar à interface principal são:

- **Quick Scan**. Realizar uma verificação rápida para detectar imediatamente as possíveis ameaças que podem estar presentes no seu computador.
- **Verificação do sistema**. Execute uma verificação do sistema para garantir que o computador esteja livre de ameaças.
- **Analisar Vulnerabilidade**. Verifique seu computador para identificar vulnerabilidades e assegurar que todos os aplicativos instalados, além do sistema operacional, estejam atualizados e funcionando corretamente.
- **Verificar a segurança do Wi-Fi**. Abra o Consultor de Segurança do Wi-Fi para conferir se a rede sem fio doméstica à qual você está conectado é segura e se tem vulnerabilidades.
- **Carteiras**. Veja e gerencie suas carteiras.
- **Abrir o Safepay**. Abra o Bitdefender Safepay™ para proteger seus dados privados ao realizar transações online.
- **Abrir o VPN**. Abra o Bitdefender VPN para adicionar uma camada extra de proteção enquanto está conectado à internet.
- **Destruidor de arquivos**. Abra o Destruidor de Arquivos para remover todos os traços de dados sensíveis do seu computador.

- **Cofres de arquivos**. Crie cofres onde você armazena seus documentos confidenciais e sensíveis.
- **Abrir o Otimizador de um Clique**. Libere espaço em disco, repare erros de registro e proteja a sua privacidade ao apagar arquivos que não são mais úteis com um único clique de botão.
- **Abrir o Otimizador de Inicialização**. Diminua o tempo de inicialização adicionando à lista de exceção os aplicativos que não precisam ser executados na inicialização.
- **Limpar meu dispositivo**. Liberar mais espaço para dados novos excluindo arquivos desnecessários.

Para começar a proteger dispositivos adicionais com o Bitdefender:

1. Clique em **Instalar em outro dispositivo**.

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

2. Clique em **ENVIAR LINK PARA DOWNLOAD** na janela que aparece.

3. Digite um endereço de email no campo correspondente e clique em **ENVIAR EMAIL**. Observe que o link de download gerado será válido apenas durante as próximas 24 horas. Se o link expirar, você precisará gerar um novo seguindo os mesmos passos.

   No dispositivo em que você deseja instalar o Bitdefender verifique a conta de e-mail que você digitou e aperte o botão de download correspondente.

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

- Bitdefender em dispositivos com Windows.
- Bitdefender Antivirus para Mac em dispositivos macOS.
- Bitdefender Mobile Security em dispositivos Android.
- Bitdefender Mobile Security em dispositivos com iOS.

2.2.4. As seções do Bitdefender

O Bitdefender vem com três seções diferentes divididas em recursos 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 quiser acessar os recursos para uma seção específica ou para começar a configurar seu produto, clique nos seguintes ícones localizados no menu de navegação da interface do Bitdefender:

- Proteção
- Privacidade
- Utilitários

Proteção

Na seção Proteção, você pode ajustar suas configurações avançadas de segurança, gerenciar amigos e spammers, ver e editar as configurações da conexão de rede, configurar o Safe Files e as funções da Prevenção Contra Ameaças Online, conferir e reparar potenciais vulnerabilidades do sistema e avaliar as redes sem fio às quais se conecta.

Os recursos que você pode gerenciar na seção Proteção são:

ANTIVIRUS

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

A partir do recurso Antivírus, você pode acessar facilmente as seguintes tarefas de verificação:

- Análise Rápida
- Análise do Sistema
- Gerenciar Verificações
- Modo de Resgate (ambiente de resgate no Windows 10)

Para mais informações sobre tarefas de análise e como configurar a proteção antivírus, consulte "*Proteção Antivírus*" (p. 67).

PREVENÇÃO CONTRA AMEAÇAS ONLINE

A Prevenção Contra Ameaças Online o ajuda a ficar protegido contra ataques de phishing, tentativas de fraude e vazamentos de dados pessoais enquanto você navega na internet.

Para mais informações sobre como configurar o Bitdefender para proteger a sua atividade na rede, consulte "*Detecção de Ameaças Online*" (p. 90).

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. 101).

DEFESA AVANÇADA CONTRA AMEAÇAS

A Defesa Avançada Contra Ameaças protege ativamente o seu sistema contra ameaças, como ransomware, spyware e cavalos de troia, analisando o comportamento de aplicativos instalados. Os processos suspeitos são identificados e, quando necessário, bloqueados.

Para mais informações sobre como proteger seu sistema contra ameaças, acesse "*Defesa Avançada Contra Ameaças*" (p. 88).

ANTISPAM

O recurso antispam do Bitdefender assegura que sua caixa de entrada fique livre de emails indesejados ao filtrar o tráfego de correio POP3.

Para mais informações sobre a proteção antispam, consulte "*Antispam*" (p. 92).

VULNERABILIDADE

O recurso 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 Vulnerabilidade** no recurso 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 **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 espiões em potencial.

Para mais informações sobre como configurar a proteção de vulnerabilidade, consulte "*Vulnerabilidade*" (p. 106).

SAFE FILES

O recurso Safe Files protege seus arquivos pessoais contra ataques de ransomware.

Para mais informações sobre como configurar o Safe Files para proteger seus arquivos pessoais contra ataques de ransomware, acesse "*Safe Files*" (p. 118).

REMEDIAÇÃO DE RANSOMWARE

A ferramenta de Remediação de Ransomware ajuda a recuperar arquivos caso eles sejam criptografados por ransomware.

Para informações sobre como recuperar arquivos criptografados, veja "*Remediação de ransomware*" (p. 121).

Privacidade

Na seção Privacidade, você pode abrir o aplicativo do Bitdefender VPN, criptografar seus dados privados, proteger suas transações online, manter sua webcam e navegação seguras e proteger seus filhos ao restringir sua atividade online.

Os recursos que você pode gerenciar na seção Privacidade são:

VPN

O VPN protege suas atividades online e esconde seu endereço IP sempre que você se conectar a redes sem fio não seguras em aeroportos, shoppings, cafés ou hotéis. Além disso, você pode acessar conteúdos que normalmente são restritos em certas áreas.

Para mais informações sobre esse recurso, acesse "*VPN*" (p. 137).

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 obter maiores informações sobre como criar drives lógicos (ou cofres) protegidos por senha e criptografados em seu computador, consulte "*Criptografia de Arquivos*" (p. 123).

PROTEÇÃO DE VÍDEO E ÁUDIO

A Proteção de vídeo e áudio mantem sua webcam segura bloqueando o acesso a aplicativos não confiáveis e notificando-o(a) quando um aplicativo tentar acessar o seu microfone.

Para saber mais sobre como manter sua webcam protegida contra acessos indesejados e como configurar o Bitdefender para notificá-lo(a)

sobre a atividade do seu microfone, vai para "*Proteção de vídeo e áudio*" (p. 114).

GERENCIADOR DE SENHAS

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

Para mais informações sobre a configuração do Gerenciador de Senhas, acesse "*Proteção do Gerenciador de Senhas para suas credenciais*" (p. 128).

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.

Para mais informações sobre o Bitdefender Safepay™, consulte "*Segurança Safepay para transações online*" (p. 140).

PROTEÇÃO DE DADOS

O recurso Proteção de Dados permite que você apague arquivos permanentemente.
Clique em **Destruidor de Arquivos** no painel 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. 145).

Utilitários

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

Ferramentas de Otimização

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

As ferramentas de otimização disponíveis são:
- Otimizador de Um Clique
- Otimizador de Inicialização
- Limpeza de Disco

Para mais informações sobre o desempenho das ferramentas de otimização, consulte "*Utilitários*" (p. 150).

Antifurto

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:

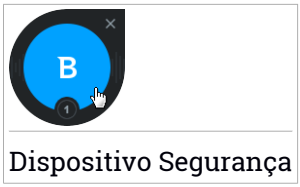
- Localização Remota
- Bloqueio Remoto
- Apagamento Remoto
- Alerta Remoto

Para mais informações sobre como você pode manter seu sistema longe de mãos erradas, consulte "*Dispositivo Antifurto*" (p. 146).

2.2.5. 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 criticas 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 1 para um evento não lido, para abrir a janela de notificações. Para mais informações, acesse *"Notificações"* (p. 9).

Analisando 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 desinfetá-los (remover o código malicioso). 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 em **Configurações** no menu de navegação na interface do Bitdefender.
  2. Na janela **Geral**, ative o **Widget de segurança**.

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

2.2.6. Mudar idioma do produto

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

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

2.3. Bitdefender Central

Bitdefender Central é a plataforma 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 do Bitdefender de qualquer computador conectado à internet,

acessando https://central.bitdefender.com, ou diretamente pelo aplicativo da Bitdefender Central em dispositivos Android e iOS.

Para instalar o aplicativo da Bitdefender Central nos seus dispositivos:

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

Assim que fizer login, você pode começar a fazer o seguinte:

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

2.3.1. Acessando a Bitdefender Central

Há várias formas de acessar a Bitdefender Central:

- Na interface principal do Bitdefender:
  1. Clique em **Minha conta** no menu de navegação da interface do Bitdefender.
  2. Clique em **Ir para a Central Bitdefender**.
  3. Entre na sua conta Bitdefender usando 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. Entre na sua conta Bitdefender usando seu endereço de e-mail e senha.

- No seu dispositivo Android ou iOS:

  Abra o aplicativo da Bitdefender Central que você instalou.

Nota
Com este material, você recebe as opções e instruções disponíveis na plataforma web.

2.3.2. Autenticação de dois fatores

O método de autenticação em 2 fatores adiciona uma camada extra de segurança à sua conta do Bitdefender, ao requerer um código de autenticação além das credenciais de login. Assim, você impedirá o roubo da conta e afugentará diversos tipos de ciberataques, como keyloggers, ataques de força bruta e de dicionário.

Ativar autenticação de dois fatores

Ao permitir a autenticação de dois fatores, você deixará a sua conta Bitdefender muito mais segura. Sua identidade será verificada cada vez que você fizer login em um dispositivo diferente, já seja para instalar um dos produtos Bitdefender, verificar o estado da sua assinatura ou executar tarefas remotamente nos seus dispositivos.

Para ativar a autenticação de dois fatores:

1. Acesse Bitdefender Central.
2. Clique no ícone no canto superior direito da tela.
3. Clique em **Conta da Bitdefender** no menu deslizante.
4. Selecione a aba **Senha e segurança**.
5. Clique em **Autenticação de dois fatores**.
6. Clique em **COMEÇAR**.

   Selecione uma das seguintes opções:

   - **Aplicativo de autenticação** - use um aplicativo de autenticação para gerar um código cada vez que você quiser acessar a sua conta Bitdefender.

Caso você queira usar o aplicativo de autenticação, mas você não tem certeza de qual escolher, aparecerá uma lista com os aplicativos de autenticação recomendados.

a. Clique em **USAR APLICATIVO DE AUTENTICAÇÃO** para começar.

b. Para entrar em um dispositivo Android ou iOS, use o seu dispositivo para escanear o código QR.

Para acessar usando um laptop ou computador, você pode adicionar manualmente o código mostrado.

Clique em **CONTINUAR**.

c. Insira o código fornecido pelo aplicativo ou o que foi mostrado no passo anterior, e então clique em **ATIVAR**.

- **E-mail** - cada vez que você acessar a sua conta Bitdefender, o código de verificação será enviado à sua caixa de e-mail. Verifique a sua conta de e-mail e então digite o código que você recebeu.

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

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

Lembre que você possui cinco minutos para verificar a sua conta de e-mail e digitar o código gerado. Se o tempo expirar, você deverá gerar um novo link seguindo os mesmos passos.

c. Clique em **ATIVAR**.

d. Você receberá dez códigos de ativação. Você pode tanto copiar, baixar ou imprimir a lista e usá-la caso perca o seu endereço de e-mail, caso contrário você não poderá acessar. Cada código pode ser usado apenas uma vez.

e. Clique em **FINALIZADO**.

Caso você queira parar de usar a autenticação de dois fatores:

1. Clique em **DESATIVAR A AUTENTICAÇÃO DE DOIS FATORES**.
2. Verifique o seu aplicativo ou conta de e-mail e digite o código que você recebeu.

   Caso você tenha escolhido receber o código de autenticação por e-mail, você terá cinco minutos para verificar a sua conta de e-mail e digitar o código gerado. Se o tempo expirar, você deverá gerar um novo link seguindo os mesmos passos.

3. Confirme sua escolha.

Adicionando dispositivos confiáveis

Para garantir que apenas você pode acessar a sua conta Bitdefender, pode ser que solicitemos o código de segurança antes. Caso queira pular este passo cada vez que se conectar com o mesmo dispositivo, nós recomendamos cadastrá-lo como um dispositivo confiável.

Para adicionar dispositivos confiáveis:

1. Acesse Bitdefender Central.
2. Clique no ícone no canto superior direito da tela.
3. Clique em **Conta da Bitdefender** no menu deslizante.
4. Selecione a aba **Senha e segurança**.
5. Clique em **Dispositivos confiáveis**.
6. Será mostrada a lista com os dispositivos Bitdefender instalados. Clique no dispositivo desejado.

Você pode adicionar quantos dispositivos desejar, contanto que eles tenham o Bitdefender instalado e sua assinatura seja válida.

2.3.3. 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
You can have one or more subscriptions on your account provided that they are for different platforms (Windows, macOS, iOS or 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**, e clique em **INSTALAR PROTEÇÃO**.
3. Escolha uma das duas opções disponíveis:
   - **Proteja este dispositivo**

     Selecione essa opção, e a seguir, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique no botão correspondente.
   - **Proteja outros dispositivos**

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

     Pressione **ENVIAR LINK DE DOWNLOAD**. Digite um endereço de email no campo correspondente e clique em **ENVIAR EMAIL**. Observe que o link de download gerado será válido apenas durante as próximas 24 horas. Se o link expirar, você precisará gerar um novo seguindo os mesmos passos.

     No dispositivo em que você deseja instalar o seu produto Bitdefender, verifique a conta de e-mail que você digitou e clique no botão de download correspondente.
4. Espere o download ser concluído, depois execute o instalador:

Renove assinatura

If you disabled the automatic renewal of your Bitdefender subscription, you can manually renew it by following these steps:

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 **ATIVAR** para continuar.

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

2.3.4. 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 do dispositivo mostram o nome do dispositivo, o estado de proteção e se há algum risco de segurança afetando a proteção dos seus dispositivos.

Para ver uma lista dos seus dispositivos ordenados de acordo com seu status ou usuários, clique na seta suspensa no canto superior direito da tela.

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 cartão de dispositivo desejado, e depois o ícone ⋮ no canto superior direito na tela.
4. Selecione **Configurações**.
5. Digite um novo nome no campo **Nome do dispositivo**, e logo clique no **SALVAR**.

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 cartão de dispositivo desejado, e depois o ícone ⋮ no canto superior direito na tela.
4. Selecione **Perfis**.
5. Clique em **Add owner** e, em seguida, preencha os respetivos campos. Customize o perfil adicionando uma foto e selecionando a data de nascimento.
6. Clique em **ADICIONAR** para salvar o perfil.
7. Selecione o proprietário desejado na lista **Proprietário do dispositivo** e clique em **ATRIBUIR**.

Para atualizar o Bitdefender remotamente no seu dispositivo Windows :

1. Acesse Bitdefender Central.
2. Selecione o painel **Meus Dispositivos**.
3. Clique no cartão de dispositivo desejado, e depois o ícone ⋮ no canto superior direito na tela.
4. 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 visualizar os detalhes sobre o dispositivo selecionado, verificar seu estado de proteção, o estado do Bitdefender VPN e quantas ameaças foram bloqueadas nos últimos sete dias. O estado

de proteção pode estar verde, quando não houver problemas afetando seu dispositivo, amarelo, quando o dispositivo requerer sua atenção, ou vermelho, quando o dispositivo estiver em risco. Quando houver problemas afetando o seu dispositivo, clique na seta suspensa na área de status superior para saber 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. 74) e "*Executar uma Análise Rápida*" (p. 73).
- **Otimizador**. Aqui você pode melhorar remotamente o desemprenho 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 em **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 em **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. 150) e "*Otimizando o tempo de inicialização do seu PC.*" (p. 151).
- **Antifurto**. 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, acesse "*Dispositivo Antifurto*" (p. 146).
- **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, acesse "*Vulnerabilidade*" (p. 106).

2.3.5. Configurações de proteção da senha do Bitdefender

Se você é o administrador da assinatura do Bitdefender Small Office Security, você pode definir uma senha para prevenir que membros da sua equipe realizem mudanças dentro do produto.

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

- Acesse Bitdefender Central.
- Clique no ícone no canto superior direito da tela.
- Clique em **Conta de administrador** no menu drop-down.
- Ative o botão correspondente.
- Digite a senha no campo correspondente, e então clique em **DEFINIR SENHA DE ADMINISTRADOR**.

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

2.3.6. Atividade

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

- **Meus dispositivos**. Aqui você pode visualizar o número de dispositivos conectados e seu estado de proteção. Para solucionar incidências de forma remota nos dispositivos detectados, clique em **Solucionar incidências**, e então clique em **VERIFICAR E REPARAR DISPOSITIVOS**.

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

- **Ameaças bloqueadas**. Aqui você pode visualizar um gráfico que mostra uma estatística geral que inclui informação sobre as ameaças bloqueadas nas últimas 24 horas e nos últimos sete dias. A informação exibida vai depender do comportamento malicioso detectado e os arquivos, aplicativos e URLs acessados.
- **Usuários principais com ameaças bloqueadas**. Aqui você pode visualizar um ranking mostrando onde a maioria das ameaças para os dispositivos foram identificadas.

2.3.7. 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

Novas ameaças são achadas e identificadas todos os dias. Por isso é muito importante manter o Bitdefender atualizado com o banco de dados de informações de ameaças mais recente.

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 atualização é executado em tempo real, o que significa que os arquivos são substituídos progressivamente. Dessa forma, o processo de atualização não afetará a operação do produto, e ao mesmo tempo, qualquer vulnerabilidade será eliminada.

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

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. 61).
- 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, acesse "*Efetuar uma atualização*" (p. 37).

2.4.1. Verifique se o Bitdefender está atualizado

Para conferir quando foi a última atualização do seu Bitdefender:

1. Clique em **Notificações** no menu de navegação 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.

2.4.2. Efetuar uma atualização

Para realizar atualizações, é necessária uma conexão à internet.

Para iniciar uma atualização, clique com o botão direito no ícone do Bitdefender na bandeja do sistema e depois selecione **Atualizar agora**.

O recurso Atualização se conectará com o servidor de atualizações da Bitdefender e buscará por 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 Windows :

1. Acesse Bitdefender Central.
2. Selecione o painel **Meus Dispositivos**.
3. Clique no cartão de dispositivo desejado, e depois o ícone no canto superior direito na tela.
4. Selecione **Atualizar**.

2.4.3. Ligar ou desligar a atualização automática

Para desativar a atualização automática:

1. Clique em **Configurações** no menu de navegação na interface do Bitdefender.
2. Selecione a aba **Atualizar**.

3. Ative ou desative o botão correspondente.
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 critica. Recomendamos que desative a atualização automática pelo menor tempo possível. Se o Bitdefender não for atualizado regularmente, não será capaz de proteger você contra as ameaças mais recentes.

2.4.4. 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 em **Configurações** no menu de navegação na 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.

Regras de processamento da atualização

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

Algumas atualizações exigem o reinício para concluir a instalação.

Por 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 notificado quando uma atualização precisar de reinicialização, ative a **Notificação de reinicialização**.

2.4.5. Atualizações contínuas

Para assegurar que você está usando a versão mais recente, seu Bitdefender buscará atualizações automaticamente. Essas atualizações podem trazer novos recursos e melhorias, reparos de problemas ou automaticamente instalar uma versão nova. Quando a nova versão do Bitdefender vem por meio de uma atualização, as configurações personalizadas são salvas e o procedimento de desinstalação e reinstalação é pulado.

Essas atualizações requererem uma reinicialização do sistema para iniciar a instalação de arquivos novos. 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 AGORA** na janela Notificações, onde a atualização mais recente é mencionada, ou reiniciar o sistema manualmente.

Nota
As atualizações incluindo novos recursos e melhorias serão proporcionadas somente aos usuários que têm o Bitdefender 2018 instalado.

3. COMO

3.1. Instalação

3.1.1. 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** no canto inferior esquerdo da interface do Bitdefender.

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

2. Clique em **ENVIAR LINK PARA DOWNLOAD** na janela que aparece.
3. Digite um endereço de email no campo correspondente e clique em **ENVIAR EMAIL**. Observe que o link de download gerado será válido apenas durante as próximas 24 horas. Se o link expirar, você precisará gerar um novo seguindo os mesmos passos.

   No dispositivo em que você deseja instalar o Bitdefender verifique a conta de e-mail que você digitou e aperte o botão de download correspondente.
4. Execute o Bitdefender que você baixou.

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

3.1.2. Como posso reinstalar o Bitdefender?

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

- você reinstalou o sistema operacional.
- você deseja resolver problemas que podem ter causado lentidão e travamentos.
- seu Bitdefender não está iniciando ou funcionando corretamente.

Se uma das situações citadas for o seu caso, siga esses passos:

- No **Windows 7**:

1. Clique **Iniciar** e acesse **Todos os Programas**.
2. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
3. Clique em **REINSTALAR** na janela que aparece.
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 **REINSTALAR** na janela que aparece.
  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 **REINSTALAR**.
  6. Você precisa reiniciar o computador para completar esse processo.

> **Nota**
> Ao seguir o procedimento de reinstalação, as configurações personalizadas são salvas e disponibilizadas no novo produto instalado. Outras configurações podem ser restauradas para o padrão.

3.1.3. Como posso mudar o idioma do meu produto Bitdefender?

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

1. Clique em **Configurações** no menu de navegação na interface do Bitdefender.

2. Na janela **Geral**, clique em **Alterar língua**.
3. Selecione a língua desejada na lista, e a seguir, clique em **SALVAR**.
4. Aguarde alguns momentos até que sejam aplicadas as configurações.

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

A partir de agora, a atualização para a versão mais recente é possível sem seguir o procedimento manual de desinstalação e reinstalação. De forma mais exata, o novo produto incluindo recursos novos e melhorias principais é entregue por meio de uma atualização. Se você já tem uma assinatura Bitdefender ativa, o produto é automaticamente ativado.

Se você está usando a versão 2018, você pode atualizar para a versão mais recente seguindo os seguintes passos:

1. Clique em **REINICIAR AGORA** na notificação que você recebe com as informações da atualização. Se você perdê-la, acesse a janela Notificações, aponte o cursor para a atualização mais recente e depois clique no botão **REINICIAR AGORA**. Aguarde a reinicialização do computador.

   A janela **O que há de novo** com informações sobre os recursos novos e melhorados aparece.
2. Clique nos links **Ler mais** para ser redirecionado para a nossa página dedicada com mais detalhes e artigos úteis.
3. Feche a janela **O que há de novo** para acessar a interface da nova versão instalada.

Os usuários que desejam atualizar gratuitamente do Bitdefender 2016 ou inferior para a versão Bitdefender mais recente devem remover sua versão atual no Painel de Controle e depois baixar o arquivo de instalação mais recente no website Bitdefender no seguinte endereço: https://www.bitdefender.com/Downloads/. A ativação é possível somente com uma assinatura válida.

3.2. Bitdefender Central

3.2.1. Como faço para acessar a conta da Bitdefender usando outra conta?

Você criou uma nova conta Bitdefender e deseja utilizá-la de agora em diante.

Para acessar usando outra conta da Bitdefender:

1. Clique em **Minha conta** no menu de navegação da interface do Bitdefender.
2. Clique no botão **Alterar conta** no canto superior direito da tela para trocar a conta vinculada ao computador.
3. Digite o endereço de e-mail no campo correspondente e clique em **PRÓXIMO**.
4. Digite sua senha, depois 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. 300).

3.2.2. 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. Clique em **Configurações** no menu deslizante.
5. Desabilite a opção **Ativar/desativar mensagens de ajuda**.

3.2.3. 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 em **Minha conta** no menu de navegação da interface do Bitdefender.
  2. Clique no botão **Alterar conta** no canto superior direito da tela.

     Uma nova janela aparece.
  3. Clique em **Esqueceu a senha?**.
  4. Verifique sua conta de e-mail, digite o código de segurança que você recebeu e depois clique em **PRÓXIMO**.

     Ou, você pode clicar em **Alterar senha** no e-mail que você recebeu.
  5. Digite a nova senha que deseja estabelecer, e em seguida digite-a novamente. Clique em **SALVAR**.
- No seu navegador da Internet:
  1. Acesse: https://central.bitdefender.com.
  2. Clique em **ENTRAR**.
  3. Digite o seu endereço de e-mail, depois clique em **PRÓXIMO**.
  4. Clique em **Esqueceu a senha?**.
  5. Confira seu email e siga as instruções fornecidas para definir uma nova senha para a sua conta Bitdefender.

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

3.2.4. 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. Clique em **Gerenciamento de conta** no menu deslizante.
5. Na área **Sessões ativas**, selecione a opção **SAIR** próxima ao dispositivo em que você deseja encerrar sessão.

3.3. A analisar com Bitdefender

3.3.1. 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.

3.3.2. Como posso analisar o meu sistema?

Para realizar uma verificação completa no sistema:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVÍRUS**, selecione **Verificação do sistema**.
3. 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, acesse "*Assistente do analisador Antivírus*" (p. 78).

3.3.3. 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 em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVÍRUS**, selecione **Gerenciar verificações**.
3. Clique em  ao lado do tipo de verificação que você deseja programar, Verificação de Sistema ou Verificação Rápida.

   Você também pode criar um tipo de verificação que atenda às suas necessidades clicando em **Criar nova tarefa de verificação**.
4. Ative a opção **Programar tarefa de verificação**.

   Escolha uma das opções correspondentes para definir uma agenda:

   - No início do sistema
   - Diariamente
   - Semanal
   - Mensal

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

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

3.3.4. 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. No painel **ANTIVÍRUS**, selecione **Gerenciar verificações**.
2. Clique em **Criar nova tarefa de verificação**.
3. No campo **Nome da tarefa**, introduza o nome da verificação, e a seguir, selecione os locais que você deseja verificar, e depois clique em **NEXT**.
4. Configure as seguintes opções gerais:
   - **Analisar apenas aplicativos**. Você pode configurar o Bitdefender para verificar apenas os aplicativos acessados.
   - **Verificar prioridade de tarefa**. Você pode escolher o impacto que o processo de verificação tem no desempenho do seu sistema.
     - Automática - A prioridade do processo de verificação vai depender da atividade do sistema. Para que o processo de verificação não afete a atividade do sistema, o Bitdefender decide se o processo de verificação deve ser executado com prioridade alta ou baixa.
     - Alta - A prioridade do processo de verificação será alta. Ao escolher essa opção, você permite que outros programas sejam executados mais devagar, diminuindo o tempo necessário para o processo de verificação ser concluído.
     - Baixa - A prioridade do processo de verificação será baixa. Ao escolher essa opção, você permite que outros programas sejam executados mais rápido, aumentando o tempo necessário para o processo de verificação ser concluído.
   - **Ações pós-verificação**. Escolha a ação que o Bitdefender deve realizar se não forem achadas ameaças:
     - Mostrar janela de resumo
     - Desligar o Computador
     - Fechar a janela de análise
5. Se deseja configurar as opções de verificação detalhadamente, clique em **Mostrar opções avançadas**.

   Clique em **SEGUINTE**.
6. Habilite **Programar tarefa de verificação** e, a seguir, escolha quando a verificação personalizada que você criou deve começar.

- No início do sistema
- Diariamente
- Mensal
- Semanal

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

7. Clique em **SALVAR** para salvar as configurações e fechar a janela de configuração.

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

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

3.3.5. Como excluir uma pasta da verificação?

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 em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVIRUS**, clique em **Configurações**.
3. Clique no separador **Exceções**.
4. Clique no menu **Lista de arquivos e pastas excluídos da verificação**, e depois no botão **Adicionar**.

5. Clique em **Buscar**, selecione a pasta que você quer excluir da verificação e depois escolha o tipo de verificação do qual ela deve ser excluída.
6. Clique em **Adicionar** para salvar as mudanças e fechar a janela.

3.3.6. 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 Exceções do Bitdefender:

1. Desative a proteção antivírus em tempo real do Bitdefender:
   a. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
   b. No painel **ANTIVIRUS**, clique em **Configurações**.
   c. Na janela **Escudo**, desative o **Escudo do Bitdefender**.

      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 mais sobre como fazer isso, por favor, acesse "*Como posso mostrar objetos ocultos no Windows?*" (p. 63).
3. Restaurar o arquivo da área de Quarentena:
   a. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
   b. No painel **ANTIVÍRUS**, clique em **Verificação Rápida**.
   c. Selecione o arquivo e depois clique em **RESTAURAR**.
4. Adicionar o arquivo à lista de Exceções. Para saber mais sobre como fazer isso, por favor, acesse "*Como excluir uma pasta da verificação?*" (p. 48).
5. Active a proteção antivírus em tempo real do Bitdefender.
6. Contate os nossos representantes do suporte para que possamos remover a detecção da atualização da informação da ameaça. Para saber mais sobre como fazer isso, por favor, acesse "*Solicite Ajuda*" (p. 300).

3.3.7. Como posso verificar quais ameaças 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 informações detalhadas sobre os processos de análise registrados, tais 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 em **Notificações** no menu de navegação da interface do Bitdefender.
2. Na aba **Todas**, selecione a notificação relacionada à última verificação.

   Aqui é onde você poderá encontrar todos os eventos de análise de ameaças, incluindo ameaças detectadas na análise durante o 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 relatório da análise, clique em **Visualizar Relatório**.

3.4. Proteção de Privacidade

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

Para ter a certeza de que as suas operações online se mantém privadas, 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 em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel do **Safepay**, clique em **Abrir Safepay**.
3. Clique no ícone  para acessar o **Teclado Virtual**.

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

3.4.2. 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. Clique no cartão de dispositivo desejado, e então selecione **Antifurto**.
4. Seleciona 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 Antifurto deixam de funcionar.

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

3.4.3. 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 arquivo armazenado no seu disco rígido local com a extensão .bvd.

Ao criar um cofre de arquivos, há dois 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, consulte "*Criptografia de Arquivos*" (p. 123).

3.4.4. 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. Clique em **EXCLUIR PERMANENTEMENTE** e depois confirme que deseja continuar com o processo.

   Aguarde que o Bitdefender termine a destruição dos arquivos.

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

3.4.5. Como protejo minha webcam contra hackers?

Você pode configurar seu Bitdefender para permitir ou negar o acesso de aplicativos instalados à sua webcam seguindo os seguintes passos:

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel de **PROTEÇÃO DE VÍDEO E ÁUDIO**, clique em **Acesso à webcam**.

   A lista de aplicativos que solicitaram acesso à sua webcam é exibida.

3. Aponte o cursor para o aplicativo cujo acesso você deseja permitir ou bloquear e depois clique no botão correspondente.

   Para ver o que outros usuários do Bitdefender escolheram fazer com o aplicativo selecionado, clique no ícone . Você será notificado sempre que um dos aplicativos listados for bloqueado por usuários do Bitdefender.

Para adicionar aplicativos à essa lista, clique no link **Adicionar um novo aplicativo à lista**.

3.4.6. Como posso restaurar manualmente arquivos criptografados quando o processo de restauração falhar?

Caso arquivos criptografados não possam ser automaticamente restaurados, você pode restaurá-los manualmente seguindo estes passos:

1. Clique em **Notificações** no menu de navegação da interface do Bitdefender.
2. Na aba **Todas**, selecione a notificação referente ao último comportamento de ransomware detectado e clique em **Arquivos encriptados**.
3. Será exibida a lista dos arquivos criptografados.

   Clique em **RECUPERAR ARQUIVOS** para continuar.

4. Caso o processo de recuperação falhe inteira ou parcialmente, você deve escolher o local em que os arquivos criptografados deveriam ser salvos. Clique em **LOCAL DA RECUPERAÇÃO** e escolha um local em seu PC.

5. Uma janela de confirmação aparecerá.

   Clique em **FINALIZAR** para finalizar o processo de restauração.

Arquivos com as seguintes extensões podem ser restaurados caso sejam criptografados:

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

3.5. Ferramentas de Otimização

3.5.1. 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. 55)
- "*Analise o seu sistema periodicamente*" (p. 56)

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 em **Utilidades** no menu de navegação da interface do Bitdefender.
2. Clique em **OTIMIZAR MEU DISPOSITIVO**
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. 150).

Analise o seu sistema periodicamente

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

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 ameaças que estejam comprometendo a segurança do seu sistema e também analisa dentro dos arquivos.

Para iniciar a Verificação do Sistema:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVÍRUS**, selecione **Verificação do sistema**.
3. Siga os passos do assistente.

3.5.2. 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 em **Utilidades** no menu de navegação da interface do Bitdefender.
2. Clique em **OTIMIZAR INICIALIZAÇÃO DE DISPOSITIVO**.
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. 151).

3.6. Informações Úteis

3.6.1. Como posso testar a minha solução de segurança?

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

O teste Eicar permite que você verifique sua solução de seguranpa utilizando um arquivo de segurança desenvolvido para esse propósito.

Para testar a sua solução de segurança:

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 uma ameaça).

   Caso clique em **Eu entendo os riscos, leve-me até lá mesmo assim**, o download do teste irá iniciar e um pop-up do Bitdefender irá informá-lo que uma ameaça foi detectada.

   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. 300).

3.6.2. 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 aparece.

4. Aguarde o processo de desinstalação ser concluído e 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 aparece.
5. Aguarde o processo de desinstalação ser concluído e 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 aparece.
6. Aguarde o processo de desinstalação ser concluído e depois reinicie o seu sistema.

Nota
O procedimento de reinstalação removerá permanentemente as configurações personalizadas.

3.6.3. Como removo o Bitdefender VPN?

O procedimento de remoção do Bitdefender VPN é similar ao que você usa para remover outros programas do seu computador

- No **Windows 7**:

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

Aguarde até que o processo de desinstalação seja finalizado.

- 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 **Bitdefender VPN** e selecione **Desinstalar**.

     Aguarde até que o processo de desinstalação seja finalizado.
- 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 **Bitdefender VPN** e selecione **Desinstalar**.
  4. Clique em **Desinstalar** novamente para confirmar sua escolha.

     Aguarde até que o processo de desinstalação seja finalizado.

3.6.4. Como remover a extensão do Antitracker da Bitdefender?

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

- Internet Explorer
  1. Clique em  ao lado da barra de pesquisa, e então selecione Gerenciar add-ons.

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

Será exibida a lista das extensões instaladas.

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

- Mozilla Firefox

1. Clique em ☰ ao lado da barra pesquisa.
2. Selecione **Add-ons** e então, selecione **Extensões**.

   Será exibida a lista das extensões instaladas.
3. Clique em **Remover** no cartão do Antitracker da Bitdefender.

3.6.5. Como desligo automaticamente o meu computador após a análise?

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

Por esse motivo, o Bitdefender permite configurar o seu produto 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 ameaças pelo Bitdefender.

Para desligar o computador uma vez finalizada a Verificação Rápida ou a Verificação de Sistema:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVÍRUS**, selecione **Gerenciar verificações**.
3. Clique em ✎ do lado da Verificação Rápida ou a Verificação de Sistema.
4. Na lista **Postar ações de verificação**, selecione **Desligar computador**, e a seguir, clique em **SEGUINTE**.
5. Habilite **Programar tarefa de verificação** e a seguir, escolha quando a tarefa deve começar.

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

Para desligar o computador quando a verificação customizada terminar:

1. Clique em do lado da verificação customizada que você criou.
2. Na janela **Tarefa de verificação**, clique em **SEGUINTE**.
3. Na lista **Postar ações de verificação**, selecione **Desligar computador**.
4. Clique em **SEGUINTE**, e depois clique em **SALVAR**.

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, acesse "*Assistente do analisador Antivírus*" (p. 78).

3.6.6. 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 em **Configurações** no menu de navegação na interface do Bitdefender.
2. Selecione a aba **Avançado**.
3. Ative o **Servidor proxy**.
4. Clique em **Mudança de proxy**.
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 Microsoft Edge, Internet Explorer, Mozilla Firefox e Google Chrome.

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

3.6.7. 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 secção **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.

3.6.8. Como posso mostrar objetos ocultos no Windows?

Estes passos são úteis nos casos de ameaça e se 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**.

3.6.9. Como posso remover outras soluções de segurança?

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

Quando utiliza mais do que uma solução de segurança no mesmo 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 o processo de desinstalação ser concluído e 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 o processo de desinstalação ser concluído e 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 o processo de desinstalação ser concluído e 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.

3.6.10. 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 ameaças que impedem o arranque normal do Windows. No Modo de Segurança funcionam apenas algumas aplicações e o Windows só carrega os controladores básicos e os componentes mínimos do sistema operativo. É por isso que a maioria das ameaças está 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

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

- Análise no acesso - previne que novas ameaças 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 email quando recebe uma.

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

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

- Análise sob pedido - permite detectar e remover ameaças que já estão localizadas 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, acesse "*Análise automática de mídia removível*" (p. 82).

Os usuários avançados poderão configurar excepções se não desejam que arquivos ou tipos de arquivos específicos sejam verificados. Para mais informações, acesse "*Configurar exceções de verificação*" (p. 84).

Quando se detecta uma ameaça, o Bitdefender irá tentar remover automaticamente o código malicioso do arquivo infectado e reconstruir o arquivo original. Esta operação é designada por desinfecção. Os arquivos que não podem ser desinfectados são movidos para a quarentena de modo a conter a infecção. Para mais informações, acesse "*Gerenciar arquivos em quarentena*" (p. 86).

Se o seu computador estiver infectado com ameaças, consulte "*Remover ameaças do seu sistema*" (p. 183). Para ajudá-lo a remover as ameaças do computador que não podem ser removidas no sistema operacional Windows, o Bitdefender lhe fornece o"*Bitdefender Modo de Resgate (ambiente de resgate no Windows 10)*" (p. 184). Este é um ambiente confiável especialmente concebido para a remoção de ameaças, o que lhe permite inicializar o computador independentemente do Windows. Quando o computador executa em Modo de Resgate (Ambiente de Resgate no Windows 10), as ameaças de Windows ficam inativas, tornando sua remoção fácil.

4.1.1. Análise no acesso (proteção em tempo real)

O Bitdefender fornece uma proteção contínua e em tempo real contra uma ampla variedade de ameaças ao verificar todos os arquivos e mensagens de e-mail acessados.

Ligar ou desligar a proteção em tempo real

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

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVIRUS**, clique em **Configurações**.
3. Na janela **Escudo**, ative ou desative o **Escudo do Bitdefender**.
4. 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 critica. Recomendamos que você desative a proteção em tempo-real o menos tempo possível. Quando a proteção em tempo real está desativada você deixa de estar protegido contra ameaças.

Ajustando as configurações 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 ajustar as configurações da proteção em tempo real:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVIRUS**, clique em **Configurações**.
3. Na janela **Escudo**, clique no menu **Exibir configurações avançadas**.

   Um janela será exibida.
4. Role a página para baixo para ajustar as configurações de verificação como for necessário.

Informação sobre as opções de análise

Poderá achar esta informação útil:

- **Analisar apenas aplicativos.** Você pode configurar o Bitdefender para verificar apenas os aplicativos acessados.
- **Analisar aplicações potencialmente indesejadas (PUA).** Selecione esta opção para verificar aplicativos não desejados. Um aplicativo potencialmente indesejado (PUA) ou programa potencialmente indesejado (PUP) é um software que normalmente vem com software freeware e mostrará pop-ups ou instalará uma barra de ferramentas no navegador padrão. Alguns deles mudarão a homepage ou o mecanismo de busca, outros executarão vários processos em segundo plano, deixando seu PC lento ou mostrando numerosos ads. Esses programas podem ser instalados sem seu consentimento (também chamados de adware) ou serão incluídos por defeito no seu kit de instalação expresso (que suporta ads).
- **Analisar compartilhamentos de rede.** Para acessar uma rede remota com segurança no seu computador, recomendamos que você mantenha habilitada a opção de Verificar compartilhamentos de rede.
- **Verificar 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. Pastas que contêm arquivos infectados não são uma ameaça imediata à segurança do seu sistema. A ameaça só pode afetar o seu sistema se o arquivo infectado for extraído

do repositório e executado sem que a proteção em tempo real esteja ativada.

Se você escolher essa opção, ative-a e depois arraste o marcador pela escala para excluir da verificação arquivos mais longos do que um valor dado em MG (Megabites).

- **Analisar e-mails.** Para evitar que qualquer ameaça seja baixada no seu computador, o Bitdefender automaticamente verifica emails de entrada e saída.

  Embora não seja recomendado, você pode desativar a verificação de ameaças do email para melhorar o desempenho do sistema. Se você desativar as opções de verificação correspondentes, os emails e arquivos recebidos não serão verificados, permitindo assim, que arquivos infectados sejam salvos no seu computador. Esta é uma ameaça grave pois a proteção em tempo real vai bloquear a ameaça quando os arquivos infectados forem acessados (abertos, movidos, copiados ou executados).

- **Analisar setores de boot.** Pode definir o Bitdefenderpara 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 boot. Quando uma ameaça infecta o setor de saída, o drive pode tornar-se inacessível e você poderá não conseguir iniciar o sistema e acessar seus dados.

- **Verificar apenas arquivos novos e modificados.** Ao verificar apenas arquivos novos e modificados, você pode melhorar significativamente a resposta geral do sistema com um comprometimento mínimo da 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 dessa ferramenta é melhorar a detecção de ameaças na inicialização do sistema e o tempo de inicialização do sistema.

Ações efetuadas em ameaças detectadas

Você pode configurar as ações tomadas pela proteção em tempo real seguindo esses passos:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVIRUS**, clique em **Configurações**.
3. Na janela **Escudo**, clique no menu **Exibir configurações avançadas**.

   Um janela será exibida.
4. Role a página para baixo até ver a opção **Ações de ameaças**.
5. Configure as definições de análise como necessário.

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.** Arquivos detectados como infectados se correspondem com uma informação de ameaça no Banco de Dados de Informações de Ameaças do Bitdefender. O Bitdefender tentará remover automaticamente o código malicioso do arquivo infectado e reconstruir o arquivo original. Esta operação é designada por desinfecção.

  Os arquivos que não podem ser desinfectados 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, acesse "*Gerenciar arquivos em quarentena*" (p. 86).

  Importante

  Para determinados tipos de ameaças, 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 desinfectar os arquivos suspeitos porque uma rotina de desinfecção não está disponível. 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 ameaças da Bitdefender. Se a presença de uma ameaça for confirmada, uma atualização de informações de ameaças é lançada para permitir sua remoção.

- **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 para 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, acesse "*Gerenciar arquivos em quarentena*" (p. 86).

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 ameaças, com um impacto mínimo no desempenho do seu sistema.

Para restaurar as definições da protecção em tempo real:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVIRUS**, clique em **Configurações**.
3. Na janela **Escudo**, clique no menu **Exibir configurações avançadas**.

   Um janela será exibida.
4. Role a página para baixo até ver a opção **Redefinir configurações**. Selecione essa opção para retornar às configurações de fábrica do antivírus.

4.1.2. Análise on-demand

O objetivo principal do Bitdefender é manter seu computador livre de ameaças. Isso é feito ao manter novas ameaças fora de seu computador e verificar seus emails e novos arquivos copiados ao seu sistema.

Há o risco de que uma ameaça já esteja alojada no seu sistema, antes mesmo de você instalar o Bitdefender. É por isso que é uma ótima idéia verificar seu computador contra ameaças residentes após instalar o Bitdefender. E, sem dúvida, é uma boa idéia verificar seu computador frequentemente contra ameaças.

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.

Analisando um arquivo ou uma pasta em busca de ameaças

Você 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 na nuvem para detectar ameaças na 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 antivírus normal.

Para realizar uma verificação rápida:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Verificação Rápida**.
3. 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.

Executando uma Análise do Sistema

A tarefa de Análise do Sistema procura em todo o computador todos os tipos de ameaças que colocam em risco a sua segurança, tais como malware, spyware, adware, rookits 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 você não estiver usando o seu computador.

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

- Certifique-se de que o Bitdefender está com seu banco de dados de informações de ameaças em dia. Analisar o seu computador utilizando banco de dados de informação de ameaças desatualizados pode impedir que o Bitdefender detecte novas ameaças criadas desde a última atualização. Para mais informações, acesse "*Mantendo o seu Bitdefender atualizado*" (p. 36).
- 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, acesse "*Configurando uma análise personalizada*" (p. 75).

Para realizar uma verificação do sistema:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVÍRUS**, selecione **Verificação do sistema**.
3. A primeira vez que você executar uma Verificação do Sistema, você verá uma apresentação da função. Clique em **OK, ENTENDI** para continuar.
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

Sempre que você achar que seu computador precisa ser verificado por ameaças potenciais, você pode configurar o Bitdefender para realizar verificações usando a janela **Gerenciar verificações**. Você pode programar uma Verificação de Sistema, uma Verificação Rápida, ou você pode criar uma verificação customizada segundo as suas necessidades.

Ao acessar a janela, os seguintes ícones são disponibilizados:

 A tarefa de verificação programada está desligada.

 A tarefa de verificação programada está ligada.

 A configuração detalhada pode ser feita nesse local.

 Deletar a verificação escolhida. Essa opção se encontra disponível apenas para novas verificações customizadas.

Para configurar uma nova verificação customizada detalhadamente:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVÍRUS**, selecione **Gerenciar verificações**.
3. Clique em **Criar nova tarefa de verificação**.
4. No campo **Nome da tarefa**, introduza o nome da verificação, e a seguir, selecione os locais que você deseja verificar, e depois clique em **NEXT**.
5. Configure as seguintes opções gerais:
   - **Analisar apenas aplicativos**. Você pode configurar o Bitdefender para verificar apenas os aplicativos acessados.
   - **Verificar prioridade de tarefa**. Você pode escolher o impacto que o processo de verificação tem no desempenho do seu sistema.
     - Automática - A prioridade do processo de verificação vai depender da atividade do sistema. Para que o processo de verificação não afete a atividade do sistema, o Bitdefender decide se o processo de verificação deve ser executado com prioridade alta ou baixa.
     - Alta - A prioridade do processo de verificação será alta. Ao escolher essa opção, você permite que outros programas sejam executados mais devagar, diminuindo o tempo necessário para o processo de verificação ser concluído.

- Baixa - A prioridade do processo de verificação será baixa. Ao escolher essa opção, você permite que outros programas sejam executados mais rápido, aumentando o tempo necessário para o processo de verificação ser concluído.

- **Ações pós-verificação**. Escolha a ação que o Bitdefender deve realizar se não forem achadas ameaças:
  - Mostrar janela de resumo
  - Desligar o Computador
  - Fechar a janela de análise

6. Se deseja configurar as opções de verificação detalhadamente, clique em **Mostrar opções avançadas**. Você encontrará informações sobre as verificações na lista ao final desta seção.

   Clique em **SEGUINTE**.

7. Habilite **Programar tarefa de verificação** e, a seguir, escolha quando a verificação personalizada que você criou deve começar.
   - No início do sistema
   - Diariamente
   - Mensal
   - Semanal

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

8. Clique em **SALVAR** para salvar as configurações e fechar a janela de configuração.

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

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.

- **Analisar aplicações potencialmente indesejadas (PUA).** Selecione esta opção para verificar aplicativos não desejados. Um aplicativo potencialmente indesejado (PUA) ou programa potencialmente indesejado (PUP) é um software que normalmente vem com software freeware e mostrará pop-ups ou instalará uma barra de ferramentas no navegador padrão. Alguns deles mudarão a homepage ou o mecanismo de busca, outros executarão vários processos em segundo plano, deixando seu PC lento ou mostrando numerosos ads. Esses programas podem ser instalados sem seu consentimento (também chamados de adware) ou serão incluídos por defeito no seu kit de instalação expresso (que suporta ads).
- **Verificar arquivos compactados.** Pastas que contêm arquivos infectados não são uma ameaça imediata à segurança do seu sistema. A ameaça só pode afetar o seu sistema se o arquivo infectado for extraído do repositório e executado sem que a proteção em tempo real esteja ativada. No entanto, é recomendável utilizar esta opção para detectar e remover qualquer ameaça potencial, mesmo se não for imediata.

  Arraste o marcador pela escala para excluir da verificação arquivos mais longos do que um valor dado em MG (Megabites).

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

- **Verificar apenas arquivos novos e modificados.** Ao verificar apenas arquivos novos e modificados, você pode melhorar significativamente a resposta geral do sistema com um comprometimento mínimo da segurança.
- **Analisar setores de boot.** Pode definir o Bitdefenderpara 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 boot. Quando uma ameaça infecta o setor de saída, o drive pode tornar-se inacessível e você poderá não conseguir iniciar o sistema e acessar seus dados.
- **Analisar Memória.** Selecione esta opção para analisar programas em execução na memória do seu sistema.
- **Analisar registro.** Selecione esta opção para analisar as chaves de registro. O Registro 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.
- **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.

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 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 ameaça 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.** Arquivos detectados como infectados se correspondem com uma informação de ameaça no Banco de Dados de Informações de Ameaças do Bitdefender. O Bitdefender tentará remover automaticamente o código malicioso do arquivo infectado e

reconstruir o arquivo original. Esta operação é designada por desinfecção.

Os arquivos que não podem ser desinfectados 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, acesse "*Gerenciar arquivos em quarentena*" (p. 86).

Importante

Para determinados tipos de ameaças, 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 desinfectar os arquivos suspeitos porque uma rotina de desinfecção não está disponível. 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 ameaças da Bitdefender. Se a presença de uma ameaça for confirmada, uma atualização de informações é lançada para permitir sua remoção.

- **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.

Apagar

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 relação aos arquivos detectados. Após a analisar terminar, você pode abrir o relatório da análise para ver informações sobres 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 a ameaça, acesse "*Remover ameaças do seu sistema*" (p. 183).

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 informações detalhadas sobre os processos de análise registrados, tais 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 em **Notificações** no menu de navegação da interface do Bitdefender.
2. Na aba **Todas**, selecione a notificação relacionada à última verificação.

   Aqui é onde você poderá encontrar todos os eventos de análise de ameaças, incluindo ameaças detectadas na análise durante o 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 análise, clique em **Exibir registro** .

4.1.3. Análise automática de mídia removível

O Bitdefender detecta automaticamente quando você conecta um dispositivo de armazenamento móvel ao seu computador e o verifica em segundo plano, quando a opção de verificação automática está ativada. Isso é recomendado para evitar que ameaças infectem seu computador.

Os dispositivos detectados se enquadram em uma destas categorias:

- CDs/DVDs
- Dispositivos de armazenamento externos como pen drives e discos rígidos 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?

Ao detectar um dispositivo de armazenamento removível, o Bitdefender começa a verificá-lo em busca de ameaças (desde que a verificação automática esteja habilitada para esse tipo de dispositivo). Será notificado através de uma janela de pop-up que um novo dispositivo foi detectado e está a ser analisado.

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.

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.

Na maioria dos casos, o Bitdefender remove automaticamente oas ameaças detectadas 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.

Esta informação pode ser útil para você:

- Tenha cuidado ao usar um CD/DVD infectado com ameaças, porque a ameaça não pode ser removida do disco (é apenas para leitura). Certifique-se de que a proteção em tempo real está ativada para evitar que ameaças se propaguem no seu sistema. É recomendado copiar quaisquer dados valiosos do disco no seu sistema e depois descartar o disco.
- Em alguns casos, o Bitdefender poderá não conseguir remover as ameaças de 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 mais sobre como superar essas ameaças, por favor, acesse "*Remover ameaças do seu sistema*" (p. 183).

Gerenciamento da análise de mídia removível

Para gerenciar a verificação automática de mídias removíveis:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVIRUS**, clique em **Configurações**.
3. Ligue ou desligue a **Verificação do arquivo hosts**.

As opções de análise são pré-configuradas para obter os melhores resultados em detecção. Caso sejam detectados arquivos infectados, o Bitdefender tentará desinfectá-los (remover o código malicioso) 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.

Para ter a melhor proteção, é recomendável deixar a opção **Verificação automática** selecionada para todos os tipos de dispositivos de armazenamento móveis.

4.1.4. 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 em **Configurações** no menu de navegação na interface do Bitdefender.
2. Selecione a aba **Avançado**.
3. Ligue ou desligue a **Verificação do arquivo hosts**.

4.1.5. Configurar exceções de verificação

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.

Você pode configurar excepções para que sejam realizadas verificações somente no acesso, sob demanda ou ambas. Os objetos excetuados da verificação no acesso não serão verificados, mesmo se forem acessados por você ou por um aplicativo.

Nota

As exceções NÃO serão aplicadas à verificação contextual. Análise Contextual é um tipo de análise por demana: Você da 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 e pastas específicas da verificação:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVIRUS**, clique em **Configurações**.
3. Selecione a aba **Exclusões**.
4. 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.
5. Adicionar exceções seguindo estes passos:
   a. Clicando **Adicionar**.
   b. Clique em **Explorar**, selecione o arquivo ou pasta que deseja excluir da análise e depois clique **Adicionar**. 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 exceção, 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 exceção 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 exceções podem tornar o seu computador vulnerável a ameaças.

Para excluir extensões de arquivo da análise:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVIRUS**, clique em **Configurações**.
3. Selecione a aba **Exclusões**.

4. Clique no menu **Lista de extensões excluídas da verificação**. Na janela que surge, pode gerenciar o arquivo e extensões excluídos da análise.
5. Adicionar exceções seguindo estes passos:
   a. Clicando **Adicionar**.
   b. Digite as extensões que você deseja excluir da verificação, separando-as por 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 exceção, selecione uma das outras opções.
   d. Clique em **ADICIONAR**.

Ativar exceções de verificação

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

Para gerenciar exceções da verificação:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVIRUS**, clique em **Configurações**.
3. Selecione a aba **Exclusões**.
4. Use as opções no menu **Lista de arquivos e pastas excluídos da verificação** para gerenciar exceções da verificação.
5. Para remover ou editar exceções da análise, clique em um dos links disponíveis. Proceder da seguinte forma:
   - Para remover uma entrada da lista, selecione-a e clique **Remover**.
   - Para editar uma entrada da tabela, dê um clique duplo (ou selecione e clique no **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**.

4.1.6. Gerenciar arquivos em quarentena

O Bitdefender isola os arquivos infectados com ameaças que não consegue desinfectar numa área segura denominada quarentena. Quando a ameaça

está na quarentena não pode prejudicar de nenhuma maneira, porque não pode ser executada ou lida.

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

Além disso, o Bitdefender analisa os arquivos em quarentena sempre que o banco de dados de informações sobre ameaças é atualizado. Os arquivos limpados são movidos automaticamente de volta ao seu local original.

Para conferir e gerenciar arquivos em quarentena:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Verificação Rápida**.

   Aqui você pode ver o nome dos arquivos em quarentena, sua localização original e o nome das ameaças detectadas.
3. Os arquivos da quarentena são gerenciados automaticamente pelo Bitdefender de acordo com as predefinições da quarentena.

   Embora não seja recomendado, você pode ajustar as configurações de quarentena segundo suas preferências clicando em **Ver Configurações**.

   Clique nos botões para ligar ou desligar:

   Verifique novamente a quarentena depois de atualizações às informações sobre ameaças
   Mantenha esta opção ativada para analisar automaticamente os arquivos da quarentena após cada atualização do banco de dados de informações de ameaças. Os arquivos limpados são movidos automaticamente de volta ao seu local original.

   Apagar conteúdo com mais de 30 dias
   Arquivos de quarentena mais antigos que 30 dias são automaticamente apagados.

   Criar exceção para arquivos restaurados
   Os arquivos que você restaurar da quarentena serão colocados de volta na sua localização original sem que sejam reparados e excluídos automaticamente de verificações futuras.

4. 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**.

4.2. Defesa Avançada Contra Ameaças

A Defesa Avançada Contra 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.

A Defesa Avançada contra Ameaças monitora continuamente os aplicativos executados no computador, à procura de ações típicas de ameaças. Cada uma destas ações é classificada e é calculada uma pontuação geral para cada processo.

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

4.2.1. Ativando ou desativando a Defesa Avançada Contra Ameaças

Para ativar ou desativar a Defesa Avançada Contra Ameaças:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **DEFESA AVANÇADA CONTRA AMEAÇAS**, ative ou desative o botão.

> **Nota**
> Para manter seu sistema protegido contra ransomware e outros tipos de ameaças, recomendamos que desligue a Defesa Avançada Contra Ameaças pelo tempo mais curto possível.

4.2.2. Conferindo ataques maliciosos detectados

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

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **DEFESA AVANÇADA CONTRA AMEAÇAS**, clique em **Defesa contra ameaças**.

3. A primeira vez que você acessar à Proteção contra Ransomware, você verá uma apresentação da função. Clique em **OK, ENTENDI** para continuar.

   Os ataques detectados nos últimos 90 dias são exibidos. Para ver detalhes sobre o tipo de ransomware detectado, o caminho do processo malicioso ou se a desinfecção foi bem-sucedida, basta clicar nele.

4.2.3. Adicionando processos a exceções

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

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

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **DEFESA AVANÇADA CONTRA AMEAÇAS**, clique em **Configurações**.
3. Na área de **Exceções**, clique em **Adicionar aplicativos à lista de exceções**.
4. Localize e selecione o aplicativo que você quer excluir da verificação, depois clique em **OK**.

   Para remover uma entrada da lista, clique na opção **Remover** ao seu lado.

4.2.4. Detecção de exploits

Uma forma usada pelos hackers para invadir sistemas é se aproveitar de certos bugs ou vulnerabilidades no software (aplicativos e plugins) e hardware dos computadores. O Bitdefender usa a mais moderna tecnologia antiexploit para evitar que seu computador seja vítima de um desses ataques, que costumam se espalhar muito rapidamente.

Ativando ou desativando a detecção de exploit

Para ativar ou desativar a detecção de exploit:

- Clique em **Proteção** no menu de navegação da interface do Bitdefender.
- No painel **DEFESA AVANÇADA CONTRA AMEAÇAS**, clique em **Configurações**.
- Clique na chave correspondente para ativar ou desativar.

Nota
A opção de Detecção de exploit aparece ativada como definição padrão.

4.3. Detecção de Ameaças Online

A Prevenção Contra Ameaças Online do Bitdefender garante uma navegação segura ao alertá-lo sobre páginas da web potencialmente maliciosas.

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

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

Para configurar a Prevenção Contra Ameaças Online:

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

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

- A prevenção contra ataques da web bloqueia ameaças provenientes da internet, incluindo downloads sem consentimento.
- 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

- Verificação da web criptografada.

  Ataques mais sofisticados podem usar tráfego da web seguro para enganar as suas vítimas. Portanto, recomendamos que você mantenha habilitada a opção Verificação da web criptografada.

- Proteção contra fraudes.

- Proteção contra phishing.

Na janela **Prevenção de ameaças na rede**, você tem a opção **Prevenção de ameaças na rede**. Para manter seu computador longe de ataques feitos por malware complexos (como ransomware) através da exploração de vulnerabilidades, mantenha a opção habilitada.

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

Para configurar e gerenciar sites, domínios e endereços IP usando a Prevenção Contra Ameaças Online fornecida pelo Bitdefender:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **PREVENÇÃO CONTRA AMEAÇAS ONLINE**, clique em **Exclusões**.
3. No campo correspondente, digite o nome do site, do domínio ou do endereço IP que você deseja adicionar às excepções, e então, faça clique em **ADICIONAR**.

   Para remover uma entrada da lista, selecione-a e clique em **Remover**.

   Clique em **SALVAR** para salvar as mudanças e fechar a janela.

4.3.1. Alertas de Bitdefender no navegador

Sempre que tenta visitar uma página Web classificada como insegura, esta é bloqueada e é apresentada uma página de aviso no seu navegador.

A página contém informações como a URL do site e a ameaça detectada.

Você precisa decidir o que fará a seguir. As seguintes opções estão disponíveis:

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

4.4. 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, acesse "*Compreender o Antispam*" (p. 93).

A proteção Antispam do Bitdefender está disponível apenas para clientes de correio eletrônico configurado para receber mensagens de email via protocolo POP3. POP3 é um dos protocolos mais utilizados para fazer o download de mensagens de email 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 email 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 email é rotulado como spam.

Se você utiliza outros clientes de email, você deve criar uma regra para mover as mensagens de e-mail marcadas como [SPAM] pelo Bitdefenderpara uma pastade 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 email for rotulado como spam.

4.4.1. 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 emails (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 emails de seus amigos à **Lista de Amigos**. O Bitdefendernão 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 email deverá entrar em sua **Caixa de Entrada** ou não.

Todo o email proveniente da internet é inicialmente verificado pelo filtro da Lista Amigos / Lista Spammers. Se o endereço do remetente se encontrar na Lista Amigos, o email 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 email está escrito em caracteres Cirílicos ou Asiáticos. Caso esteja o email será marcado como SPAM e movido para a pasta **Spam**.

Nota

Se o email é marcado como SEXUALLY EXPLICIT na linha do assunto, o Bitdefender vai considerá-lo SPAM.

Clientes de email e protocolos suportados

A proteção Antispam é fornecida para todos os clientes de email POP3/SMTP. No entanto a barra de ferramentas do Antispam Bitdefender apenas se integra em:

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

4.4.2. Ligar ou desligar a proteção antispam

A proteção Antispam está ativada por padrão.

Para ligar ou desligar a ferramenta Antispam:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTISPAM**, ative ou desative o botão.

4.4.3. 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, vá para "*Clientes de email e protocolos suportados*" (p. 94).

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 email selecionado é spam. O email 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 email selecionado não é spam e o Bitdefender não deveria tê-lo identificado como tal. O email 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 - adicina o remetente do email selecionado para a lista de Spammers. Você poderá ter que clicar **OK** para acusar recebimento. As mensagens de email recebidas destes endereços na lista de Spammers, são automaticamente marcados como [spam].
Adicionar Amigo - adiciona o remetende do email selecionado à lista de Amigos. Você poderá ter que clicar **OK** para acusar recebimento. Você sempre receberá emails desse endereço, não importa o que a mensagem contenha.

Spammers- abre a **Lista de Spammers** que contém todos os endereços de email, dos quais não quer receber mensagens, independentemente do seu conteúdo. Para mais informações, acesse "*Configurar a lista de Spammers*" (p. 98).

Amigos - abre a **Lista de amigos** que contém todos os endereços de email dos quais deseja receber mensagens de e-mail, independentemente do seu conteúdo. Para mais informações, acesse "*Configurar a Lista de Amigos*" (p. 97).

Indicar os erros de detecção

Se você está usando um cliente de email 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 emails 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 email será removida para a pasta de Entrada.

Indicar mensagens de spam não detectadas

Se você está usando um cliente de email 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 email, 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 email 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 email à lista de Amigos / Spammers.

4.4.4. Configurar a Lista de Amigos

A **Lista de Amigos** é uma lista de todos os endereços de 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 em **Proteção** no menu de navegação da interface do Bitdefender.
  2. No painel **ANTISPAM**, clique em **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:

- @domain.com e domain.com - todas as mensagens de e-mail recebidas de domain.com chegarão à sua **Caixa de entrada** independentemente do seu conteúdo;
- domínio - todos os emails vindos de domínio (não importa quais os sufixos do domínio) serão marcados como Spam;
- com - todos os emails 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. 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 em **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 uma lista de Amigos salva anteriormente, clique em **CARREGAR** e abra o arquivo correspondente .bwl. 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.

4.4.5. 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 email na **Lista de Spammers** será marcado como Spam, sem pais 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 antispam do Bitdefender integrada ao seu cliente de e-mail.
- Alternativa:
  1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
  2. No painel **ANTISPAM**, clique em **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:

- @domain.come domain.com - todas as mensagens de e-mail recebidas de domain.com chegarão à sua **Caixa de entrada** independentemente do seu conteúdo;
- domínio - todos os emails vindos de domínio (não importa quais os sufixos do domínio) serão marcados como Spam;
- com - todos os emails 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 email legítimos (tais como Yahoo!, Gmail, Hotmail, ou outros) à lista de spammers. Caso contrário, os emails 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 emails 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 em **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 em **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.

4.4.6. Configurando filtros antispam locais

Como descrito em "*Compreender o Antispam*" (p. 93), o Bitdefender utiliza um conjunto de diferentes filtros antspam para identificar o spam. Os filtros antispam são pré-configurados para uma protecção 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 em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTISPAM**, clique em **Configurações**.
3. Clique nos botões correspondentes para ativar ou desativar.

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**.

4.4.7. 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 emails de spam não detectados. Isto ajuda a melhorar a detecção antispam do Bitdefender.

Configurar o envio de amostra de email para Nuvem Bitdefender através da seleção das opções desejadas ao seguir estes passos:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTISPAM**, clique em **Configurações**.
3. Clique nos botões correspondentes para ativar ou desativar.

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**.

4.5. 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.

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.

Como uma medida de segurança, você será notificado sempre que um aplicativo potencialmente malicioso tiver o acesso à internet bloqueado.

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, consulte "*Gerenciando Configurações de Conexão*" (p. 105).

4.5.1. Ligar ou desligar a proteção firewall

Para ativar ou desativar a proteção por firewall:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **FIREWALL**, ative ou desative o botão.

Atenção

Devido ao fato de expor o seu computador a conexões não autoriadas, desligar a firewall deveria ser uma medida temporária. Volte a ligar a firewall assim que possível.

4.5.2. Gerenciamento de regras de aplicativos

Para ver e gerenciar as regras do firewall controlando o acesso de aplicações a recursos da rede e internet:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel do **FIREWALL**, clique em **Acesso de aplicativos**.
3. A primeira vez que você acessar o Firewall, você verá uma apresentação da função. Clique em **OK, ENTENDI** para continuar.

Você pode ver os 15 últimos programas (processos) que passaram pelo Firewall do Bitdefender e a rede da internet à qual você está conectado. Para ver as regras criadas para um aplicativo específico, basta clicar nele e depois clicar no link **Ver regras do aplicativo**. A janela **Regras** se abre.

Para cada regra é apresentada a seguinte informação:

- **REDE** - o processo e os tipos de adaptador de rede (Doméstica/Escritório/Pública ou Todos) aos quais a regra se aplica. 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.
- **TRÁFEGO** - a regra se aplica em ambas as direções, de entrada e de saída.
- **PORTAS** - o protocolo de PORTA ao qual a regra se aplica. Por configuração padrão, as regras se aplicam a todas as portas.
- **IP** - o protocolo de internet (IP) ao qual a regra se aplica. Por configuração padrão, as regras se aplicam a qualquer endereço de IP.
- **ACESSO** - exibe se o aplicativo tem ou não permissão para acessar a rede ou internet sob as circunstâncias especificadas.

Para editar ou apagar as regras do aplicativo selecionado, clique no ícone ⋯.

- **Editar regra** - abre uma janela onde você pode editar a regra atual.
- **Apagar regra** - abre uma janela onde você pode remover o conjunto atual de regras do aplicativo selecionado.

Adicionando regras de aplicativos

Para adicionar uma regra de aplicativo:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel do **FIREWALL**, clique em **Configurações**.
3. Na janela **Regras**, clique em **Adicionar regra**.

Na janela **Configurações** você pode aplicar as seguintes alterações:

- **Aplicar essa regra a todos os aplicativos.** Ative esse botão para aplicar a regra aplicada a todos os aplicativos.
- **Caminho do Programa.** Clique em **PROCURAR** e selecione o aplicativo ao qual a regra se aplica.
- **Permissão.** Selecione uma das seguintes permissões disponíveis:

Permissão	Descrição
Permitir	O aplicativo especificado será permitido o acesso à rede / internet nas circunstâncias determinadas.
Negar	O aplicativo especificado será permitido o acesso à rede / internet nas circunstâncias determinadas.

- **Tipo de rede.** Selecione o tipo de rede ao qual a regra se aplica. Pode alterar o tipo abrindo o menu pendente **Tipo de Rede** e selecionando um dos tipos disponíveis na lista.

Tipo de rede	Descrição
Qualquer Rede	Permitir todo o tráfego entre seu computador e outros computadores, independente do tipo de rede.

Tipo de rede	Descrição
Casa/Escritório	Permite o tráfego entre o seu computador e os computadores na rede local.
Público	Todo o tráfego é filtrado.

- **Protocolo.** Selecione do menu o protocolo IP ao qual a regra se aplica.
  - Se deseja que a regra se aplique a todos os protocolos, selecione **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 desejar que a regra se aplique ao ICMP, selecione **ICMP**.
  - Se desejar que a regra se aplique ao IGMP, selecione **IGMP**.
  - 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 atribuidos pelo Internet Assigned Numbers Authority (IANA). Pode encontrar a lista completa de números IP atribuidos em http://www.iana.org/assignments/protocol-numbers.

- **Direção.** Selecione do menu a direção do tráfego ao qual a regra se aplica.

Direção	Descrição
Saída	As regras valem apenas para tráfego de saída.
Entrada	As regras valem apenas entrada.
Ambos	As regras valem para as duas direções.

Na janela **Avançado**, você pode personalizar as seguintes configurações:

- **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.

Para remover o conjunto atual de regras e restaurar as regras padrão, clique no link **Redefinir regras** na janela **Regras**

4.5.3. Gerenciando Configurações de Conexão

Se você se conecta à internet usando um adaptador Wi-Fi ou Ethernet, você pode ajustar quais configurações devem ser aplicadas para ter uma navegação segura. Você pode escolher as seguintes opções:

- **Dinâmica** - o tipo de rede será automaticamente definido com base no perfil da rede conectada, Doméstica/Escritório ou Pública. Quando isso acontece, só as regras de Firewall para o tipo específico de rede ou aquelas definidas para aplicar a todos os tipos de rede serão aplicadas.
- **Doméstica/Escritório** – o tipo de rede será sempre Doméstica/Escritório, sem considerar o perfil da rede conectada. Quando isso acontece, só as regras de Firewall para o tipo Doméstica/Escritório ou aquelas definidas para aplicar a todos os tipos de rede serão aplicadas.
- **Pública** – o tipo de rede será sempre Pública, sem considerar o perfil da rede conectada. Quando isso acontece, só as regras de Firewall para o tipo Pública ou aquelas definidas para aplicar a todos os tipos de rede serão aplicadas.

Para configurar seus adaptadores de rede:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel do **FIREWALL**, clique em **Configurações**.
3. Selecione a aba **Adaptadores de rede**.
4. Selecione as configurações que deseja aplicar quando se conectar aos seguintes adaptadores:
   - Wi-Fi
   - Ethernet

4.5.4. Configurando definições avançadas

Para configurações avançadas de firewall:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel do **FIREWALL**, clique em **Configurações**.
3. Selecione a aba **Configurações**.

As seguintes funções podem ser configuradas:

- **Proteção de verificação de porta** - detecta e bloqueia tentativas de descobrir 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.

- **Modo de alerta** - os alertas são exibidos cada vez que um aplicativo tenta se conectar à internet. Selecione **Permitir** ou **Bloquear**. Quando o Modo de Alerta está ativo, a função de Perfis é desligada automaticamente. O Modo de Alerta pode ser usado simultaneamente com o **Modo de Bateria**.

- **Permitir acesso à rede do domínio** - aceite ou negue o acesso a recursos e itens compartilhados definidos pelos seus controladores de domínio.

- **Modo Invisível** - para não ser detectado por outros computadores. Clique em **Editar configurações sigilosas** para escolher quando seu dispositivo deve ou não ficar visível para outros computadores.

- **Comportamento padrão de aplicativo** - permita que o Bitdefender aplique configurações automáticas a aplicativos sem regras definidas. Clique em **Editar regras padrão** para escolher se as configurações automáticas devem ser aplicadas ou não.

  - Automático - o acesso de aplicativos será permitido ou negado com base no Firewall automático e nas regras do usuário.
  - Permitir - os aplicativos que não têm nenhuma regra de Firewall definida serão automaticamente permitidos.
  - Bloquear - os aplicativos que não têm nenhuma regra de Firewall definida serão automaticamente bloqueados.

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 no 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.

4.6.1. Procurar vulnerabilidades no seu sistema

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

Para verificar seu sistema em busca de vulnerabilidades:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **VULNERABILIDADE**, clique em **Verificação de vulnerabilidade**.
3. A primeira vez que você acessar a Verificação de Vulnerabilidade, você recebe uma apresentação da função. Clique em **INICIAR VERIFICAÇÃO** para continuar, e então, aguarde até que o Bitdefender verifique seu sistema em busca de vulnerabilidades.
   - **Atualizações Críticas do Windows**

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

     As atualizações podem demorar a serem instaladas.
   - **Atualizações do aplicativo**

Para visualizar informação sobre o aplicativo que precisa ser atualizado, clique no nome dele na lista.

Caso um aplicativo não esteja atualizado, clique no link **FAZER DOWNLOAD DA NOVA VERSÃO** para fazer download da última versão.

- **Contas do Windows fracas**

  Pode ver a lista dos usuários de contas Windows configurados no seu computador e o nível de proteção que as suas senhas garantem.

  Você pode escolher entre pedir ao usuário para alterar a senha no próximo acesso ou alterar a senha imediatamente.

  Para definir uma nova senha para seu sistema, selecione **Definir a senha agora**.

  Para criar uma senha segura, recomendamos o uso de uma combinação de maiúsculas e minúsculas, números e caracteres especiais (como #, $ ou @).

- **Redes Wi-Fi e roteadores**

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

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

4.6.2. 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 em **Notificações** no menu de navegação 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, clique em **Instalar**.
   - Se as atualizações automáticas do Windows estiverem desabilitadas, clique em **Habilitar**.
   - Se o aplicativo estiver desatualizado, clique em **Atualizar agora** para encontrar um link da página do distribuidor de onde você poderá instalar a versão mais recente do aplicativo.
   - Se uma conta de usuário do Windows tiver uma senha vulnerável, clique em **Alterar senha** para obrigar o usuário a mudar a senha no próximo logon ou você mesmo alterar a senha. Para obter uma senha forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).
   - Caso a função do Windows Autorun esteja ativada, clique em **Reparar** para desativá-la.
   - Se a rede à qual você está conectado tem vulnerabilidades que podem por seu sistema em risco, clique em **Alterar configurações do Wi-Fi**.
   - 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 em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **VULNERABILIDADE**, clique em **Configurações**.

   Importante
   Para ser notificado automaticamente sobre vulnerabilidades no sistema ou em aplicações, mantenha a opção **Vulnerabilidade** ativa.

3. Escolha as vulnerabilidades do sistema que deseja que sejam regularmente verificadas usando os botões correspondentes.

   Atualizações 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 de usuário

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 @).

Autorreprodução

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 ameaças usam Autorun para se propagar automaticamente na mídia removível do PC. Por isso, recomenda-se desativar este recurso do Windows.

Consultor de Segurança 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.

4.6.3. 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 emails 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 VPN.

O Consultor de Segurança do Wi-Fi do Bitdefender lhe dá informação sobre:

- Redes Wi-Fi domésticas
- Redes Wi-Fi de trabalho
- Redes Wi-Fi públicas

Desligando ou ligando as notificações do Consultor de Segurança do Wi-Fi

Para ligar ou desligar as notificações do Consultor de Segurança do Wi-Fi:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **VULNERABILIDADE**, clique em **Configurações**.
3. Na janela **Configurações**, ative ou desative a opção **Consultor de Segurança do Wi-Fi**.

Configurando a rede Wi-Fi doméstica

Para começar a configurar sua rede doméstica:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **VULNERABILIDADE**, clique em **Segurança do Wi-Fi**.
3. Na aba **Rede Wi-Fi doméstica**, clique em **SELECIONAR REDE WI-FI DOMÉSTICA**.

Uma lista com as redes sem fio às quais você já se conectou até o momento é exibida.

4. 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**.

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

Configurando a rede Wi-Fi de trabalho

Para começar a configurar sua rede de escritório:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **VULNERABILIDADE**, clique em **Segurança do Wi-Fi**.
3. Na aba **Wi-Fi de escritório**, clique em **SELECIONAR WI-FI DE ESCRITÓRIO**.

   Uma lista com as redes sem fio às quais você já se conectou até o momento é exibida.

4. Aponte para sua rede de escritório, e depois clique em **SELECIONAR**.

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

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

Para remover a rede sem fio que você definiu como rede de escritório, 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:

- A Defesa Avançada Contra Ameaças está ligada
- O Firewall do Bitdefender está ligado e as seguintes configurações são aplicadas ao seu adaptador sem fio:

- Modo Sigiloso - Ligado
- Tipo de rede - Pública

- As seguintes configurações da Prevenção Contra Ameaças Online são ativadas:
  - Verificação da web criptografada
  - 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 em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **VULNERABILIDADE**, clique em **Segurança do Wi-Fi**.
3. Dependendo das informações que você precisar, selecione uma das três abas, **Wi-Fi doméstico**, **Wi-Fi de escritório** ou **Wi-Fi pública**.
4. 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 descriptografadas 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.

4.7. Proteção de vídeo e áudio

Cada vez há mais ameaças desenhadas para acessar as webcams e microfones integrados. Para evitar o acesso não autorizado à sua webcam e para mantê-lo(a) informado sobre quais aplicativos não confiáveis acessaram o seu microfone e quando, o Bitdefender Video & Audio inclui:

- Proteção da Webcam
- Monitorador de microfone

4.7.1. Proteção da Webcam

O fato de que hackers podem assumir o controle da sua webcam para espiá-lo não é mais novidade, e as soluções para protegê-la, como a retirada de privilégios de aplicativos, desativar a câmera integrada do dispositivo ou cobri-la, não são muito práticas. Para evitar tentativas de ganhar acesso à sua privacidade, a Proteção da Webcam do Bitdefender monitora permanentemente os aplicativos que tentam acessar sua câmera e bloqueia aqueles que não estão listados como confiáveis.

Como uma medida de segurança, você será notificado sempre que um aplicativo não confiável tentar ganhar acesso à sua câmera.

Ligando ou desligando a Proteção da Webcam

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel de **PROTEÇÃO DE VÍDEO E ÁUDIO**, clique em **Configurações**.
3. Na janela **Webcam**, ative ou desative o botão correspondente.

Configurando a Proteção da Webcam

Você pode configurar quais regras devem ser aplicadas quando um aplicativo tentar ganhar acesso à sua câmera seguindo os seguintes passos:

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel de **PROTEÇÃO DE VÍDEO E ÁUDIO**, clique em **Configurações**.
3. Selecione a aba **Webcam**.

As seguintes opções estão disponíveis:

Regras de bloqueio de aplicativos

- **Bloquear todos os acessos à webcam** - nenhum aplicativo terá acesso permitido à sua webcam.
- **Bloquear o acesso de navegadores à webcam** - nenhum navegador da web, exceto o Internet Explorer e Microsoft Edge, terá acesso permitido à sua webcam. Os aplicativos da Windows Store são executados em um único processo. Por isso, o Internet Explorer e o Microsoft Edge não podem ser detectados pelo Bitdefender como navegadores, e, portanto, estão excluídos da lista.
- **Definir as permissões com base na escolha da comunidade** - se a maioria dos usuários do Bitdefender considera um aplicativo popular inofensivo, seu acesso à webcam será automaticamente permitido. Se um aplicativo popular for considerado perigoso pela maioria, seu acesso será automaticamente negado.

  Você será informado sempre que um dos seus aplicativos instalados forem listados como bloqueados pela maioria dos usuários do Bitdefender.

Notificações

- **Notificar quando aplicativos permitidos se conectarem à webcam** - você será notificado sempre que um aplicativo permitido acessar sua câmera.

Adicionando aplicativos à lista da Proteção da Webcam

Os aplicativos que tentam se conectar à sua webcam são detectados automaticamente e, dependendo do seu comportamento e da escolha da comunidade, seu acesso é permitido ou negado. No entanto, você pode começar a configurar as ações manualmente por conta própria seguindo esses passos:

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel de **PROTEÇÃO DE VÍDEO E ÁUDIO**, clique em **Acesso à webcam**.
3. A primeira vez que você acessar à Proteção Webcam, você verá uma apresentação da função.
4. Clique no link desejado:
   - **Selecionar Aplicativos Windows Store** - será exibida uma lista com os aplicativos Windows Store detectados. Ative os botões perto dos aplicativos que você deseja adicionar à lista.
   - **Comece a adicionar aplicativos à lista de acesso da webcam** - vá para o arquivo .exe que deseja adicionar à lista, em seguida, clique em **OK**.

     Para adicionar aplicativos adicionais, clique em **Adicionar um novo aplicativo à lista**.

Para ver o que os usuários do Bitdefender escolheram fazer com o aplicativo selecionado, clique no ícone .

Os aplicativos que solicitarão acesso à sua câmera e a hora da última atividade aparecerão nesta janela.

Você será notificado sempre que um dos aplicativos permitidos for bloqueado pelos usuários do Bitdefender.

Para impedir o acesso de um aplicativo adcionado à sua webcam, clique no ícone . O ícone muda para , o que significa que o aplicativo selecionado não terá acesso à sua webcam.

4.7.2. Monitorador de microfone

Aplicativos nocivos podem acessar o seu microfone embutido de forma silenciosa ou em segundo plano sem o seu consentimento. Para que você fique sabendo de potenciais exploits maliciosos, o monitorador de microfone do Bitdefender irá notificá-lo sobre esses eventos. Assim, nenhum aplicativo conseguirá acessar o seu microfone fora do seu controle.

Ligando e desligando o Monitorador de microfone

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel de **PROTEÇÃO DE VÍDEO E ÁUDIO**, clique em **Configurações**.
3. Selecione a aba **Microfone**.
4. Na janela **Microfone**, ative ou desative o botão correspondente.

Configurando notificações para o Monitorador de microfone

Para configurar as notificações que devem aparecer quando aplicativos tentarem obter acesso ao seu microfone, siga esses passos:

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel de **PROTEÇÃO DE VÍDEO E ÁUDIO**, clique em **Configurações**.
3. Selecione a aba **Microfone**.

Notificações

- **Enviar notificação quando um aplicativo tentar acessar o microfone**
- **Enviar notificação quando navegadores acessarem o microfone**
- **Enviar notificação quando aplicativos não confiáveis acessarem o microfone**
- **Mostrar notificações com base na escolha dos usuários do Bitdefender**

Adicionando aplicativos à lista do Monitorador de microfone

Aplicativos que tentarem se conectar ao seu microfone serão automaticamente detectados e adicionados à Lista de notificação. No entanto, você pode configurar manualmente se uma notificação deve ser mostrada ou não, simplemente seguindo esses passos:

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.

2. No painel **PROTEÇÃO DE VÍDEO E ÁUDIO**, clique em **Acesso ao microfone**.
3. A primeira vez que você acessar o Monitorador de microfone, você verá uma apresentação da funcionalidade.
4. Clique no link desejado:
   - **Selecionar aplicativos da Windows Store a serem adicionados à lista** - será exibida uma lista com os aplicativos da Windows Store detectados. Ative os botões perto dos aplicativos que você deseja adicionar à lista.
   - **Comece a adicionar aplicativos à lista** - vá para o arquivo .exe que deseja adicionar à lista, em seguida, clique em **OK**.

     Para adicionar aplicativos adicionais, clique em **Adicionar um novo aplicativo à lista**.

Para ver o que os usuários do Bitdefender escolheram fazer com o aplicativo selecionado, clique no ícone .

Os aplicativos que solicitarão acesso ao seu microfone e a hora da última atividade aparecerão nesta janela.

Para parar de receber notificações sobre a atividade de um aplicativo específico, clique no ícone . O ícone muda para , o que significa que nenhuma notificação do Bitdefender será mostrada quando o aplicativo selecionado tentar acessar o seu microfone.

4.8. Safe Files

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 emails 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:

- Encriptar dados privados e pessoais sem a possibilidade de desencriptação até que um resgate seja pago pela vítima.
- Travar a tela do computador e exibir uma mensagem pedindo dinheiro. Neste caso, nenhum arquivo é encriptado, mas o usuário é forçado a realizar o pagamento.
- Bloquear a execução de aplicativos.

Com o Bitdefender Safe Files você pode proteger arquivos pessoais, como documentos, fotos ou filmes, contra ataques de ransomware.

Nota
A Defesa Avançada Contra Ameaças e o Safe Files são duas camadas de proteção contra ransomware. A Defesa Avançada Contra Ameaças é o recurso que impede ataques de ransomware que vão em direção das áreas críticas do seu sistema, enquanto o Safe Files assegura que nenhum arquivo importante no seu computador seja criptografado.

4.8.1. Ativando ou desativando o Safe Files

Para ativar ou desativar a ferramenta Safe Files:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **SAFE FILES**, ative ou desative o botão.

Sempre que um aplicativo tentar acessar um arquivo protegido, um pop-up do Bitdefender será exibido. Você poderá permitir ou bloquear o acesso.

Nota
O recurso Safe Files não vem ativado.

4.8.2. Proteja seus arquivos pessoais contra ataques de ransomwares

Se você deseja proteger arquivos pessoais:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **SAFE FILES** clique em **Pastas protegidas**.
3. A primeira vez que você acessar as Pastas Protegidas, você verá uma apresentação da função. Clique em **PROTEGER MAIS PASTAS** para continuar.

4. Selecione a pasta que queira proteger. Em seguida, clique em **OK**.

   Para adicionar mais pastas, clique no link **Proteger mais pastas**. Você também pode arrastar pastas para esta janela.

As configurações de fábrica já protegem as pastas Imagens, Vídeos, Músicas e Área de Trabalho. Dados pessoais armazenados em serviços online de armazenamento de arquivos, como Box, Dropbox, Google Drive e OneDrive também são adicionados ao ambiente de proteção, desde que seus aplicativos estejam instalados no sistema.

Para evitar a lentidão do sistema, recomendamos que adicione no máximo 30 pastas, ou salve múltiplos arquivos em uma única pasta.

Nota
Pastas personalizadas somente podem ser protegidas para os usuários atuais. Arquivos de sistema e de aplicativos não podem ser adicionadas às exceções.

4.8.3. Configurando o acesso de aplicativos

As aplicações que tentam mudar ou apagar arquivos protegidos podem ser sinalizadas como potencialmente inseguras e adicionadas à lista de aplicações bloqueadas. Se um aplicativo como esse for bloqueado e você tiver certeza de que seu comportamento é normal, pode permitir seu acesso seguindo estes passos:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **SAFE FILES**, clique em **Acesso de aplicativos**.
3. Os aplicativos que tenham solicitado acesso para alterar arquivos nas suas pastas são listados. Clique no botão ao lado do aplicativo que você tem certeza de que é seguro.

Na mesma janela, você pode desativar a proteção contra ransomware para aplicativos específicos ao clicar no botão correspondente.

Caso queira adicionar mais aplicativos, clique no link **Adicionar um novo aplicativo à lista**.

4.8.4. Proteção na inicialização

Sabe-se que muitos aplicativos maliciosos 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.

Para desativar a proteção na inicialização:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **SAFE FILES** clique em **Configurações**.
3. Desative a **Proteção na inicialização**.

> **Nota**
> Os aplicativos adicionados à lista de exclusões também serão verificados e tratados adequadamente.

4.9. Remediação de ransomware

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

4.9.1. Ativar ou desativar a Remediação de Ransomware

Para ativar ou desativar a Remediação de Ransomware:

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

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

4.9.2. Para ativar ou desativar a Restauração Automática

A Restauração Automática assegura que seus arquivos sejam restaurados automaticamente em caso de criptografia por ransomware.

Para ativar ou desativar a restauração automática:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.

2. No painel **REMEDIAÇÃO DE RANSOMWARE**, clique em **Configurações**.
3. Ative ou desative o botão **Restauração automática** .

4.9.3. Ver arquivos restaurados automaticamente

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

Para ver arquivos restaurados automaticamente:

1. Clique em **Notificações** no menu de navegação da interface do Bitdefender.
2. Na aba **Todas**, selecione a notificação referente ao último comportamento de ransomware remediado e clique em **Arquivos restaurados**.

   Será exibida a lista dos arquivos restaurados. Nesse local você também pode ver o local onde seus arquivos foram restaurados.

4.9.4. Restauração manual de arquivos criptografados

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

1. Clique em **Notificações** no menu de navegação da interface do Bitdefender.
2. Na aba **Todas**, selecione a notificação referente ao último comportamento de ransomware detectado e clique em **Arquivos encriptados**.
3. Será exibida a lista dos arquivos criptografados.

   Clique em **RECUPERAR ARQUIVOS** para continuar.
4. Caso o processo de recuperação falhe inteira ou parcialmente, você deve escolher o local em que os arquivos criptografados deveriam ser salvos. Clique em **LOCAL DA RECUPERAÇÃO** e escolha um local em seu PC.
5. Uma janela de confirmação aparecerá.

   Clique em **FINALIZAR** para finalizar o processo de restauração.

Arquivos com as seguintes extensões podem ser restaurados caso sejam criptografados:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv;

.mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

4.9.5. Como adicionar aplicações às exceções

Você pode configurar regras de excepção para aplicativos de confiança para que a função de Remediação de Ameaças não bloqueie caso executem ações típicas de ransomware.

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

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **REMEDIAÇÃO DE RANSOMWARE**, clique em **Exceções**.
3. Para começar a adicionar aplicativos, clique em **Adicionar um novo aplicativo à lista**.

4.10. 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 confidencias 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.

4.10.1. Gerenciando os cofres de arquivos

Para gerenciar seus cofres de arquivos do Bitdefender:

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel **CRIPTOGRAFIA DE ARQUIVOS**, clique em **Configurações**.

   Os cofres de arquivos existentes aparecerão nesta janela.

4.10.2. Criar cofre de arquivos

Para criar um novo cofre:

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel **CRIPTOGRAFIA DE ARQUIVOS**, clique em **Criar Novo Cofre de Arquivos**.
3. Especifique o nome e o local do cofre de arquivos.
   - Digite o nome do cofre de arquivos no campo correspondente.
   - Clique em **PROCURAR**, selecione o local do cofre e salve o arquivo do cofre sob o nome desejado.
4. Escolha uma letra do disco do menu correspondente. Quando abre o cofre, um disco virtual com a letra seleccionada aparecerá em O Meu Computador.
5. Se deseja mudar o tamanho padrão (100 MB) do cofre, use as setas para cima ou para baixo na caixa **Tamanho do cofre (MB)**.
6. 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.
7. Clique em **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.

4.10.3. Importando um cofre de arquivos

Para importar um cofre de arquivos armazenado localmente:

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel **CRIPTOGRAFIA DE ARQUIVOS**, clique em **Importar cofre**.
3. Procure pelo local do cofre e selecione-o (o arquivo .bvd).
4. Clique em **Abrir**.

4.10.4. 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.

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel **CRIPTOGRAFIA DE ARQUIVOS**, clique em **Configurações**.
3. Selecione o cofre que deseja abrir e clique em **DESTRANCAR**.
4. Digite a senha necessária, depois clique em **OK**.
5. Clique em **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, selecione **Bitdefender** > **Cofre de Arquivos do Bitdefender** e depois **Destrancar**. Digite a senha requisitada, e clique em **OK**.

4.10.5. 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 em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel **CRIPTOGRAFIA DE ARQUIVOS**, clique em **Configurações**.

3. Selecione o cofre no qual deseja adicionar arquivos e clique em **DESTRANCAR**.
4. Digite a senha necessária, depois clique em **OK**.
5. Clique em **ABRIR** para abrir seu cofre.
6. 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 ao seu cofre com mais rapidez, clique com o botão direito no arquivo ou pasta que deseja copiar para o cofre, selecione **Bitdefender** > **Cofre de Arquivos do Bitdefender** e depois **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.

4.10.6. 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 em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel **CRIPTOGRAFIA DE ARQUIVOS**, clique em **Configurações**.
3. Selecione o cofre que deseja trancar e clique em **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 com mais rapidez, clique com o botão direito no arquivo .bvd representando o cofre, selecione **Bitdefender** > **Cofre de Arquivos de Bitdefender** e depois **Trancar**.

4.10.7. 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 em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel **CRIPTOGRAFIA DE ARQUIVOS**, clique em **Configurações**.
3. Selecione o cofre do qual deseja remover arquivos e clique em **DESTRANCAR**, caso esteja trancado.
4. Clique em **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**).

4.10.8. 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 em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel **CRIPTOGRAFIA DE ARQUIVOS**, clique em **Configurações**.
3. Selecione o cofre cuja senha deseja alterar e clique em **CONFIGURAÇÕES**.
4. Digite a senha atual do cofre no campo **Senha Antiga** .
5. 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 no arquivo, selecione **Bitdefender** > **Cofre de Arquivos do Bitdefender** e depois **Alterar senha do cofre**.

4.11. 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 email, 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 email 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 email
- Senhas para os aplicativos
- Senhas para redes Wi-Fi

4.11.1. 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 em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel **GERENCIADOR DE SENHAS**, clique em **Criar nova carteira**.
3. Clique em **Criar nova**.
4. 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.
5. Clique em **CONTINUAR**.
6. 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 depois clique em **CONTINUAR**.
7. Selecione o navegador da Internet de onde você deseja importar credenciais.
8. Clique em **FINALIZAR**.

4.11.2. Importar uma base de dados existente

Para importar um banco de dados da Carteira armazenado localmente:

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel **GERENCIADOR DE SENHAS**, clique em **Criar nova carteira**.

3. Clique em **DE UM LOCAL**.
4. Acesse o local no seu dispositivo onde você deseja salvar o banco de dados da carteira e escolha um nome para ele.
5. Clique em **Abrir**.
6. Dê um nome à sua carteira e digite a senha designada quando ela foi criada.
7. Clique em **IMPORTAR**.
8. Selecione os programas de onde deseja que a Carteira importe credenciais, e logo o botão **FINALIZAR**.

4.11.3. Exportar a base de dados da Carteira

Para exportar o banco de dados da sua Carteira:

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel **GERENCIADOR DE SENHAS**, clique em **Minhas carteiras**.
3. Clique no ícone ⋮ na Carteira desejada, e então selecione **Exportar**.
4. Procure pelo local do banco de dados da sua Carteira e selecione-o (o arquivo .db).
5. 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 em **ATIVAR CARTEIRA** e depois digite a senha designada quando ela foi criada.

4.11.4. Sincronize suas carteiras na nuvem

Para ativar ou desativar a sincronização das carteiras na nuvem:

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel **GERENCIADOR DE SENHAS**, clique em **Minhas carteiras**.
3. Clique no ícone ⋮ na Carteira desejada, e então selecione **Configurações**.
4. 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 sincronizar estiver bloqueada, clique em **ATIVAR CARTEIRA** e depois digite a senha designada quando ela foi criada

4.11.5. Gerenciar as suas credenciais da Carteira

Para gerenciar suas senhas:

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel **GERENCIADOR DE SENHAS**, clique em **Minhas carteiras**.
3. Selecione o banco de dados da carteira desejado e depois clique em **ATIVAR CARTEIRA**.
4. 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
- Aplicações
- 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**.

4.11.6. Ativando e desativando a proteção do Gerenciador de Senhas

Para ativar ou desativar a proteção do Gerenciador de Senhas:

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.

2. No painel **GERENCIADOR DE SENHAS**, ative ou desative o botão.

4.11.7. Alterando as configurações do Gerenciador de Senhas

Para configurar a senha mestre detalhadamente:

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel **GERENCIADOR DE SENHAS**, clique em **Configurações**.
3. Selecione a aba **Configurações de Segurança**.

As seguintes opções estão disponíveis:

- **Perguntar minha senha mestre quando entrar no meu dispositivo** - você terá que inserir sua senha mestre ao acessar o dispositivo.
- **Solicitar senha principal ao abrir navegadores e aplicativos** - será solicitada a senha principal ao acessar um navegador ou aplicativo.
- **Não solicitar minha senha-mestre** - você não precisará inserir sua senha-mestre ao acessar seu computador, um navegador ou um aplicativo.
- **Bloquear automaticamente a Carteira ao deixar meu dispositivo desatendido** - você terá que inserir sua senha mestre ao voltar ao seu dispositivo depois de 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 em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel **GERENCIADOR DE SENHAS**, clique em **Configurações**.
3. 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 recursos Preenchimento Automático simplifica a conexão aos seus websites favoritos ou login nas suas contas online. Na primeira fez 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 em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel **GERENCIADOR DE SENHAS**, clique em **Configurações**.
3. Selecione a aba **Configurações de Preenchimento automático**.
4. Configure as seguintes opções:
   - **Configure como o Gerenciador de Senhas 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 da web - abre um submenu com todos os logins de sites armazenados na Carteira. Clique em **Adicionar página** para adicionar novas páginas à lista.
- Preencher formulários - 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.

4.12. Anti-tracker

Uma grande parte dos sites que você utiliza usa rastreadores para coletar informação sobre seu comportamento para compartilhar com empresas ou para mostrar publicidade direcionada para você. Com isso, os donos dos sites ganham dinheiro por proporcionar conteúdo de graça ou para continuarem operando. Além de coletar informação, os rastreadores podem desacelerar sua navegação ou desperdiçar sua banda larga.

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

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

- Internet Explorer
- Google Chrome
- Mozilla Firefox

Os rastreadores que detectamos estão divididos nas seguintes categorias:

- **Publicidade** - usados para analisar o tráfego do site, o comportamento do usuário ou os padrões de tráfego dos visitantes.
- **Interação com o cliente** - usados para medir a interação com o usuário através de diferentes formas de entrada, como chat ou suporte.
- **Essenciais** - usados para monitorar funcionalidades críticas do site.
- **Analíticas do site** - usados para coletar dados sobre o uso do site.
- **Mídia social** - usados para monitorar o público em mídias sociais, suas atividades e o engajamento dos usuários nas diferentes plataformas de mídias sociais.

4.12.1. Interface do Antitracker

Ao ativar a extensão do Antitracker da Bitdefender, o ícone  aparece ao lado da barra de pesquisa no seu navegador. Cada vez que você visitar um site, vai aparecer um contador no ícone referente aos rastreadores detectados e bloqueados. Para visualizar mais detalhes sobre os rastreadores bloqueados, clique no ícone para abrir a interface. Além do número de rastreadores bloqueados, você pode visualizar o tempo que a página precisa para carregar e as categorias às quais os rastreadores pertencem. Para visualizar a lista de sites que estão rastreando, clique na categoria desejada.

Para impedir que o Bitdefender bloqueie rastreadores no site que você está visitando, clique em **Pausar proteção neste site**. A configuração se aplica somente enquanto você tiver o site aberto, e volta ao estado inicial ao fechar o site.

Para permitir que os rastreadores de uma categoria específica monitorizem sua atividade, clique na atividade desejada, e a seguir, no botão correspondente. Se mudar de ideia, clique no mesmo botão novamente.

4.12.2. Desligar o Antitracker da Bitdefender

Para desligar o Antitracker da Bitdefender:

- No seu navegador da Internet:
  1. Abra seu navegador da web.
  2. Clique no ícone ao lado da barra de endereços no seu navegador.
  3. Clique no ícone no canto superior direito.
  4. Use a chave correspondente para desativá-lo.

     O ícone do Bitdefender fica cinza.
- A partir da interface do Bitdefender:
  1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
  2. No painel **ANTITRACKER**, clique em **Configurações**.
  3. Desligue a chave correspondente do lado do navegador no qual você deseja desabilitar a extensão.

4.12.3. Permitir o rastreamento do site

Se você deseja ser rastreado ao visitar um site em particular, você pode adicionar seu endereço às excepções da seguinte forma:

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

   Se você deseja adicionar outro site, digite o endereço no campo correspondente, e a seguir, clique em .

4.13. VPN

O aplicativo do VPN pode ser instalado a partir do seu produto Bitdefender e usado sempre que você desejar adicionar uma camada de proteção extra à sua conexão. O VPN funciona como um túnel entre o seu dispositivo e a rede à qual você se conecta, protegendo sua conexão, criptografando seus dados usando criptografia de nível bancário e escondendo seu endereço IP onde quer que esteja. Seu tráfego é redirecionado por meio de um servidor separado, tornando seu dispositivo quase impossível de ser identificado dentre os incontáveis dispositivos que usam nossos serviços. Além disso, enquanto estiver conectado à internet com o Bitdefender VPN, você pode acessar conteúdos que normalmente são restritos em áreas específicas.

Nota
Alguns países censuram a internet e, portanto, o uso de VPNs em seus territórios foi banido por lei. Para evitar consequências legais, uma mensagem de aviso pode aparecer ao tentar usar o aplicativo Bitdefender VPN pela primeira vez. Ao continuar a usar esse aplicativo, você confirma que está ciente das regulamentações aplicáveis e dos riscos aos quais você pode estar exposto.

4.13.1. Instalando o VPN

O aplicativo de VPN pode ser instalado a partir da interface do Bitdefender da seguinte forma:

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel do **VPN**, clique em **Instalar VPN**.
3. Na janela com a descrição do aplicativo do VPN, leia o **Acordo de Assinatura** e depois clique em **INSTALAR O BITDEFENDER VPN**.

   Aguarde um momento até os arquivos serem baixados e instalados.

   Se for detectado outro VPN, recomendamos que você o desinstale. Ao ter instaladas várias soluções VPN, você pode experimentar lentidão no sistema ou outros problemas funcionais.
4. Clique em **ABRIR O VPN BITDEFENDER** para finalizar o processo de instalação.

Nota
O Bitdefender VPN requer o .Net Framework 4.5.2 ou superior para ser instalado. Caso não tenha esse pacote instalado, uma janela de notificação aparecerá. Clique em **instalar o .Net Framework** para ser redirecionado para uma página onde você pode baixar a versão mais recente desse software.

4.13.2. Abrindo o VPN

Para acessar a interface principal do Bitdefender VPN, use um dos seguintes métodos:

- Para a bandeja do sistema
  1. Clique com o botão direito no ícone na bandeja do sistema e depois clique em **Exibir**.
- A partir da interface do Bitdefender:
  1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
  2. No painel do **VPN**, clique em **Abrir VPN**.

4.13.3. Interface do VPN

A interface do VPN exibe o status do aplicativo, conectado ou desconectado. O local do servidor para usuários com a versão gratuita é determinado automaticamente pelo Bitdefender para o servidor mais adequado, enquanto os usuários Premium têm a possibilidade de alterar o local do servidor ao qual desejam se conectar. Para mais informações sobre as assinaturas de VPN, acesse "*Assinaturas*" (p. 139).

Para conectar ou desconectar, basta clicar no status exibido no topo da tela, ou dê um clique com o botão direito na bandeja do sistema. O ícone da bandeja do sistema exibe um símbolo verde quando o VPN está conectado e vermelho quando o VPN está desconectado

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

Para ter acesso a mais opções, acesse a área do **Menu** ao clicar no ícone no lado superior esquerdo. Você tem as seguintes opções:

- **Minha conta** - detalhes sobre a sua conta Bitdefender e a assinatura do VPN são exibidos. Clique em **Trocar conta** se deseja entrar com outra conta.

- **Configurações** – dependendo das suas necessidades, você pode personalizar o comportamento do seu produto:
  - receba notificações quando o VPN se conectar ou desconectar automaticamente
  - executar o aplicativo do VPN automaticamente na inicialização do Windows
  - executar o aplicativo do VPN automaticamente quando seu dispositivo se conectar a redes sem fio não seguras
- **Atualizar para o Premium** - Se você está usando a versão gratuita, pode atualizar para o plano Premium aqui.
- **Suporte** - você é redirecionado para a nossa plataforma do Centro de Suporte onde poderá ler um artigo útil sobre como utilizar o Bitdefender VPN.
- **Sobre** - são apresentadas informações sobre a versão instalada.

4.13.4. Assinaturas

O Bitdefender VPN oferece gratuitamente uma quota de tráfego diário de 200 MB por dispositivo para proteger a conexão sempre que a sua equipe precisar.

Para obter tráfego ilimitado e acesso irrestrito a conteúdos no mundo todo podendo escolher um local de servidor da escolha da sua equipe, atualize para a versão premium.

Você pode atualizar para a versão do Bitdefender Premium VPN em qualquer momento no painel **Minhas assinaturas** disponível na conta do seu Bitdefender.

A assinatura do Bitdefender Premium VPN é independente da assinatura do Bitdefender Small Office Security, ou seja, você poderá usá-lo durante todo o seu período de validade. Caso a assinatura do Bitdefender Premium VPN expire e a do Bitdefender Small Office Security continue ativa, você voltará para o plano gratuito.

O Bitdefender VPN é um produto multiplataforma, disponível nos produtos Bitdefender compatíveis com Windows, macOS, Android e iOS. Ao atualizar para o plano premium, você pode usar sua assinatura em todos os produtos, desde que faça login com a mesma conta do Bitdefender.

4.14. 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, acesse "*Proteção do Gerenciador de Senhas para suas credenciais*" (p. 128).

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™.

4.14.1. 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:

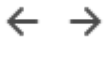
- Na interface do Bitdefender:
  1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
  2. No painel do **Safepay**, clique em **Abrir Safepay**.
- Do Windows:
  - No **Windows 7**:
    1. Clique **Iniciar** e acesse **Todos os Programas**.
    2. Clique em **Bitdefender**.
    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.

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  respetivamente.
- 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 informação importante clicando e selecionando **Imprimir**.

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

4.14.2. Configurando definições

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

Lista de domínios

Os sites que você adicionou aos Favoritos com a opção **Abrir automaticamente no Safepay** habilitada aparecerão aqui. Se você quer que um site da lista pare de abrir automaticamente com o Bitdefender Safepay™, clique em × do lado da entrada desejada na coluna **Remover**.

Bloquear 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.

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.

Clique em **IMPORTAR CERTIFICADOS** e siga o assistente para usá-los 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.

4.14.3. Gerenciando bookmarks

Caso você tenha desabilitado a detecção automática de alguma ou de todas as páginas, ou o Bitdefendersimplesmente 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. Digite o URL e o título do favorito, e depois 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.

4.14.4. Ligando as notificações do Safepay

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

Para desligar as notificações do Safepay:

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel do **Safepay**, clique em **Configurações**.
3. Desligue as **notificações do Safepay**.

4.14.5. Usando o VPN com o Safepay

Para realizar pagamentos online em um ambiente seguro enquanto estiver conectado a redes não seguras, o produto Bitdefender está configurado para executar automaticamente o aplicativo do VPN ao mesmo tempo com o Safepay.

Para começar a usar o VPN junto com o Safepay:

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel do **Safepay**, clique em **Configurações**.
3. Ligue **Usar o VPN com o Safepay**.

4.15. Proteção de Dados

4.15.1. 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. Clique em **EXCLUIR PERMANENTEMENTE** e depois confirme que deseja continuar com o processo.

   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 em **Privacidade** no menu de navegação da interface do Bitdefender.
2. No painel **PROTEÇÃO DE DADOS**, selecione **Destruidor de Arquivos**.
3. Siga o assistente do Destruidor de Arquivos:
   a. Clique no botão **ADICIONAR PASTAS** para adicionar os arquivos ou pastas que deseja remover permanentemente.

      Você também pode arrastar esses arquivos ou pastas para esta janela.
   b. Clique em **EXCLUIR 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.

4.16. Dispositivo Antifurto

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 Antifurto, 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 Antifurto 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 reacessar 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 Antifurto 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 Antifurto

Para acessar as funções Antifurto, utilize uma das opções abaixo:

- Na interface principal do Bitdefender:
  1. Clique em **Utilidades** no menu de navegação da interface do Bitdefender.
  2. Clique em **IR PARA A CENTRAL BITDEFENDER**.

     Você será redirecionado para a página da Bitdefender Central. Assegure-se de acessar a conta com suas creden
  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. Entre na sua conta Bitdefender usando 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. Seleciona 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 Antifurto deixam de funcionar.

4.17. 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 pelas ameaças 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 ameaças automaticamente. Uma vez que um dispositivo USB esteja imunizado, as ameaças já não poderão 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 armazenagem 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 a ameaça no autorun** aparecerá ao invés da opção Imunizar.

Para evitar que o seu computador execute ameaças de dispositivos USB não imunizados, desative a função de media autorun. Para mais informações, acesse "*Usando o monitoramento automático de vulnerabilidade*" (p. 108).

5. OTIMIZAÇÃO DO SISTEMA

5.1. Utilitários

O Bitdefender vem com uma seção de utilidades 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 de 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 que poderiam ser os principais responsáveis pelo seu pouco espaço em disco e lhe oferece a possibilidade de conservá-los ou não.

5.1.1. 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 em **Utilidades** no menu de navegação da interface do Bitdefender.
2. Clique em **OTIMIZAR MEU DISPOSITIVO**
   a. **Analisando**

      Espere o Bitdefender terminar de procurar por problemas no sistema.

      - Limpeza de Disco - identifica os arquivos e pastas desnecessárias.

- 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**

Espere 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**.

5.1.2. 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 em **Utilidades** no menu de navegação da interface do Bitdefender.
2. Clique em **OTIMIZAR INICIALIZAÇÃO DE DISPOSITIVO**.

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.
- **Atrasar.** 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.
- **Desativar.** 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.

5.1.3. 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 ajuda a otimizar seu espaço em disco facilmente identificando os arquivos que poderiam ser os principais responsáveis pelo seu pouco espaço em disco. Você ainda terá a possibilidade de decidir o que você quer fazer com os arquivos identificados.

Para começar a limpar seu sistema:

1. Clique em **Utilidades** no menu de navegação da interface do Bitdefender.
2. Clique em **LIMPAR MEU DISPOSITIVO**.
3. A primeira vez que você acessar a Limpeza de Disco, você verá uma apresentação da função. Clique em **OK, ENTENDI** para continuar.

   a. **Unidades de Disco e dispositivos**

   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 **ANALISAR DISCO** na área do disco que você deseja limpar.

   b. **Analisando disco**

   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. Para selecionar em qual ordem os resultados devem ser exibidos, utilize a seta para baixo **ORDENAR POR** que se encontra na parte esquerda da tela. Você pode filtrar os resultados por tamanho (desde 10 MB até mais de 5 GB) ou por tipo (os arquivos são ordenados em pastas diferenciadas por suas extensões).

   Selecione os arquivos que você deseja apagar e depois clique em **CONFIRMAR SELEÇÃO** para iniciar o processo.

   Arquivos protegidos ou importantes responsáveis pela operação do seu sistema também são identificados, mas eles não podem ser selecionados ou deletados.

   Clique no ícone  para ter acesso às pastas pertencentes aos arquivos selecionados.

   d. **Confirme sua seleção**

Será exibida a lista dos arquivos selecionados. De uma olhada e comprove se você realmente não precisa mais desses arquivos, já que mais adiante, eles não poderão ser recuperados da lixeira. Confirme sua escolha clicando em **APAGAR**.

e. **Resumo dos Resultados**

O status do processo será mostrado da seguinte forma:

O status do processo será mostrado da seguinte forma:
Um ou mais arquivos selecionados não pôde ser deletado **ou** nenhum dos arquivos selecionados pôde ser deletado.

Clique em **Terminar** para fechar a janela.

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.
- Notificações de ofertas especiais 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:

- A Defesa Avançada Contra Ameaças está ligada
- O Firewall do Bitdefender está ligado e as seguintes configurações são aplicadas ao seu adaptador sem fio:
  - Modo Sigiloso - Ligado
  - Tipo de rede - Pública
- As seguintes configurações da Prevenção Contra Ameaças Online são ativadas:
  - Verificação da web criptografada
  - Proteção contra fraudes
  - Proteção contra phishing

5.2.1. Perfil de Trabalho

A execução de várias tarefas no trabalho, tais como o envio de emails, 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 em **Configurações** no menu de navegação na interface do Bitdefender.
2. Selecione a aba **Perfis**.
3. Clique no botão **CONFIGURAR** na área do Perfil de Trabalho.
4. 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
5. Clique em **SALVAR** para salvar as mudanças 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 abre um certo aplicativo de trabalho, você pode adicioná-lo manualmente à **Lista de aplicativos de trabalho**.

Para adicionar manualmente aplicativos à lista de aplicativos de trabalho no Perfil de Trabalho:

1. Clique em **Configurações** no menu de navegação na interface do Bitdefender.
2. Selecione a aba **Perfis**.
3. Clique no botão **CONFIGURAR** na área do Perfil de Trabalho.
4. Na janela **Configurações do perfil de trabalho**, clique em **Lista de aplicativos**.
5. Clique em **ADICIONAR**.

   Uma nova janela aparece. Vá até o arquivo executável do aplicativo, selecione-o e clique em **OK** para adicioná-lo à lista.

5.2.2. Perfil de Filme

A exibição de conteúdo de vídeo de alta qualidade, como filmes de alta definição, exige recursos significativos do sistema. O Perfil de Filme ajusta as 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 em **Configurações** no menu de navegação na interface do Bitdefender.
2. Selecione a aba **Perfis**.
3. Clique no botão **CONFIGURAR** na área do Perfil de Filme.
4. 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.
5. Clique em **SALVAR** para salvar as mudanças e fechar a janela.

Adicionando manualmente reprodutores de vídeo à lista do Perfil de Filme

Se o Bitdefender não entrar automaticamente no Perfil de Cinema quando você abre um certo aplicativo de reprodução de vídeo, você pode adicioná-lo manualmente à **Lista de aplicativos de filmes**.

Para adicionar manualmente reprodutores de vídeo à lista de aplicativos de filmes no Perfil de Cinema:

1. Clique em **Configurações** no menu de navegação na interface do Bitdefender.
2. Selecione a aba **Perfis**.
3. Clique no botão **CONFIGURAR** na área do Perfil de Filme.

4. Na janela **Configurações do perfil de cinema**, clique em **Lista de reprodutores**.
5. Clique em **ADICIONAR**.

   Uma nova janela aparece. Vá até o arquivo executável do aplicativo, selecione-o e clique em **OK** para adicioná-lo à lista.

5.2.3. 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 em **Configurações** no menu de navegação na interface do Bitdefender.
2. Selecione a aba **Perfis**.
3. Clique no botão **CONFIGURAR** na área do Perfil de Jogos.
4. 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.
5. Clique em **SALVAR** para salvar as mudanças e fechar a janela.

Adicionando jogos manualmente à lista de Jogos

Se o Bitdefender não entrar automaticamente no Perfil de Jogos quando você abre um certo jogo ou aplicativo, você pode adicioná-lo manualmente à **Lista de aplicativos de jogos**.

Para adicionar manualmente jogos à lista de aplicativos de jogos no Perfil de Jogos:

1. Clique em **Configurações** no menu de navegação na interface do Bitdefender.
2. Selecione a aba **Perfis**.
3. Clique no botão **CONFIGURAR** na área do Perfil de Jogos.
4. Na janela **Configurações do Perfil de Jogos**, clique em **Lista de jogos**.
5. Clique em **ADICIONAR**.

   Uma nova janela aparece. Vá até o arquivo executável do jogo, selecione-o e clique em **OK** para adicioná-lo à lista.

5.2.4. Perfil Wi-Fi Público

Enviar emails, 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 em **Configurações** no menu de navegação na interface do Bitdefender.
2. Selecione a aba **Perfis**.
3. Clique no botão **CONFIGURAR** na área do perfil Wi-Fi Público.
4. Deixe marcada a caixa **Ajusta as configurações do produto para reforçar a proteção quando conectado a uma rede Wi-Fi pública não segura**.
5. Clique em **Guardar**.

5.2.5. 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 bateira 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 em **Configurações** no menu de navegação na interface do Bitdefender.
2. Selecione a aba **Perfis**.
3. Clique no botão **CONFIGURAR** na área do perfil Modo de Bateria.
4. 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.
5. Clique em **SALVAR** para salvar as mudanças 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.

5.2.6. 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 em **Configurações** no menu de navegação na interface do Bitdefender.
2. Selecione a aba **Perfis**.
3. Desça a página até ver a opção de Otimização em Tempo Real e depois use o botão correspondente para ligá-la ou desligá-la.

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. 162)
- "*A análise não inicia*" (p. 164)
- "*Não posso mais usar uma app*" (p. 166)
- "*O que fazer quando o Bitdefender bloqueia um site, domínio, endereço IP ou aplicativo online seguro*" (p. 167)
- "*O que fazer se o Bitdefender detectar uma aplicação segura como ransomware*" (p. 167)
- "*Como atualizar o Bitdefender numa ligação à Internet lenta*" (p. 172)
- "*Os Serviços do Bitdefender não estão respondendo*" (p. 172)
- "*O filtro antispam não funciona corretamente*" (p. 173)
- "*A funcionalidade Preenchimento Automático não funciona na minha Carteira*" (p. 178)
- "*A Remoção do Bitdefender falhou*" (p. 179)
- "*O meu sistema não reinicia após a instalação de Bitdefender*" (p. 180)

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. 300).

6.1.1. O meu sistema parece estar lento

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

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 todas as outras soluções de segurança utilizadas antes de instalar o Bitdefender. Para mais informações, acesse "*Como posso remover outras soluções de segurança?*" (p. 64).

- **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 multiplos aplicativos ao mesmo tempo. Para mais informações, acesse "*Requisitos mínimos do sistema*" (p. 3).

- **Você instalou aplicativos que não usa**.

  Qualquer computador tem programas ou aplicativos sem utilizar. 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 por ameaças. Spyware, malware, 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 ameaças que estejam comprometendo a segurança do seu sistema.

  Para iniciar a Verificação do Sistema:

  1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
  2. No painel **ANTIVÍRUS**, selecione **Verificação do sistema**.
  3. Siga os passos do assistente.

6.1.2. A análise não inicia

Este tipo de problema pode ter duas causas principais:

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

  Neste caso, reinstale o Bitdefender:

  - No **Windows 7**:
    1. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Programas e Recursos**.
    2. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
    3. Clique em **REINSTALAR** na janela que aparece.
    4. Aguarde o processo de reinstalação ser concluído e depois reinicie 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 **REINSTALAR** na janela que aparece.
    5. Aguarde o processo de reinstalação ser concluído e depois reinicie 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 **REINSTALAR** na janela que aparece.
    6. Aguarde o processo de reinstalação ser concluído e depois reinicie seu sistema.

> **Nota**
> Ao seguir o procedimento de reinstalação, as configurações personalizadas são salvas e disponibilizadas no novo produto instalado. Outras configurações podem ser restauradas para o padrão.

- **O Bitdefender não é a única solução de segurança instalada no seu sistema**.

  Neste caso:

  1. Remover a outra solução de segurança. Para mais informações, acesse "*Como posso remover outras soluções de segurança?*" (p. 64).
  2. Reinstale o Bitdefender:
     - 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 **REINSTALAR** na janela que aparece.
       d. Aguarde o processo de reinstalação ser concluído e depois reinicie 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 **REINSTALAR** na janela que aparece.
       e. Aguarde o processo de reinstalação ser concluído e depois reinicie 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 **REINSTALAR** na janela que aparece.

f. Aguarde o processo de reinstalação ser concluído e depois reinicie seu sistema.

Nota
Ao seguir o procedimento de reinstalação, as configurações personalizadas são salvas e disponibilizadas no novo produto instalado. Outras configurações podem ser restauradas para o padrão.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção "*Solicite Ajuda*" (p. 300).

6.1.3. Não posso mais usar uma app

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.

Esse tipo de situação ocorre quando a Defesa Avançada Contra Ameaças detecta erroneamente alguns aplicativos como maliciosos.

A Defesa Avançada Contra Ameaças é um recurso do Bitdefender que monitora constantemente os aplicativos em execução no seu sistema e reporta aqueles com comportamento potencialmente malicioso. Como esse recurso é baseado em um sistema heurístico, poderá haver casos nos quais aplicativos legítimos são reportados pela Defesa Avançada Contra Ameaças.

Quando isso acontecer, você poderá excluir o respectivo aplicativo para que não seja monitorado pela Defesa Avançada Contra Ameaças.

Para adicionar o programa à lista de exceções:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **DEFESA AVANÇADA CONTRA AMEAÇAS**, clique em **Configurações**.

3. Na área de **Exceções**, clique em **Adicionar aplicativos à lista de exceções**.
4. Localize e selecione o aplicativo que você quer excluir da verificação, depois clique em **OK**.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção "*Solicite Ajuda*" (p. 300).

6.1.4. O que fazer quando o Bitdefender bloqueia um site, domínio, endereço IP ou 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 site, domínio, endereço IP ou aplicativo online seguro como inseguro, o que poderia fazer com que a verificação de tráfego HTTP do Bitdefender o bloqueie incorretamente.

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

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

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **PREVENÇÃO CONTRA AMEAÇAS ONLINE**, clique em **Exclusões**.
3. Adicione o endereço do site bloqueado, o nome do domínio, endereço IP ou aplicativo online no campo correspondente e clique em **ADICIONAR**.
4. Clique em **SALVAR** para salvar as mudanças e fechar a janela.

Apenas sites, domínios, endereços IP e aplicativos nos quais você confia plenamente deveriam ser adicionados à lista. Esses serão excluídos da análise pelos seguintes mecanismos: ameaças, phishing e fraude.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção "*Solicite Ajuda*" (p. 300).

6.1.5. 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 um aplicativo seja adicionado à lista de aplicações não confiáveis e se você tem certeza de que é seguro usá-lo, siga esses passos:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **SAFE FILES**, clique em **Acesso de aplicativos**.
3. Os aplicativos que tenham solicitado acesso para alterar arquivos nas suas pastas são listados. Clique no botão **Permitir** ao lado do aplicativo que você tem certeza de que é seguro.

6.1.6. 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 em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel do **FIREWALL**, clique em **Configurações**.
3. Na janela **Regras**, clique em **Adicionar regra**.
4. 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. 300).

6.1.7. 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 entre o respectivo dispositivo da seguinte forma:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel do **FIREWALL**, clique em **Configurações**.
3. Na janela **Regras**, clique em **Adicionar regra**.
4. Na janela **CONFIGURAÇÕES**, ative a opção **Aplicar essa regra a todos os aplicativos**.
5. Selecione a aba **Avançado**.
6. Na caixa **Endereço remoto personalizado**, digite o endereço de IP do computador ou da impressora aos quais deseja ter acesso irrestrito.

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, 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. 300).

6.1.8. A minha Internet está lenta

Esta situação poderá surgir depois de instalar o Bitdefender. Este problema poderá ser causado por erros na configuração da firewall do Bitdefender.

Para solucionar essa situação:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel do **FIREWALL**, clique no botão desligar para desativar a função.
3. 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. 300).
   - Se a conexão com a internet melhorou após desativar o firewall do Bitdefender:
     a. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
     b. No painel do **FIREWALL**, clique em **Configurações**.
     c. Vá para a aba **Adaptadores de rede** e configure sua conexão com a internet como **Doméstica/Escritório**.
     d. Na janela **Configurações**, desative a **Proteção de verificação de porta**.

        Na área **Modo Sigiloso**, clique em **Editar conexões sigilosas**. Ligue o Modo Sigiloso para o adaptador de rede ao qual você está conectado.
     e. 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. 300).

6.1.9. Como atualizar o Bitdefender numa ligação à Internet lenta

Se tiver uma ligação à Internet lenta (por exemplo, ligação telefónica), poderão ocorrer erros durante o processo de atualização.

Para manter seu sistema atualizado com o banco de dados de informações de ameaças mais recente do Bitdefender:

1. Clique em **Configurações** no menu de navegação na interface do Bitdefender.
2. Selecione a aba **Atualizar**.
3. Desligar o botão **Atualização silenciosa**.
4. A próxima vez que uma atualização estiver disponível, você será pedido para selecionar a atualização que você deseja descarregar. Selecionar apenas **Atualização de assinaturas**.
5. O Bitdefender baixará e instalará somente o banco de dados de informações de ameaças.

6.1.10. 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, acesse "*Como posso remover outras soluções de segurança?*" (p. 64).

Se o erro persistir, entre em contato com nossos representantes de suporte conforme descrito na seção "*Solicite Ajuda*" (p. 300).

6.1.11. 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 email legítimas estão marcados 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 email à sua lista de Amigos. As mensagens de email 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 email de onde você recebe tais mensagens à lista de Amigos.

- Uma parte significante 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, vá para "*Clientes de email e protocolos suportados*" (p. 94).

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 email 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 emails 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 em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTISPAM**, clique em **Gerenciar amigos**.

   Uma janela de confirmação aparecerá.

3. Digite o endereço de e-mail onde deseja sempre receber as mensagens de email e depois clique em **Adicionar**. Pode adicionar quantos endereços de email desejar.
4. Clique em **OK** para guardar as alterações e fechar a janela.

Indica os erros de detecção

Se você está usando um cliente de email 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 emails 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 email 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, vá para "*Clientes de email e protocolos suportados*" (p. 94).

2. Adicionar spammers à lista de Spammers. As mensagens de email 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 email 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 fácilmente 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 email. Siga esses passos:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.

2. No painel **ANTISPAM**, clique em **Gerenciar spammers**.

   Uma janela de confirmação aparecerá.

3. Digite o endereço de email do spammer e depois clique em **Adicionar**. Pode adicionar quantos endereços de email desejar.

4. 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 acessar o status da proteção antispam, clique em **Proteção** no menu de navegação da interface do Bitdefender. Verifique o painel **Antispam** para comprovar se a função está habilitada.

  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 email via protocolo POP3. Isso significa o seguinte:

  - Emails 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 email 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 email a partir de um servidor de correio. Se você não sabe o protocolo que o seu cliente de email utiliza para importar mensagens de email, pergunte à pessoa que configurou o seu cliente de email.

- 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. 300).

6.1.12. 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 Mais Ferramentas.
  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. 300).

6.1.13. 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 aparece.
  4. Aguarde o processo de desinstalação ser concluído e 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 aparece.
  5. Aguarde o processo de desinstalação ser concluído e 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 aparece.
  6. Aguarde o processo de desinstalação ser concluído e depois reinicie o seu sistema.

6.1.14. O meu sistema não reinicia após a instalação de Bitdefender

Se instalou o Bitdefender e não consegue reiniciar o seu sistema no modo normal, 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 mais sobre como fazer isso, por favor, acesse *"Como posso reiniciar no Modo de Segurança?"* (p. 65).
  2. Remove 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 aparece.
       d. Aguarde o processo de desinstalação ser concluído e depois reinicie o seu sistema.

e. 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 aparece.

  e. Aguarde o processo de desinstalação ser concluído e depois reinicie o seu sistema.

  f. 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 aparece.

  f. Aguarde o processo de desinstalação ser concluído e depois reinicie o seu sistema.

  g. 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 mais sobre como fazer isso, por favor, acesse "*Como posso reiniciar no Modo de Segurança?*" (p. 65).

  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 o processo de desinstalação ser concluído e 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 o processo de desinstalação ser concluído e 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 o processo de desinstalação ser concluído e 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 mais sobre como fazer isso, por favor, acesse "*Como posso reiniciar no Modo de Segurança?*" (p. 65).

2. Usar a opção de Restauro do Sistema do Windows para restaurar o computador para uma data anterior antes de instalar o produto Bitdefender.
3. Reinicie o sistema no modo normal e contate os nossos representantes do suporte conforme descrito na seção "*Solicite Ajuda*" (p. 300).

6.2. Remover ameaças do seu sistema

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

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

- "*Bitdefender Modo de Resgate (ambiente de resgate no Windows 10)*" (p. 184)
- "*O que fazer se o Bitdefender encontrar ameaças no seu computador?*" (p. 187)
- "*Como posso limpar uma ameaça em um arquivo?*" (p. 188)
- "*Como posso limpar uma ameaça de um arquivo de e-mail?*" (p. 190)
- "*O que fazer se eu suspeitar que um arquivo seja perigoso?*" (p. 191)
- "*O que são arquivos protegidos por senha no registro de análise?*" (p. 191)
- "*Quais são os itens ignorados no relatório de análise?*" (p. 192)
- "*O que são arquivos muito comprimidos no registro de análise?*" (p. 192)
- "*Por que é que o Bitdefender eliminou automaticamente um arquivo infectado?*" (p. 192)

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. 300).

6.2.1. Bitdefender Modo de Resgate (ambiente de resgate no Windows 10)

O **Modo de Resgate** é um recurso do Bitdefender que permite que você verifique e desinfete todas as partições do disco rígido dentro e fora do seu sistema operacional.

Quando o Bitdefender Total Security é instalado no **Windows 7, Windows 8 e Windows 8.1** e o arquivo de imagem do Modo de Resgate do Bitdefender baixado, o Modo de Resgate pode ser usado mesmo se você não conseguir iniciar o Windows.

No Windows 10, o Ambiente de Resgate do Bitdefender é integrado com o Windows RE, portanto, não há necessidade de baixar uma imagem do modo de resgate nesse sistema operacional.

Baixando a Imagem do Modo de Resgate do Bitdefender

Para poder usar o Modo de Resgate no **Windows 7, Windows 8 e Windows 8.1**, é necessário primeiro baixar seu arquivo de imagem da seguinte forma:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Modo de Resgate**.
3. Clique em **SIM** na janela de confirmação que aparece para reiniciar seu computador.

   Aguarde até que a Imagem do Modo de Resgate do Bitdefender seja 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.

> **Nota**
> Devido à integração com o ambiente de recuperação do Windows no **Windows 10**, não há necessidade de baixar uma Imagem do Modo de Resgate nesse sistema operacional.

Iniciando seu sistema no Modo de Resgate no Windows 7, Windows 8 e Windows 8.1

Você pode entrar no Modo de Recuperação de duas formas:

Na interface do Bitdefender

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Modo de Resgate**.
3. Clique em **SIM** na janela de confirmação que aparece para reiniciar seu computador.
4. 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.
5. 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:

- No **Windows 7**:
  1. Pressione a tecla **F8** até as **Opções Avançadas de Inicialização** aparecerem.
  2. Use as teclas de setas para selecionar o Modo de Resgate do Bitdefender, depois pressione **Enter**.

     O Modo de Recuperação do Bitdefender irá carregar dentro de alguns minutos.
- No **Windows 8 e Windows 8.1**:
  1. Pressione a tecla **Shift** até as **Opções Avançadas de Inicialização** aparecerem.
  2. Selecione a opção **Usar outro sistema operacional**, e depois Modo de Resgate do Bitdefender.

     O Modo de Recuperação do Bitdefender irá carregar dentro de alguns minutos.

Nota
Só é possível iniciar seu computador no Modo de Resgate se a Imagem do Modo de Resgate tiver sido previamente baixada, como descrito em "Baixando a Imagem do Modo de Resgate do Bitdefender" (p. 184).

Iniciando seu sistema no Ambiente de Resgate do Windows 10

Você pode entrar no Ambiente de Resgate somente a partir do seu Bitdefender da seguinte forma:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Ambiente de Resgate**.
3. Clique em **Reiniciar** na janela que aparece.

   O Ambiente de Resgate do Bitdefender carrega em alguns instantes.

Verificando seu sistema no Modo de Resgate (Ambiente de Resgate no Windows 10)

Para verificar seu sistema no Modo de Resgate (Ambiente de Resgate):

- No **Windows 7, Windows 8 e Windows 8.1**:

  1. Entre no Modo de Recuperação, conforme descrito em "Iniciando seu sistema no Modo de Resgate no Windows 7, Windows 8 e Windows 8.1" (p. 184).
  2. O logo do Bitdefender surgirá e os motores da solução de segurança começarão a ser copiados.
  3. Uma janela de boas-vindas aparecerá. Clique em **Continuar**.
  4. Uma atualização do banco de dados de informações de ameaças começou.
  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. Se qualquer ameaça for detectada, siga as instruções para removê-la.
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.

- No **Windows 10**:

1. Entre no Ambiente de Resgate, como descrito em "Iniciando seu sistema no Ambiente de Resgate do Windows 10" (p. 186).
2. O processo de verificação do Bitdefender começa automaticamente assim que o sistema for carregado no Ambiente de Resgate.
3. Aguarde o término da análise. Se qualquer ameaça for detectada, siga as instruções para removê-la.
4. Para sair do Ambiente de Resgate, clique no botão **SAIR** na janela com os resultados da verificação.

6.2.2. O que fazer se o Bitdefender encontrar ameaças no seu computador?

Você poderá descobrir que tem uma ameaça no seu computador de uma das seguintes formas:

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

Nessas situações, atualize o Bitdefender para se certificar de que possui o banco de dados mais recentes de informações sobre a ameaça 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 e 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 em **Proteção** no menu de navegação da interface do Bitdefender.
   b. No painel **ANTIVIRUS**, clique em **Configurações**.
   c. Na janela **Escudo**, desative o **Escudo do Bitdefender**.
2. Mostrar objetos ocultos no Windows. Para saber mais sobre como fazer isso, por favor, acesse "*Como posso mostrar objetos ocultos no Windows?*" (p. 63).
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 mais sobre como fazer isso, por favor, acesse "*Como posso reiniciar no Modo de Segurança?*" (p. 65).
2. Mostrar objetos ocultos no Windows. Para saber mais sobre como fazer isso, por favor, acesse "*Como posso mostrar objetos ocultos no Windows?*" (p. 63).
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 contatar a Bitdefender para suporte, como descrito na seção "*Solicite Ajuda*" (p. 300).

6.2.3. Como posso limpar uma ameaça em um 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 ameaças no interior, mas não pode aplicar outras ações.

Se o Bitdefender avisar que foi detectado uma ameaça dentro de um arquivo e não estiver disponível uma ação, significa que não é possível remover a ameaça devido a restrições nas definições de permissão do arquivo.

Pode limpar uma ameaça armazenada num arquivo da seguinte forma:

1. Identifique o arquivo que contém a ameaça ao realizar uma Análise Completa do sistema.
2. Desative a proteção antivírus em tempo real do Bitdefender:
   a. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
   b. No painel **ANTIVIRUS**, clique em **Configurações**.
   c. Na janela **Escudo**, desative o **Escudo do Bitdefender**.
3. Vá à localização do arquivo e descomprima-o com uma aplicação de arquivo, como o WinZip.
4. Identifique e elimine o 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 uma ameaça armazenada num arquivo não é uma ameaça imediata ao seu sistema, pois a ameaça deve ser descompactada e executada 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. 300).

6.2.4. Como posso limpar uma ameaça de um arquivo de e-mail?

O Bitdefender também pode identificar ameaças em bancos de dados de e-mail e arquivos de e-mail armazenados no disco.

Por vezes, é necessário identificar a mensagem infectada com a informação fornecida no relatório da análise, e elimine-o manualmente.

Assim é como você pode limpar uma ameaça armazenada em um arquivo de e-mail:

1. Analisar a base de dados do correio eletrônico com o Bitdefender.
2. Desative a proteção antivírus em tempo real do Bitdefender:
   a. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
   b. No painel **ANTIVIRUS**, clique em **Configurações**.
   c. Na janela **Escudo**, desative o **Escudo do Bitdefender**.
3. Abra o relatório da análise e utilize a informação de identificação (Assunto, De, Para) das mensagens infectadas para localizá-las no cliente de correio 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 2010/2013/2016: 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. 300).

6.2.5. 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 mais sobre como fazer isso, por favor, acesse "*Como posso analisar o meu sistema?*" (p. 45).
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 mais sobre como fazer isso, por favor, acesse "*Solicite Ajuda*" (p. 300).

6.2.6. 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.

6.2.7. 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.

6.2.8. 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 desencriptação 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.

6.2.9. Por que é que o Bitdefender eliminou automaticamente um arquivo infectado?

Se for detectado um arquivo infectado, o Bitdefender tentará automaticamente desinfectá-lo. Se a desinfecção falhar, o arquivo é movido para a quarentena de modo a restringir a infecção.

Para determinados tipos de ameaças, a desinfecção não é possível porque o arquivo detectado é totalmente malicioso. 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 PARA MAC

7. INSTALAÇÃO E REMOÇÃO

Este capítulo inclui os seguintes tópicos:

7.1. Requisitos de Sistema

Você pode instalar o Bitdefender Antivirus for Mac em computadores Macintosh com OS X Yosemite (10.10.5), OS X El Capitan (10.11.6), macOS Sierra (10.12.6), macOS High Sierra (10.13.6) ou macOS Mojave (10.14 ou superior).

Espaço mínimo necessário de 1 GB 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 macOS 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 **Relatório de Sistema** para informações detalhadas de hardware.

7.2. Instalando o Bitdefender Antivirus for Mac

O aplicativo do Bitdefender Antivirus for Mac pode ser instalado a partir da sua conta Bitdefender da seguinte forma:

1. Faça login como administrador.
2. Acesse: https://central.bitdefender.com.
3. Entre na sua conta Bitdefender usando seu endereço de e-mail e senha.
4. Selecione o painel **Meus Dispositivos**, e clique em **INSTALAR PROTEÇÃO**.
5. Escolha uma das duas opções disponíveis:
   - **Proteja este dispositivo**

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

b. Guarde o arquivo de instalação.

- **Proteja outros dispositivos**

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

b. Pressione **ENVIAR LINK DE DOWNLOAD**.

c. Digite um endereço de email no campo correspondente e clique em **ENVIAR EMAIL**.

Observe que o link de download gerado será válido apenas durante as próximas 24 horas. Se o link expirar, você precisará gerar um novo seguindo os mesmos passos.

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

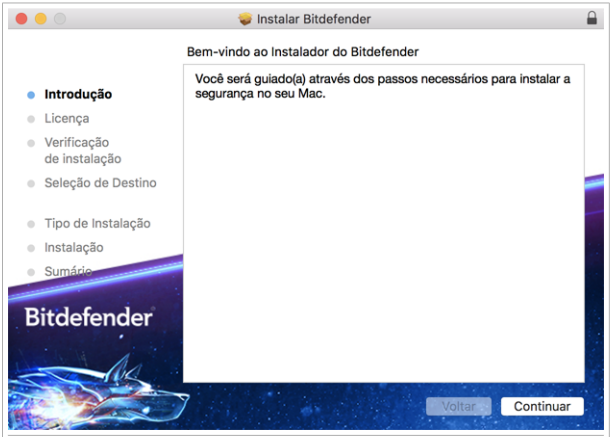
6. Execute o Bitdefender que você baixou.
7. Complete os passos de instalação.

7.2.1. 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



Janela de Boas-Vindas

Clique em **Continuar**.

Passo 2 - Leia o Acordo de Assinatura

Ler o Acordo de Assinatura

Antes de continuar o processo de instalação, você deve concordar com o Acordo de Assinatura. Por favor, leia o cordo de Assinatura com calma, já

que ele contém os termos e condições segundo os quais você pode usar o Bitdefender Antivirus for Mac.

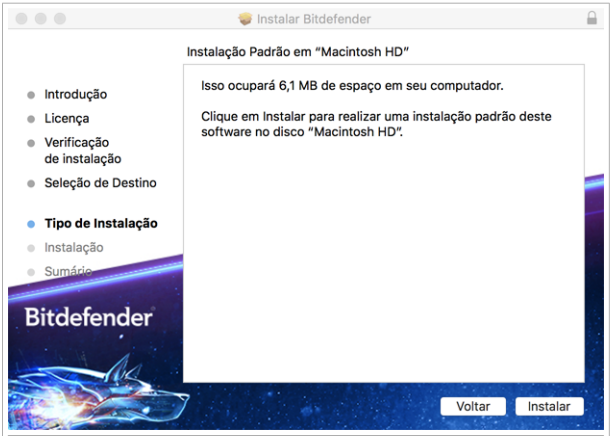
Nesta janela, você também pode selecionar o idioma no qual você deseja instalar o produto.

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

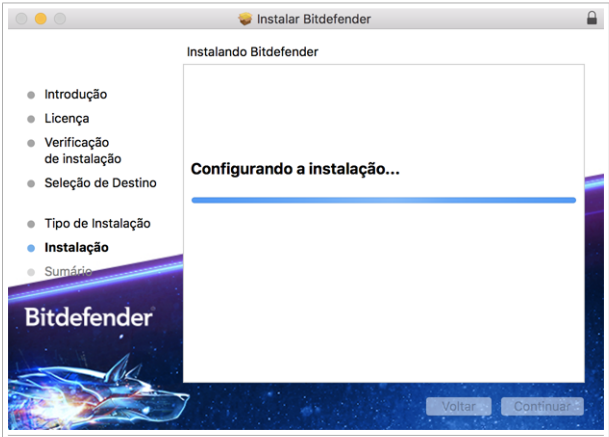


Iniciar a Instalação

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.

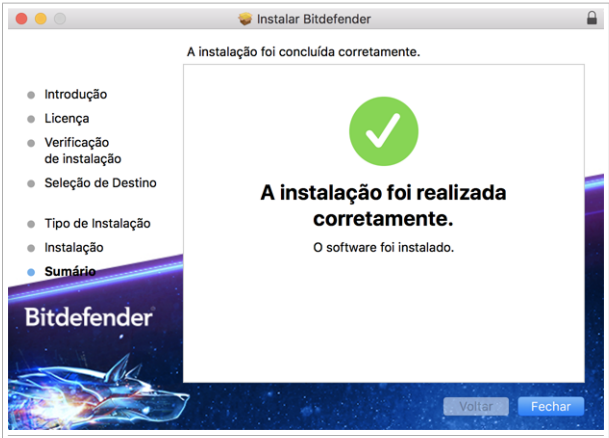
Passo 4 - Instalando o Bitdefender Antivirus for Mac



Instalando o Bitdefender Antivirus for Mac

Aguarde a instalação ser concluída e clique em **Continuar**.

Passo 5 - Terminar



Terminar

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

O processo de instalação agora está completo.

Importante

- Se você está instalando o Bitdefender Antivirus for Mac no macOS versão High Sierra 10.13.0 ou superior, a notificação **System Extension Blocked** é exibida. A notificação informa que as extensões assinadas por Bitdefender foram bloqueadas e devem ser habilitadas manualmente. Clique **OK** para continuar. Na janela Bitdefender Antivirus for Mac que é exibida, clique no link **Security & Privacy**. Clique em **Permitir** na parte inferior da janela ou selecione Bitdefender SRL na lista, e depois clique em **ACEITAR**.
- Se você está instalando o Bitdefender Antivirus for Mac no macOS Mojave 10.14 ou superior, aparecerá uma notificação. Essa notificação informa que você deve permitir que o Bitdefender Antivirus for Mac carregue seus arquivos no seu sistema. Para continuar, selecione o link de **Segurança & Privacidade** e clique em **ACEITAR**. Clique em **Permitir** ao lado de Bitdefender SRL.

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 janerla do **Finder** e vá para a pasta de Aplicações.
2. Abra a pasta do Bitdefender e clique duas vezes sobre o botão Desinstalar Bitdefender.
3. Clique em **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 “Contate-nos” (p. 299).

8. INTRODUÇÃO

Este capítulo inclui os seguintes tópicos:

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 ("ameaças"), incluindo:

- ransomware
- adware
- Vírus
- Spyware
- Cavalos de Troia
- keyloggers
- worms

Este aplicativo detecta e remove não só ameaças para Mac, mas também 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.

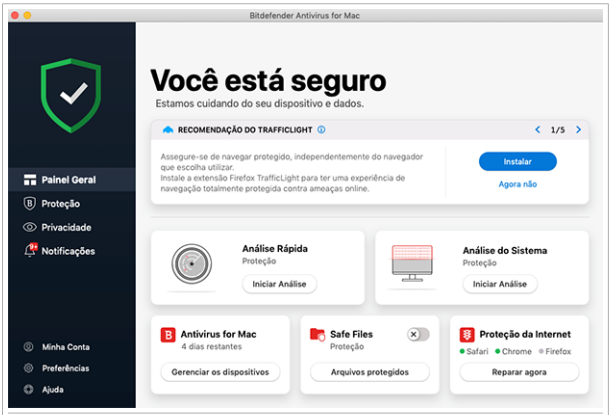
Importante

A primeira vez que você abrir o Bitdefender Antivirus for Mac no macOS Mojave 10.14 ou superior, aparecerá uma recomendação de segurança. Essa recomendação aparece porque nós precisamos de permissões para fazer uma verificação completa do seu sistema em busca de ameaças. Para dar permissões, você precisa ter iniciado sessão como administrador e seguir esses passos:

1. Clique no link **Preferências do Sistema**.
2. Clique no ícone e insira as credenciais de administrador.
3. Uma nova janela aparece. Arraste o arquivo **BDLDaemon** até a lista de aplicativos permitidos.

8.3. A Janela Principal

Bitdefender Antivirus for Mac 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.



A Janela Principal

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 o ícone do ângulo direito para continuar sendo guiado, ou **Pular guia** para fechar o assistente.

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 vermelho. Para informações detalhadas sobre problemas e como repará-los, acesse "*Reparando Incidências*" (p. 215).

Para lhe oferecer uma operação efetiva e proteção reforçada enquanto realiza diferentes atividades, o **Bitdefender** Autopilot agirá como o seu consultor de segurança pessoal. Dependendo da atividade que você realizar, seja trabalhar ou fazer pagamentos online, o Bitdefender Autopilot fornecerá recomendações contextuais com base no uso e necessidades do seu dispositivo. Isso irá ajudá-lo a descobrir e se beneficiar das vantagens trazidas pelos recursos inclusos no aplicativo Bitdefender Antivirus for Mac.

Você pode acessar as seções da Bitdefender no menu de navegação à esquerda para uma configuração mais detalhada das tarefas de administração avançadas (abas **Proteção** e **Privacidade**), notificações, sua conta Bitdefender e a área de Preferências. Você também pode nos contatar (aba **Ajuda**) para obter suporte caso tenha perguntas ou algo inesperado apareça.

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 proporciona uma forma fácil de procurar por ameaças em arquivos e pastas. Basta arrastar e soltar o arquivo ou pasta no ícone do Dock e a verificação iniciará imediatamente.

Ícone no Dock

8.5. Menu de navegação

No lado esquerdo da interface da Bitdefender está o menu de navegação, que lhe permite acessar rapidamente os recursos e ferramentas do Bitdefender que você precisa para utilizar seu produto. As abas disponíveis nesta área são:

- **Painel**. Aqui você pode solucionar problemas de segurança rapidamente, visualizar recomendações de acordo com as necessidades e uso do seu dispositivo, realizar ações rápidas e acessar sua conta Bitdefender para gerenciar os dispositivos que você adicionou à sua assinatura da Bitdefender.
- **Proteção**. Aqui você pode executar verificações de antivírus, adicionar arquivos às listas de exceções, proteger arquivos e aplicativos contra ataques de ransomware, proteger seus backups com a Proteção da Máquina do Tempo e configurar a proteção enquanto navega na internet.
- **Privacidade**. Aqui, você pode abrir o aplicativo do Bitdefender VPN e instalar a extensão do Antitracker no seu navegador.
- **Notificações**. Aqui você pode visualizar as ações realizadas nos arquivos verificados.
- **Minha conta**. Daqui, você pode acessar sua conta Bitdefender para verificar suas assinaturas e realizar tarefas de segurança nos dispositivos que você gerencia. Detalhes sobre a conta Bitdefender e assinatura em uso também estão disponíveis.
- **Preferências**. Aqui você pode alterar as configurações do Bitdefender.
- **Ajuda**. Aqui você pode entrar em contato com o departamento de Suporte Técnico sempre que precisar de assistência com seu produto Bitdefender. Você também pode mandar feedback para melhorar o produto.

8.6. Modo Escuro

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

9. PROTEGENDO CONTRA SOFTWARES MALICIOSOS

Este capítulo inclui os seguintes tópicos:

9.1. Melhores Práticas

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

- Mantenha o **Bitdefender Escudo** ligado para permitir que os arquivos do sistema sejam verificados automaticamente pelo Bitdefender Antivirus for Mac.
- Mantenha seu Bitdefender Antivirus for Mac atualizado com as informações sobre ameaças e atualizações de produto mais recentes.
- Confira e repare os problemas relatados pelo Bitdefender Antivirus for Mac regularmente. Para informações detalhadas, acesse "*Reparando Incidências*" (p. 215).
- Confira o registro detalhado de eventos em relação à atividade do Bitdefender Antivirus for Mac no seu computador. Sempre que acontecer algo relevante para a segurança do seu sistema ou dados, uma nova

mensagem será adicionada à área de notificações do Bitdefender. Para mais detalhes, acesse "*Notificações*" (p. 217).

- 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. 220).

9.2. Verificando seu Mac

Além da ferramenta **Escudo da Bitdefender**, que continuamente monitora os aplicativos instalados regularmente à procura de ações típicas de ameaças e previne que novas ameaças 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. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. Selecione a aba **Antivírus**.
3. Clique em um dos três botões para iniciar a verificação desejada.
   - **Verificação Rápida** - procura por ameaças 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 ameaças 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 de Exceções na janela de Proteção.

- **Verificação Personalizada** - ajuda a procurar por ameaças em arquivos, pastas ou volumes específicos.

Você também pode iniciar uma Verificação de Sistema ou Verificação Rápida no painel de controle.

9.3. Assistente de Análise

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

Verificação em processo

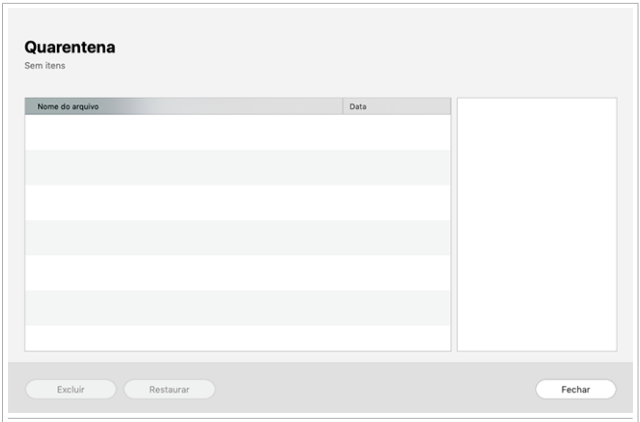
Informações em tempo real sobre as ameaças detectadas e resolvidas são exibidas durante cada verificação.

Espere que o Bitdefender Antivirus for Mac termine a análise.

Nota
O processo de análise pode demorar algum tempo, dependendo da complexidade da mesma.

9.4. Quarentena

O Bitdefender Antivirus for Mac permite isolar os arquivos infectados ou suspeitos em uma área segura, chamada quarentena. Quando a ameaça está na quarentena não pode prejudicar de nenhuma maneira, porque não pode ser executada ou lida.



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**.

Para visualizar a lista de itens adicionados à quarentena:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. A janela **Antivírus** se abre.

   Clique em **Abrir** no painel de **Quarentena**.

9.5. Escudo da Bitdefender (proteção em tempo real)

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

Para desativar a proteção em tempo real:

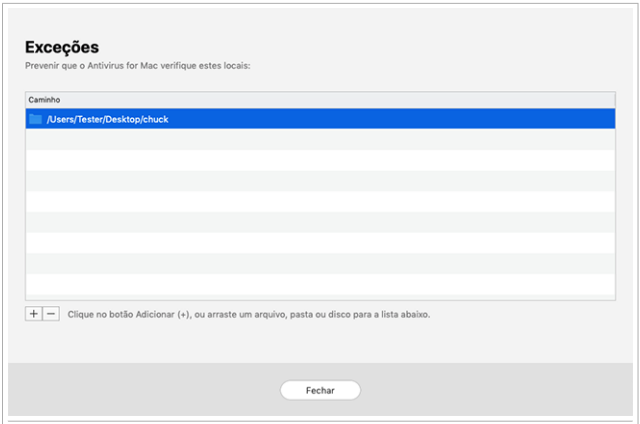
1. Clique em **Preferências** no menu de navegação da interface do Bitdefender.
2. Desligue o **Bitdefender Shield** na janela de **Proteção**.

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

9.6. Exceções 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



Exceções de Análise

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

Para acessar a lista de exceções:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. A janela **Antivírus** se abre.

   Clique em **Abrir** no painel de **Exceções**.

Há duas formas de configurar uma exceção de verificação:

- Arraste e solte um arquivo, pasta ou volume na lista de exceções.
- Clique no botão com o sinal de mais (+), localizado abaixo da lista de exceções. A seguir, escolha o arquivo, pasta ou volume a ser excluído da verificação.

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

9.7. Proteção na Web

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.

Habilitando extensões do TrafficLight

Para ativar as extensões do TrafficLight:

1. Clique em **Resolver agora** no cartão de **Proteção web** no Painel de Controle.
2. A janela de **Proteção na Web** se abre.

   O navegador detectado instalado no seu sistema aparecerá. Para instalar a extensão do TrafficLight no seu navegador, clique em **Obter Extensão**.
3. Você vai ser redirecionado para:

   http://bitdefender.com/solutions/trafficlight.html
4. Selecione **Download grátis**.
5. Siga estes passos para instalar a extensão do TrafficLight correspondente ao seu navegador.

Gerenciando configurações de extensões

Uma variedade de recursos está disponível para protegê-lo de todas as formas de amaças que você pode encontrar enquanto navega na internet. Para acessá-los, clique no ícone do TrafficLight próximo às configurações do navegador, e depois clique em **Configurações**:

- **Configurações do Bitdefender TrafficLight**
  - Filtro Avançado de Ameaças - previne que você acesse websites usados para ataques de malware, phishing e fraude.
  - Detector de rastreadores - detecta rastreadores em páginas visitadas e o informa sobre sua presença.
  - Analisador de Resultados de Busca - proporciona alertas antecipados de websites de risco nos seus resultados de busca.

    Caso todas as configurações estejam desativadas, nenhuma página será verificada.
- **Lista Segura**

  As páginas podem ser excluídas da verificação pelos motores do Bitdefender. No campo correspondente, digite o nome do website que deseja adicionar à lista e depois clique em **ADICIONAR**.

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

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 da página imediatamente pois ela contém malware ou outras ameaças.

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

9.8. Anti-tracker

Uma grande parte dos sites que você utiliza usa rastreadores para coletar informação sobre seu comportamento para compartilhar com empresas ou para mostrar publicidade direcionada para você. Com isso, os donos dos sites ganham dinheiro por proporcionar conteúdo de graça ou para continuarem operando. Além de coletar informação, os rastreadores podem desacelerar sua navegação ou desperdiçar sua banda larga.

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

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

- Google Chrome
- Mozilla Firefox
- Safari

Os rastreadores que detectamos estão divididos nas seguintes categorias:

- **Publicidade** - usados para analisar o tráfego do site, o comportamento do usuário ou os padrões de tráfego dos visitantes.

- **Interação com o cliente** - usados para medir a interação com o usuário através de diferentes formas de entrada, como chat ou suporte.
- **Essenciais** - usados para monitorar funcionalidades críticas do site.
- **Analíticas do site** - usados para coletar dados sobre o uso do site.
- **Mídia social** - usados para monitorar o público em mídias sociais, suas atividades e o engajamento dos usuários nas diferentes plataformas de mídias sociais.

Activando o Bitdefender Antitracker

Para activar a extensão do Antitracker da Bitdefender no seu navegador:

1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
2. Selecione a aba **Antitracker**.
3. Clique em **Habilitar extensão** no navegador em que pretende ativar a extensão.

9.8.1. Interface do Antitracker

Ao ativar a extensão do Antitracker da Bitdefender, o ícone  aparece ao lado da barra de pesquisa no seu navegador. Cada vez que você visitar um site, vai aparecer um contador no ícone referente aos rastreadores detectados e bloqueados. Para visualizar mais detalhes sobre os rastreadores bloqueados, clique no ícone para abrir a interface. Além do número de rastreadores bloqueados, você pode visualizar o tempo que a página precisa para carregar e as categorias às quais os rastreadores pertencem. Para visualizar a lista de sites que estão rastreando, clique na categoria desejada.

Para impedir que o Bitdefender bloqueie rastreadores no site que você está visitando, clique em **Pausar proteção neste site**. A configuração se aplica somente enquanto você tiver o site aberto, e volta ao estado inicial ao fechar o site.

Para permitir que os rastreadores de uma categoria específica monitorizem sua atividade, clique na atividade desejada, e a seguir, no botão correspondente. Se mudar de ideia, clique no mesmo botão novamente.

9.8.2. Desligar o Antitracker da Bitdefender

Para desligar o Antitracker da Bitdefender no seu navegador:

1. Abra seu navegador da web.
2. Clique no ícone ao lado da barra de endereços no seu navegador.
3. Clique no ícone no canto superior direito.
4. Use a chave correspondente para desativá-lo.

   O ícone do Bitdefender fica cinza.

9.8.3. Permitir o rastreamento do site

Se você deseja ser rastreado ao visitar um site em particular, você pode adicionar seu endereço às excepções da seguinte forma:

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

   Se você deseja adicionar outro site, digite o endereço no campo correspondente, e a seguir, clique em .

9.9. Safe Files

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.

Utilizando a última tecnologia, a Bitdefender assegura a integridade do sistema ao proteger suas áreas essenciais contra ataques de ransomware sem prejudicar seu desempenho. Contudo, você pode desejar proteger seus arquivos pessoais, como documentos, fotos ou filmes, contra o acesso de aplicativos não confiáveis. Utilizando a última tecnologia, a Bitdefender assegura a integridade do sistema ao proteger suas áreas essenciais contra ataques de ransomware sem prejudicar seu desempenho.

Para adicionar arquivos ao ambiente protegido posteriormente:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. Selecione a aba **Antiransomware**.
3. Clique em **Arquivos protegidos** na área de arquivos seguros.
4. Clique no botão com o sinal de mais (+), localizado abaixo da lista de arquivos protegidos. Depois, escolha o arquivo, pasta ou volume a ser protegido caso ataques de ransomware tentem acessá-lo.

Para evitar a lentidão do sistema, recomendamos que adicione no máximo 30 pastas, ou salve múltiplos arquivos em uma única pasta.

As configurações de fábrica já protegem as pastas Imagens, Documentos, Área de Trabalho e Downloads.

Nota
Pastas personalizadas somente podem ser protegidas para os usuários atuais. Drives externos, arquivos de sistema e de aplicativos não podem ser adicionados ao ambiente de proteção.

Você será informado sempre que um aplicativo desconhecido com um comportamento incomum tentar modificar os arquivos que você adicionou. Clique em **Permitir** ou **Bloquear** para adicioná-lo à lista Gerenciamento de aplicativos.

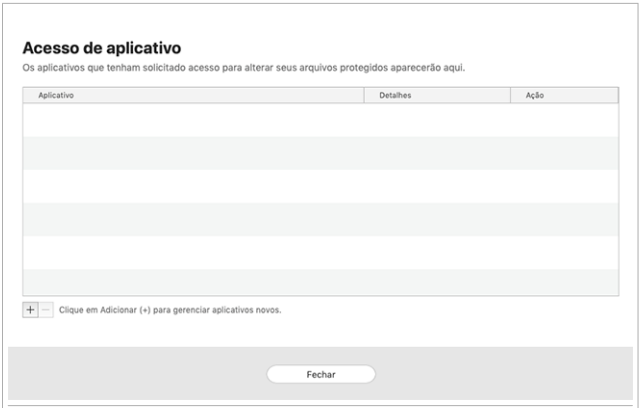
9.9.1. Gerenciamento de aplicativos

As aplicações que tentam mudar ou apagar arquivos protegidos podem ser sinalizadas como potencialmente inseguras e adicionadas à lista de aplicações bloqueadas. Se um aplicativo como esse for bloqueado e você tiver certeza de que seu comportamento é normal, pode permitir seu acesso seguindo estes passos:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. Selecione a aba **Antiransomware**.
3. Clique em **Acesso ao aplicativo** na área de arquivos seguros.
4. Mudar o estado para Permitir, ao lado do aplicativo bloqueado.

Os aplicativos configurados como “Permitir” também podem ser configurados como “Bloqueado”.

Use o método de arrastar e soltar ou clique no símbolo de mais (+) para adicionar mais aplicativos à lista.



Safe Files

9.10. Time Machine Protection

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.

Caso você precise restaurar os itens de um backup da Máquina do Tempo, confira a página de suporte da Apple para ver as instruções.

Ativar ou desativar a Proteção da Máquina do Tempo

Ativar ou desativar a Proteção da Máquina do Tempo:

1. Clique em **Proteção** no menu de navegação da interface do **Bitdefender**.
2. Selecione a aba **Antiransomware**.
3. Selecione ou desmarque o botão de **Proteção da Máquina do Tempo**.

9.11. 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.

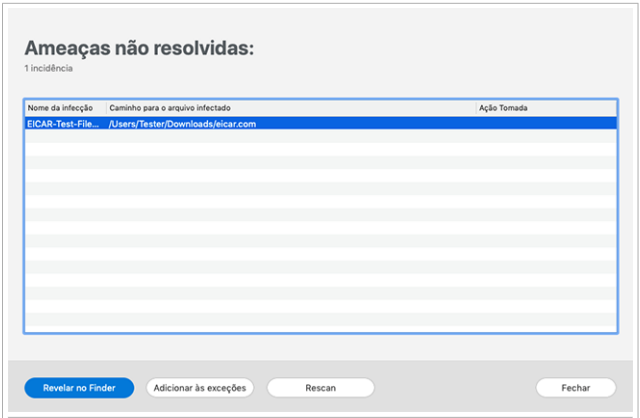
Reparar os problemas indicados pelo Bitdefender Antivirus for Mac é uma forma rápida e fácil de garantir a melhor proteção do seu sistema e dados.

Os problemas detectados incluem:

- A atualização de informações sobre ameaças não foi baixada dos nossos servidores.
- Ameaças foram detectadas no seu sistema e o produto não pode desinfectá-las automaticamente.
- A proteção em tempo real está desabilitada.

Para verificar e reparar os problemas detectados:

1. 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 vermelho.
2. Confira a descrição para mais informações.
3. Quando um problema é detectado, clique no botão correspondente para realizar uma ação.



Janela de ameaças não resolvidas

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

Você pode escolher as seguintes ações para ameaças não resolvidas:

- Apagar manualmente. Escolha essa ação para remover as infecções manualmente.
- Adicionar às Exceções. Essa ação não está disponível para ameaças encontradas dentro de arquivos.

9.12. 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 alguma ameaça ou vulnerabilidade fori encontrada no seu computador, etc. Adicionalmente, pode tomar outras ações se necessário ou alterar ações tomadas pelo Bitdefender.

Para acessar as notificações, clique em **Notificações** no menu de navegação 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.

9.13. Atualizações

Novas ameaças são achadas e identificadas todos os dias. Por isso é muito importante manter o Bitdefender Antivirus for Mac atualizado com as informações de ameaças mais recentes.

As atualizações de informações sobre ameaças são executadas na hora, ou seja, os arquivos que precisam ser atualizados são substituídos progressivamente. Dessa forma, a atualização não afetará a operação do produto, e ao mesmo tempo, qualquer vulnerabilidade será eliminada.

- Se o Bitdefender Antivirus for Mac estiver atualizado, pode 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 as ameaças mais recentes descobertas pelos laboratórios da Bitdefender.

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

Alternativamente, você pode solicitar uma atualização manualmente ao pressionar CMD + U.

Você pode ver o progresso de atualização e arquivos baixados.

9.13.2. 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 informações sobre ameaças.

9.13.3. 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.

9.13.4. Encontrando mais informações sobre o Bitdefender Antivirus for Mac

Para encontrar mais informações sobre a versão do Bitdefender Antivirus for Mac que você tem instalada, acesse a janela **Informação**. Na mesma janela, você pode acessar e ver o Acordo de Assinatura, a Política de Privacidade e as licenças Open-source.

Para acessar a seção Informação:

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

10. CONFIGURANDO PREFERÊNCIAS

Este capítulo inclui os seguintes tópicos:

10.1. Acessando as preferências

Para abrir a janela de preferências do Bitdefender Antivirus for Mac:

1. Faça uma das seguintes:
   - Clique em **Preferências** no menu de navegação da interface do Bitdefender.
   - Clique em Bitdefender Antivirus for Mac na barra de menu e escolha **Preferências**.
   - Pressione Command-Vírgula(,).

10.2. 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.

- **Escudo da Bitdefender.** O Escudo da Bitdefender fornece uma proteção contínua e em tempo real contra uma ampla variedade de ameaças ao verificar todos os arquivos instalados, suas versões atualizadas e arquivos novos e modificados. Não recomendamos que você desligue o Escudo da Bitdefender, mas se for necessário, faça-o pelo tempo mais curto possível. Se o Escudo da Bitdefender estiver desligado, você não estará protegido contra ameaças.
- **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 uma ação coletiva para todos os problemas e itens suspeitos achados durante o processo de verificação.

- **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.

10.3. Preferências avançadas

Você pode escolher uma ação coletiva para todos os problemas e itens suspeitos achados durante o processo de verificação.

Ação para itens infectados

Tente desinfetar ou mover para quarentena - Se forem detectados arquivos infectados, o Bitdefender tentará desinfetá-los (eliminar o código malicioso) ou colocá-los em quarentena.

Não fazer nada - Nada será feito com os arquivos detectados.

Ação para itens suspeitos

Colocar arquivos em quarentena - Se arquivos suspeitos forem detectados, o Bitdefender irá colocá-los em quarentena.

Não fazer nada - Nada será feito com os arquivos detectados.

10.4. Ofertas Especiais

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.

Para ativar ou desativar notificações de ofertas especiais:

1. Clique em **Preferências** no menu de navegação da interface do Bitdefender.
2. Selecione a aba **Outros**.
3. Ative ou desative o botão **Minhas ofertas** .

A opção **Minhas ofertas** aparece ativa como definição padrão.

11. VPN

Este capítulo inclui os seguintes tópicos:

11.1. Sobre o VPN

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

O VPN funciona como um túnel entre o seu dispositivo e a rede à qual você se conecta, protegendo sua conexão, criptografando seus dados usando criptografia de nível bancário e escondendo seu endereço IP onde quer que esteja. Seu tráfego é redirecionado por meio de um servidor separado, tornando seu dispositivo quase impossível de ser identificado dentre os incontáveis dispositivos que usam nossos serviços. Além disso, enquanto estiver conectado à internet com o Bitdefender VPN, você pode acessar conteúdos que normalmente são restritos em áreas específicas.

Nota

Alguns países censuram a internet e, portanto, o uso de VPNs em seus territórios foi banido por lei. Para evitar consequências legais, uma mensagem de aviso pode aparecer ao tentar usar o aplicativo Bitdefender VPN pela primeira vez. Ao continuar a usar esse aplicativo, você confirma que está ciente das regulamentações aplicáveis e dos riscos aos quais você pode estar exposto.

11.2. Abrindo o VPN

Existem três formas de abrir o aplicativo do Bitdefender VPN:

- Clique em **Privacidade** no menu de navegação da interface do **Bitdefender**. Clique em **Abrir** no cartão do Bitdefender VPN.

- Clique no ícone na barra do menu.
- Acesse a pasta de Aplicativos, abra a pasta do Bitdefender e clique duas vezes sobre o ícone do Bitdefender VPN.

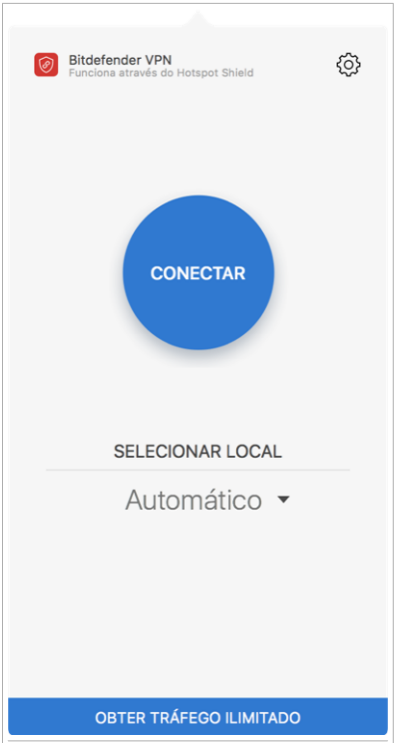
A primeira vez que abrir o aplicativo, será solicitada permissão para que o Bitdefender possa adicionar configurações. Ao permitir que o Bitdefender adicione configurações, você concorda que a atividade da rede do seu dispositivo poderá ser filtrada ou monitorada ao usar o aplicativo do VPN.

Nota
O aplicativo do Bitdefender VPN só poderá ser instalado em macOS Sierra (10.12.6), macOS High Sierra (10.13.6) ou macOS Mojave (10.14 ou superior).

11.3. Interface

A interface do VPN exibe o status do aplicativo, conectado ou desconectado. O local do servidor para usuários com a versão gratuita é determinado automaticamente pelo Bitdefender para o servidor mais adequado, enquanto os usuários Premium têm a possibilidade de alterar o local do servidor ao qual desejam se conectar selecionando-o na lista **SELECIONAR LOCAL**. Para detalhes sobre as assinaturas de VPN, acesse "*Assinaturas*" (p. 225).

Para conectar ou desconectar, basta clicar no status exibido no topo da tela. A barra de menu fica preta quando o VPN está conectado e branca quando o VPN está desconectado.



Interface do VPN

Enquanto estiver conectado, o tempo transcorrido é mostrado na parte inferior da interface. Para acessar mais opções, clique no ícone ⚙ no canto superior direito:

- **Minha conta** - detalhes sobre a sua conta Bitdefender e a assinatura do VPN são exibidos. Clique em **Trocar conta** se deseja entrar com outra conta.
- **Configurações** - dependendo das suas necessidades, você pode personalizar o comportamento do seu produto:
  - configure o VPN para que seja executado na inicialização do sistema
  - receba notificações quando o VPN se conectar ou desconectar automaticamente

- **Atualizar para o Premium** - Se você está usando a versão gratuita, pode atualizar para o plano Premium aqui. Clique em **ATUALIZAR AGORA** para ser redirecionado para uma página da web de onde você pode comprar a assinatura.
- **Suporte** - você é redirecionado para a nossa plataforma do Centro de Suporte onde poderá ler um artigo útil sobre como utilizar o Bitdefender VPN.
- **Sobre** - são apresentadas informações sobre a versão instalada.
- **Sair** - saia do aplicativo.

11.4. Assinaturas

O Bitdefender VPN oferece gratuitamente uma quota de tráfego diário de 200 MB por dispositivo para proteger a conexão sempre que a sua equipe precisar.

Para obter tráfego ilimitado e acesso irrestrito a conteúdos no mundo todo podendo escolher um local de servidor da escolha da sua equipe, atualize para a versão premium.

Você pode atualizar para a versão do Bitdefender Premium VPN em qualquer momento no painel **Minhas assinaturas** disponível na conta do seu Bitdefender.

A assinatura do Bitdefender Premium VPN é independente da assinatura do Bitdefender Small Office Security, ou seja, você poderá usá-lo durante todo o seu período de validade. Caso a assinatura do Bitdefender Premium VPN expire e a do Bitdefender Small Office Security continue ativa, você voltará para o plano gratuito.

O Bitdefender VPN é um produto multiplataforma, disponível nos produtos Bitdefender compatíveis com Windows, macOS, Android e iOS. Quando você atualizar para o plano Premium, poderá usar sua assinatura em todos os seus produtos, desde que faça login com a mesma conta Bitdefender.

12. BITDEFENDER CENTRAL

Este capítulo inclui os seguintes tópicos:

- "*Sobre Bitdefender Central*" (p. 226)
- "*Minhas assinaturas*" (p. 229)
- "*Meus dispositivos*" (p. 230)

12.1. Sobre Bitdefender Central

Bitdefender Central é a plataforma 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, acessando https://central.bitdefender.com, ou diretamente pelo aplicativo da Bitdefender Central em dispositivos Android e iOS.

Para instalar o aplicativo da Bitdefender Central nos seus dispositivos:

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

Assim que fizer login, você pode começar a fazer o seguinte:

- Faça o download e instale o Bitdefender nos sistemas operacionais Windows, macOS, iOS e Android. Os produtos disponíveis para download são:
  - Bitdefender Antivirus for Mac
  - A linha de produtos Windows da Bitdefender
  - Bitdefender Mobile Security para Android
  - Bitdefender Mobile Security para iOS
- Controlar e renovar suas assinaturas do Bitdefender.
- Adicionar novos dispositivos à sua rede e controlar suas funções de onde quer que você esteja.

12.2. 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. Entre na sua conta usando seu endereço de e-mail e senha.
- Em seu dispositivo Android ou iOS:

  Abra o aplicativo da Bitdefender Central que você instalou.

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

12.3. Autenticação de dois fatores

O método de autenticação em 2 fatores adiciona uma camada extra de segurança à sua conta do Bitdefender, ao requerer um código de autenticação além das credenciais de login. Assim, você impedirá o roubo da conta e afugentará diversos tipos de ciberataques, como keyloggers, ataques de força bruta e de dicionário.

Ativar autenticação de dois fatores

Ao permitir a autenticação de dois fatores, você deixará a sua conta Bitdefender muito mais segura. Sua identidade será verificada cada vez que você fizer login em um dispositivo diferente, já seja para instalar um dos produtos Bitdefender, verificar o estado da sua assinatura ou executar tarefas remotamente nos seus dispositivos.

Para ativar a autenticação de dois fatores:

1. Acesse Bitdefender Central.
2. Clique no ícone no canto superior direito da tela.

3. Clique em **Conta da Bitdefender** no menu deslizante.
4. Selecione a aba **Senha e segurança**.
5. Clique em **COMEÇAR**.

   Selecione uma das seguintes opções:

   - **Aplicativo de autenticação** - use um aplicativo de autenticação para gerar um código cada vez que você quiser acessar a sua conta Bitdefender.

     Caso você queira usar o aplicativo de autenticação, mas você não tem certeza de qual escolher, aparecerá uma lista com os aplicativos de autenticação recomendados.

     a. Clique em **USAR APLICATIVO DE AUTENTICAÇÃO** para começar.

     b. Para entrar em um dispositivo Android ou iOS, use o seu dispositivo para escanear o código QR.

        Para acessar usando um laptop ou computador, você pode adicionar manualmente o código mostrado.

        Clique em **CONTINUAR**.

     c. Insira o código fornecido pelo aplicativo ou o que foi mostrado no passo anterior, e então clique em **ATIVAR**.

   - **E-mail** - cada vez que você acessar a sua conta Bitdefender, o código de verificação será enviado à sua caixa de e-mail. Verifique a sua conta de e-mail e digite o código fornecido.

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

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

     c. Clique em **ATIVAR**.

Caso você queira parar de usar a autenticação de dois fatores:

1. Clique em **DESATIVAR A AUTENTICAÇÃO DE DOIS FATORES**.
2. Verifique o seu aplicativo ou conta de e-mail e digite o código que você recebeu.
3. Confirme sua escolha.

12.4. Adicionando dispositivos confiáveis

Para garantir que apenas você pode acessar a sua conta Bitdefender, pode ser que solicitemos o código de segurança antes. Caso queira pular este passo cada vez que se conectar com o mesmo dispositivo, nós recomendamos cadastrá-lo como um dispositivo confiável.

Para adicionar dispositivos confiáveis:

1. Acesse Bitdefender Central.
2. Clique no ícone no canto superior direito da tela.
3. Clique em **Conta da Bitdefender** no menu deslizante.
4. Selecione a aba **Senha e segurança**.
5. Clique em **Dispositivos confiáveis**.
6. Será mostrada a lista com os dispositivos Bitdefender instalados. Clique no dispositivo desejado.

Você pode adicionar quantos dispositivos desejar, contanto que eles tenham o Bitdefender instalado e sua assinatura seja válida.

12.5. Minhas assinaturas

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

12.5.1. 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 **ATIVAR** para continuar.

A assinatura está ativada agora.

Para começar a instalar o produto nos seus dispositivos, acesse "*Instalando o Bitdefender Antivirus for Mac*" (p. 194).

12.5.2. 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.

12.6. 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 do dispositivo mostram o nome do dispositivo, o estado de proteção e se há algum risco de segurança afetando a proteção dos seus dispositivos.

12.6.1. Personalize seu dispositivo

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 cartão de dispositivo desejado, e depois o ícone ⋮ no canto superior direito na tela.
4. Selecione **Configurações**.

5. Digite um novo nome no campo **Nome do dispositivo**, e logo clique no **SALVAR**.

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 cartão de dispositivo desejado, e depois o ícone ⋮ no canto superior direito na tela.
4. Selecione **Perfis**.
5. Clique em **Add owner** e, em seguida, preencha os respetivos campos. Personalize o perfil adicionando uma foto, selecionando uma data de nascimento, além de um e-mail e número de telefone.
6. Clique em **ADICIONAR** para salvar o perfil.
7. Selecione o proprietário desejado na lista **Proprietário do dispositivo** e clique em **ATRIBUIR**.

12.6.2. Ações remotas

Para atualizar o Bitdefender remotamente no seu dispositivo:

1. Acesse Bitdefender Central.
2. Selecione o painel **Meus Dispositivos**.
3. Clique no cartão de dispositivo desejado, e depois o ícone ⋮ no canto superior direito na tela.
4. Selecione **Atualizar**.

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

- **PAINEL**. Nesta janela, você pode visualizar os detalhes sobre o dispositivo selecionado, verificar seu estado de proteção e quantas ameaças foram bloqueadas nos últimos sete dias. O estado de proteção pode estar verde, quando não houver problemas afetando seu dispositivo, amarelo, quando o dispositivo requerer sua atenção, ou vermelho, quando o dispositivo estiver em risco. Quando houver problemas afetando o seu dispositivo, clique na seta suspensa na área de status superior para saber 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 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. 205).

13. PERGUNTAS MAIS FREQÜENTES

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:
   a. Acesse: https://central.bitdefender.com.
   b. Digite as informações necessárias nos campos correspondentes. Os dados que nos fornecer serão mantidos confidenciais.
   c. Antes de continuar, você deve concordar com os Termos de Uso. Acesse os Termos de Uso e leia-os com atenção pois eles contêm os termos e condições segundo os quais você pode usar o Bitdefender.

      Além disso, você pode acessar e ler a Política de Privacidade.
   d. Clique em **CRIAR CONTA**.
2. Faça o download do Bitdefender Antivirus for Mac da seguinte forma:
   a. Selecione o painel **Meus Dispositivos**, e clique em **INSTALAR PROTEÇÃO**.
   b. Escolha uma das duas opções disponíveis:
      - **Proteja este dispositivo**
        i. Selecione essa opção, e a seguir, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique no botão correspondente.
        ii. Guarde o arquivo de instalação.
      - **Proteja outros dispositivos**
        i. Selecione essa opção, e a seguir, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique no botão correspondente.
        ii. Pressione **ENVIAR LINK DE DOWNLOAD**.

iii. Digite um endereço de email no campo correspondente e clique em **ENVIAR EMAIL**.

Observe que o link de download gerado será válido apenas durante as próximas 24 horas. Se o link expirar, você precisará gerar um novo seguindo os mesmos passos.

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

c. Execute o Bitdefender que você baixou.

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 essa informação, clique em **Notificações** no menu de navegação na interface do Bitdefender.

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 informações sobre ameaças.

Como eu posso remover o Bitdefender Antivirus for Mac?

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

1. Abra uma janerla do **Finder** e vá para a pasta de Aplicações.
2. Abra a pasta do Bitdefender e clique duas vezes sobre o botão Desinstalar Bitdefender.
3. Clique em **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 "Contate-nos" (p. 299).

Como removo as extensões do TrafficLight do meu navegador?

- Para remover as extensões do TrafficLight do Mozilla Firefox, siga estes passos:
  1. Vá em **Ferramentas** e selecione **Add-ons**.
  2. Selecione **Extensões** na coluna à esquerda.
  3. Selecione a extensão e clique em **Remover**.
  4. Reinicie o navegador para completar o processo de remoção.
- Para remover as extensões do TrafficLight do Google Chrome, siga estes passos:
  1. Na parte superior direita, clique em **Mais** ⋮.
  2. Vá em **Mais Ferramentas** e selecione **Extensões**.

3. Clique no ícone **Remover...** ao lado da extensão que você deseja remover.
4. Clique em **Remover** para confirmar o processo de remoção.

- Para remover o Bitdefender TrafficLight do Safari, siga estes passos:
  1. Ir a **Preferências** ou pressionar **Command-Vírgula(,)**.
  2. Selecione **Extensões**.

     Será exibida a lista das extensões instaladas.
  3. Seleccione a extensão do Bitdefender TrafficLight, e clique em **Desinstalar**.
  4. Clique novamente em **Desinstalar** para confirmar o processo de remoção.

Quando devo usar o Bitdefender VPN?

Você precisa ter cuidado quando acessa, baixa ou envia conteúdos na internet. Para garantir que você fique em segurança enquanto navega na web, recomendamos usar o Bitdefender VPN quando você:

- quiser se conectar a redes sem fio públicas
- quiser acessar conteúdos que normalmente são restritos em áreas específicas, não importa se estiver em casa ou viajando
- quiser manter seus dados pessoais privados (nomes de usuário, senhas, informações de cartão de crédito, etc.)
- desejar esconder seu endereço IP

O Bitdefender VPN vai ter um impacto negativo na bateria do meu dispositivo?

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

Por que estou encontrando lentidão na internet enquanto uso o Bitdefender VPN?

O Bitdefender VPN foi projetado para suavizar sua experiência enquanto navega na internet. No entanto, a lentidão pode ser causada pela sua

conectividade com a internet ou pela distância do servidor ao qual você está conectado. Nesse caso, se não for uma necessidade conectar a um servidor distante com respeito à sua localização (por exemplo, dos EUA ou China), recomendamos que você permita ao Bitdefender VPN conectá-lo automaticamente ao servidor mais próximo, ou encontrar um servidor próximo à sua localização atual.

MOBILE SECURITY PARA IOS

14. O QUE É BITDEFENDER MOBILE SECURITY FOR IOS

Atividades online, como pagar contas, fazer reservas para as férias ou comprar bens e serviços são convenientes e práticas. Mas, como muitas atividades realizadas na internet, elas vêm acompanhadas de altos riscos e, se detalhes de segurança forem ignorados, dados pessoais podem ser hackeados. E o que é mais importante do que proteger os dados armazenados em contas online e no seu smartphone?

O Bitdefender Mobile Security for iOS permite:

- Proteja seus dados ao se conectar a redes sem fio não seguras.
- Tenha cuidado com websites e domínios maliciosos enquanto estiver online.
- Verificar se ocorreu qualquer vazamento nas contas online que você usa diariamente.

O Bitdefender Mobile Security for iOS é entregue sem custos e requer ativação com uma conta Bitdefender.

15. INTRODUÇÃO

Requerimentos do Aparelho

O Bitdefender Mobile Security for iOS funciona em qualquer dispositivo com iOS 11.2 ou superior e precisa de uma conexão com a internet para ser ativado e detectar quaisquer vazamentos de dados nas suas contas online.

Instalando o Bitdefender Mobile Security for iOS

- **Da Bitdefender Central**
  - No iOS
    1. Acesse Bitdefender Central.
    2. Pressione o ícone no canto superior esquerdo da tela, e então selecione **Meus Dispositivos**.
    3. Pressione **INSTALAR A PROTEÇÃO**, e logo pressione **Proteger este dispositivo**.
    4. Selecione o dono do dispositivo. Se o dispositivo for de outra pessoa, pressione o botão correspondente.
    5. Você será redirecionado para o aplicativo da **App Store**. Na tela da App Store, pressione a opção de instalação.
  - No Windows, macOS, Android
    1. Acesse Bitdefender Central.
    2. Pressione o ícone no canto superior esquerdo da tela, e então selecione **Meus dispositivos**.
    3. Pressione **INSTALAR A PROTEÇÃO**, e logo pressione **Proteger outro dispositivo**.
    4. Selecione o dono do dispositivo. Selecione o dono do dispositivo. Se o dispositivo pertence a outra pessoa, pressione o botão correspondente.
    5. Pressione **Enviar link de download**.
    6. Digite um endereço de e-mail no campo correspondente e pressione **ENVIAR E-MAIL**. Observe que o link de download gerado será válido

apenas durante as próximas 24 horas. Se o link expirar, você precisará gerar um novo seguindo os mesmos passos.

7. No dispositivo em que você deseja instalar o Bitdefender verifique a conta de e-mail que você digitou e aperte o botão de download correspondente.

- **Na App Store**

  Busque por Bitdefender Mobile Security for iOS para localizar e instalar o aplicativo.

Uma janela introdutória contendo detalhes sobre as funções do produto é exibida na primeira vez que você abrir o aplicativo. Pressione **Começar** para continuar para o próximo passo.

Antes de passar pelos passos de validação, você deve concordar com o Acordo de Assinatura. Por favor, leia o cordo de Assinatura com calma, já que ele contém os termos e condições segundo os quais você pode usar o Bitdefender Mobile Security for iOS.

Pressione **Continuar** para passar para o próximo passo.

Entre na sua conta Bitdefender

Para usar o Bitdefender Mobile Security for iOS, você precisa vincular seu dispositivo a uma conta Bitdefender, do Facebook, Google ou Microsoft acessando a conta dentro do aplicativo. Na primeira vez que abrir o aplicativo, será pedido que você acesse uma conta.

Para vincular seu dispositivo a uma conta Bitdefender:

1. Digite seu endereço de e-mail da sua conta da Bitdefender no campo correspondente e clique em **PRÓXIMO**. Se você não tem uma conta da Bitdefender e deseja criar uma, selecione o link correspondente e depois siga as instruções na tela até a conta ser ativada.

   Para entrar usando uma conta do Facebook, Google ou Microsoft, pressione o serviço que deseja usar na área **Ou entrar com**. Você será redirecionado para a página de login do serviço selecionado. Siga as instruções para vincular sua conta ao Bitdefender Mobile Security for iOS.

> **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.

2. Digite a senha, e depois clique em **ENTRAR**.

   Aqui você pode acessar a Política de Privacidade do Bitdefender.

Painel Geral

Toque no ícone do Bitdefender Mobile Security for iOS na gaveta de aplicativos do seu aparelho para abrir a interface do aplicativo.

Na primeira vez que abrir o aplicativo, será solicitado que você permita ao Bitdefender enviar-lhe notificações. Pressione **Permitir** para permanecer informado toda vez que o Bitdefender tiver que comunicar algo relevante para o seu app. Para gerenciar as notificações do Bitdefender, vá em Configurações > Notificações > Segurança móvel.

Para ter acesso às informações que você precisa, pressione no ícone correspondente na base da tela.

VPN
Mantenha sua privacidade independentemente da rede à qual você estiver conectado(a) para manter sua comunicação por internet criptografada. Para mais informações, acesse "*VPN*" (p. 244).

Proteção na Web
Fique seguro(a) enquanto navega pela web e quando aplicativos menos seguros tentarem acessar domínios não confiáveis. Para mais informações, acesse "*Proteção na Web*" (p. 247).

Privacidade de Conta
Descubra se suas contas de e-mail foram invadidas ou não. Para mais informações, acesse "*Privacidade de Conta*" (p. 250).

Para ver mais opções, pressione o ícone ••• no seu dispositivo enquanto estiver na tela inicial do aplicativo. As seguintes opções aparecerão:

- **Restaurar compras** - aqui você pode restaurar para a assinatura Premium VPN que você comprou através da conta do iTunes.

- **Definições** - aqui você pode acessar as configurações do VPN, conforme a seguir:
  - **Acordo** - você pode ler os termos que se aplicam ao uso dos serviços do Bitdefender VPN. Se clicar em **Não concordo mais**, você não poderá usar os serviços do Bitdefender VPN até você pressionar **Eu concordo**.
  - **Abrir aviso de Wi-Fi** - você pode ativar ou desativar a notificação do produto que aparecerá cada vez que você se conectar a uma rede Wi-Fi não segura. O objetivo dessa notificação é ajudar a manter os seus dados privados e seguros utilizando o Bitdefender VPN.
- **Feedback** - aqui você pode lançar o e-mail padrão de cliente e nos enviar o seu feedback sobre o aplicativo.
- **Informação do aplicativo** - aqui você tem acesso a informações sobre a versão instalada, bem como o seu Acordo de Assinatura, a Política de Segurança e conformidades de licenças open-source.

16. VPN

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

O VPN funciona como um túnel entre o seu dispositivo e a rede à qual você se conecta, protegendo sua conexão, criptografando seus dados usando criptografia de nível bancário e escondendo seu endereço IP onde quer que esteja. Seu tráfego é redirecionado por meio de um servidor separado, tornando seu dispositivo quase impossível de ser identificado dentre os incontáveis dispositivos que usam nossos serviços. Além disso, enquanto estiver conectado à internet com o Bitdefender VPN, você pode acessar conteúdos que normalmente são restritos em áreas específicas.

Nota
China, Iraque, Emirados Árabes Unidos, Turquia, Belarus, Omã, Irã e Rússia praticam a censura na Internet e, portanto, o uso de VPNs em seu território foi proibido por lei. Consequentemente, a funcionalidade do Bitdefender VPN não estará disponível em seu território.

Para ativar o Bitdefender VPN:

1. Pressione o ícone na base da tela.
2. Pressione **Conectar** sempre que quiser permanecer protegido enquanto estiver conectado a redes sem fio não seguras.

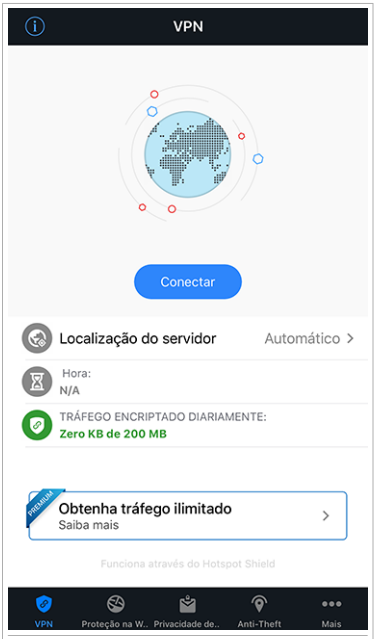
   Pressione **Desconectar** quando desejar desativar a conexão.

Nota
Na primeira vez que ligar o VPN, será solicitado que você permita ao Bitdefender configurar ajustes de VPN que monitorarão o tráfego de rede. Pressione **Permitir** para continuar. Se um método de autenticação (leitura de digital ou código PIN) tiver sido configurado para proteger seu smartphone, será solicitado que você o use.

O ícone VPN aparece na barra de status quando o VPN está ativo.

Para economizar bateria, recomendamos que você desligue o VPN quando não precisar usá-lo.

Se você tiver uma assinatura Premium e quiser se conectar a um servidor da sua escolha, pressione **Localização do Servidor** na interface do VPN e depois selecione o local desejado. Para detalhes sobre as assinaturas de VPN, acesse "*Assinaturas*" (p. 245).



VPN

16.1. Assinaturas

O Bitdefender VPN oferece gratuitamente uma quota de tráfego diário de 200 MB por dispositivo para proteger a conexão sempre que a sua equipe precisar.

Para obter tráfego ilimitado e acesso irrestrito a conteúdos no mundo todo podendo escolher um local de servidor da escolha da sua equipe, atualize para a versão premium.

Você pode atualizar para a versão do Bitdefender Premium VPN em qualquer momento no painel **Minhas assinaturas** disponível na conta do seu Bitdefender.

A assinatura do Bitdefender Premium VPN é independente da assinatura do Bitdefender Small Office Security, ou seja, você poderá usá-lo durante todo o seu período de validade. Caso a assinatura do Bitdefender Premium VPN expire e a do Bitdefender Small Office Security continue ativa, você voltará para o plano gratuito.

O Bitdefender VPN é um produto multiplataforma, disponível nos produtos Bitdefender compatíveis com Windows, macOS, Android e iOS. Quando você atualizar para o plano Premium, poderá usar sua assinatura em todos os seus produtos, desde que faça login com a mesma conta Bitdefender.

17. PROTEÇÃO NA WEB

A Proteção na Web Bitdefender assegura uma experiência de navegação segura alertando-o sobre páginas da web maliciosas e quando aplicativos instalados menos seguros tentam acessar domínios não confiáveis.

Quando um URL sinalizar uma página da web conhecida como phishing ou fraudulenta, ou para conteúdo malicioso como spyware ou vírus, a página da web é bloqueada e é mostrado um alerta. Acontece a mesma coisa quando aplicativos instalados tentam acessar domínios maliciosos.

Para ativar a Proteção na Web:

1. Pressione o ícone na base da tela.
2. Clique em **AVALIE PROTEÇÃO DA WEB**.
3. Escolha um dos períodos gratuitos de avaliação, e então, confirme os detalhes de pagamento.
4. Habilitar a chave de Proteção na Web.

Nota
A primeira vez que ligar a Proteção na Web, você deverá permitir ao Bitdefender configurar ajustes de VPN que monitorarão o tráfego de rede. Pressione **Permitir** para continuar. Se um método de autenticação (leitura de digital ou código PIN) tiver sido configurado para proteger seu smartphone, será solicitado que você o use. Para poder detectar o acesso a domínios não confiáveis, a Proteção na Web trabalha conjuntamente com os serviços VPN.

Importante
Se você está em uma área onde o uso de um serviço VPN é restrito por lei, a função de Proteção na Web não estará disponível.

17.1. Alertas de Bitdefender

Sempre que você tentar visitar um website classificado como não seguro, ele será bloqueado. Para avisá-lo sobre o evento, você será notificado pelo Bitdefender no centro de Notificações e no seu navegador. A página de alertas contém informações como a URL do website e a ameaça detectada. Você precisa decidir o que fará a seguir.

Além disso, você receberá notificações no Centro de Notificações quando um aplicativo menos seguro tentar acessar domínios não confiáveis. Clique

na notificação exibida para ser redirecionado(a) à janela, onde você poderá decidir o que fazer a seguir.

As seguintes opções estão disponíveis para os dois casos:

- Sair do website clicando em **VOLTAR À SEGURANÇA**.
- Continuar para o website, apesar do aviso, clicando na notificação mostrada, e então, em **Quero acessar a página**.

  Confirme sua escolha.

Proteção na Web

17.2. Assinaturas

A Proteção na Web é uma função baseada na assinatura com a possibilidade de experimentá-la gratuitamente para poder decidir se cumpre com suas necessidades. Existem dois tipos de assinatura disponíveis: anual e mensal.

Se sua assinatura da Proteção na Web da Bitdefender expirar, você não receberá mais alertas ao acessar conteúdo malicioso.

Se você comprou um dos pacotes do Bitdefender, como o Bitdefender Total Security, você terá acesso ilimitado à Proteção na Web.

18. PRIVACIDADE DE CONTA

A Privacidade de Conta do Bitdefender detecta se ocorreu qualquer vazamento de dados nas contas que você usa para fazer pagamentos, compras ou assinaturas online em diferentes aplicativos e websites. Os dados que podem ser armazenados em uma conta podem ser senhas, informações de cartão de crédito ou bancárias e, se não forem protegidos adequadamente, pode ocorrer roubo de identidade ou invasão de privacidade.

O status de privacidade de uma conta é exibido logo após a validação.

Para verificar se qualquer conta foi invadida, pressione **Buscar por vazamentos**.

Para começar a proteger suas informações pessoais:

1. Pressione o ícone na base da tela.
2. Pressione **Adicionar** no lado superior direito da tela.
3. Digite seu endereço de e-mail no campo correspondente e pressione **PRÓXIMO**.

   O Bitdefender precisa validar esta conta antes de exibir informações pessoais. Portanto, um e-mail com um código de validação é enviado ao endereço de e-mail fornecido.
4. Verifique sua caixa de entrada e depois digite o código recebido na área **Privacidade de Conta** do seu aplicativo. Se você não encontrar o e-mail de validação na caixa de entrada, verifique a pasta de spam também.

   O status de privacidade da conta validada é exibido.

Se vazamentos forem encontrados em qualquer uma das suas contas, recomendamos que você altere a senha o mais rápido possível. Para criar uma senha forte e segura, considere estas dicas:

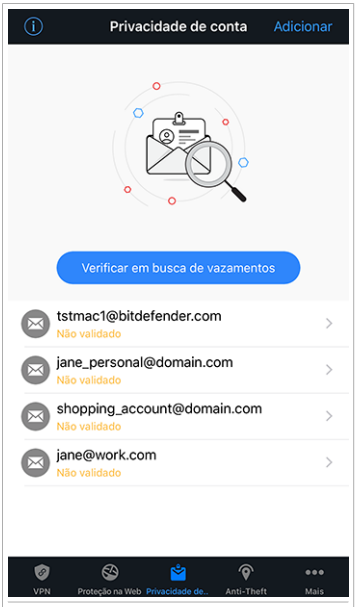
- Faça com que ela tenha ao menos oito caracteres.
- Inclua caracteres minúsculos e maiúsculos.
- Use pelo menos um número ou símbolo, como #, @, % ou !.

Ao proteger uma conta após um vazamento de privacidade, você pode confirmar as alterações marcando os vazamentos identificados como **Resolvido**. Para fazer isso:

1. Pressione ··· ao lado da conta que você acabou de proteger.
2. Pressione **Marcar como resolvido**.

   A conta aparecerá na lista de **RESOLVIDOS**.

Quando todos os vazamentos detectados estiverem marcados como **Resolvido**, a conta não aparecerá mais com a marcação de vazamento, ao menos até que ocorra um novo.



Privacidade de Conta

19. 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, acessando https://central.bitdefender.com, ou diretamente pelo aplicativo da Bitdefender Central em dispositivos Android e iOS.

Para instalar o aplicativo da Bitdefender Central nos seus dispositivos:

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

Assim que fizer login, você pode começar a fazer o seguinte:

- Faça o download e instale o Bitdefender nos sistemas operacionais Windows, macOS, iOS e Android. Os produtos disponíveis para download são:
  - Bitdefender Mobile Security para Android
  - Bitdefender Mobile Security para iOS
  - 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

Há duas formas de acessar a Bitdefender Central

- No seu navegador da Internet:
  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.

- Em seu dispositivo Android ou iOS:

  Abra o aplicativo da Bitdefender Central que você instalou.

> **Nota**
> Com este material, você recebe as opções e instruções disponíveis na plataforma web.

Autenticação de dois fatores

O método de autenticação em 2 fatores adiciona uma camada extra de segurança à sua conta do Bitdefender, ao requerer um código de autenticação além das credenciais de login. Assim, você impedirá o roubo da conta e afugentará diversos tipos de ciberataques, como keyloggers, ataques de força bruta e de dicionário.

Ativar autenticação de dois fatores

Ao permitir a autenticação de dois fatores, você deixará a sua conta Bitdefender muito mais segura. Sua identidade será verificada cada vez que você fizer login em um dispositivo diferente, já seja para instalar um dos produtos Bitdefender, verificar o estado da sua assinatura ou executar tarefas remotamente nos seus dispositivos.

Para ativar a autenticação de dois fatores:

1. Acesse Bitdefender Central.
2. Pressione o ícone no canto superior direito da tela.
3. Clique em **Conta do Bitdefender** no menu deslizante.
4. Selecione a aba **Senha e segurança**.
5. Toque em **Autenticação em dois fatores**.
6. Toque em **COMEÇAR A USAR**.

   Selecione uma das seguintes opções:

   - **Aplicativo de autenticação** - use um aplicativo de autenticação para gerar um código cada vez que você quiser acessar a sua conta Bitdefender.

Caso você queira usar o aplicativo de autenticação, mas você não tem certeza de qual escolher, aparecerá uma lista com os aplicativos de autenticação recomendados.

a. Toque em **USAR APLICATIVO DE AUTENTICAÇÃO** para começar.

b. Para entrar em um dispositivo Android ou iOS, use o seu dispositivo para escanear o código QR.

Para acessar usando um laptop ou computador, você pode adicionar manualmente o código mostrado.

Pressione **CONTINUAR**.

c. Insira o código fornecido pelo aplicativo ou mostrado no passo anterior, e então toque em **ATIVAR**.

- **E-mail** - cada vez que você acessar a sua conta Bitdefender, o código de verificação será enviado à sua caixa de e-mail. Verifique a sua conta de e-mail e então digite o código que você recebeu.

a. Toque em **USAR E-MAIL** para começar.

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

Lembre que você possui cinco minutos para verificar a sua conta de e-mail e digitar o código gerado. Se o tempo expirar, você deverá gerar um novo link seguindo os mesmos passos.

c. Pressione **ATIVAR**.

d. Você receberá dez códigos de ativação. Você pode tanto copiar, baixar ou imprimir a lista e usá-la caso perca o seu endereço de e-mail, caso contrário você não poderá acessar. Cada código pode ser usado apenas uma vez.

e. Pressione **FEITO**.

Caso você queira parar de usar a autenticação de dois fatores:

1. Toque em **DESATIVAR A AUTENTICAÇÃO EM DOIS FATORES**.
2. Verifique o seu aplicativo ou conta de e-mail e digite o código que você recebeu.

   Caso você tenha escolhido receber o código de autenticação por e-mail, você terá cinco minutos para verificar a sua conta de e-mail e digitar o código gerado. Se o tempo expirar, você deverá gerar um novo link seguindo os mesmos passos.

3. Confirme sua escolha.

Adicionando dispositivos confiáveis

Para garantir que apenas você pode acessar a sua conta Bitdefender, pode ser que solicitemos o código de segurança antes. Caso queira pular este passo cada vez que se conectar com o mesmo dispositivo, nós recomendamos cadastrá-lo como um dispositivo confiável.

Para adicionar dispositivos confiáveis:

1. Acesse Bitdefender Central.
2. Pressione o ícone no canto superior direito da tela.
3. Clique em **Conta do Bitdefender** no menu deslizante.
4. Selecione a aba **Senha e segurança**.
5. Pressione **Dispositivos confiáveis**.
6. Será mostrada a lista com os dispositivos Bitdefender instalados. Toque no dispositivo desejado.

Você pode adicionar quantos dispositivos desejar, contanto que eles tenham o Bitdefender instalado e sua assinatura seja válida.

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 do dispositivo mostram o nome do dispositivo, o estado de proteção e se há algum risco de segurança afetando a proteção dos seus dispositivos.

Para identificar e gerenciar facilmente seus dispositivos, você pode personalizar o nome do dispositivo e criar ou atribuir um proprietário para cada um deles:

1. Pressione o ícone no canto superior esquerdo da tela, e então selecione **Meus dispositivos**.
2. Pressione o cartão de dispositivo desejado, e depois o ícone no canto superior direito na tela. As seguintes opções estão disponíveis:
   - **Configurações** - aqui você pode alterar o nome do dispositivo selecionado.

- **Perfil** - aqui um perfil pode ser atribuído ao dispositivo selecionado. Pressione em **Adicionar proprietário** e preencha os campos correspondentes. Defina o nome, e-mail, número de telefone, data de nascimento e você pode até selecionar uma foto de perfil.
- **Remover** - daqui, você pode remover um perfil com o dispositivo designado da sua conta Bitdefender.

Entrar com outra conta Bitdefender

Para entrar com outra conta Bitdefender:

1. Pressione o ícone na base da tela.
2. Pressione **Sair**.
3. Digite o endereço de e-mail e senha da sua conta Bitdefender nos campos correspondentes.
4. Pressione **ENTRAR**.

MOBILE SECURITY PARA ANDROID

20. RECURSOS DE PROTEÇÃO

O Bitdefender Mobile Security protege seu dispositivo Android com os seguintes recursos:

- Verificador de Malware
- Proteção na Web
- VPN
- Antifurto, incluindo:
  - Localização Remota
  - Bloqueio remoto do aparelho
  - Apagamento remoto do aparelho
  - Alertas do aparelho remoto
- Privacidade de Conta
- 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.

21. INTRODUÇÃO

Requerimentos do Aparelho

O Bitdefender Mobile Security funciona em qualquer dispositivo com Android 4.1 ou superior. É necessária uma conexão ativa à Internet para a varredura de ameaça nas nuvens.

Instalando o Bitdefender Mobile Security

- **Da Bitdefender Central**
  - Android
    1. Acesse: https://central.bitdefender.com.
    2. Entre na sua conta Bitdefender.
    3. Toque em ☰ no canto superior esquerdo da tela, e então selecione **Meus dispositivos**.
    4. Pressione **INSTALAR A PROTEÇÃO**, e logo pressione **Proteger este dispositivo**.
    5. Selecione o dono do dispositivo. Se o dispositivo for de outra pessoa, pressione o botão correspondente.
    6. Você será redirecionado para o aplicativo do **Google Play**. Na tela da Google Play, pressione a opção de instalação.
  - No Windows, macOS, iOS
    1. Acesse: https://central.bitdefender.com.
    2. Entre na sua conta Bitdefender.
    3. Toque em ☰ no canto superior esquerdo da tela, e então selecione **Meus dispositivos**.
    4. Pressione **INSTALAR A PROTEÇÃO**, e logo pressione **Proteger outro dispositivo**.
    5. Selecione o dono do dispositivo. Selecione o dono do dispositivo. Se o dispositivo pertence a outra pessoa, pressione o botão correspondente.
    6. Pressione **Enviar link de download**.

7. Digite um endereço de e-mail no campo correspondente e pressione **ENVIAR E-MAIL**. Observe que o link de download gerado será válido apenas durante as próximas 24 horas. Se o link expirar, você precisará gerar um novo seguindo os mesmos passos.
8. No dispositivo em que você deseja instalar o Bitdefender verifique a conta de e-mail que você digitou e aperte o botão de download correspondente.

- **Do Google Play**

  Busque por Bitdefender Mobile Security para localizar e instalar o aplicativo.

  Alternativamente, escaneie o código QR:

Código QR

Antes de passar pelos passos de validação, você deve concordar com o Acordo de Assinatura. Por favor, leia o cordo de Assinatura com calma, já que ele contém os termos e condições segundo os quais você pode usar o Bitdefender Mobile Security.

Pressione **CONTINUAR** para passar para o próximo passo.

Entre na sua conta Bitdefender

Para usar o Bitdefender Mobile Security, você precisa vincular seu dispositivo a uma conta Bitdefender, do Facebook, Google ou Microsoft 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 desde sua conta Bitdefender, o aplicativo tentará fazer login automaticamente com essa conta.

Para vincular seu dispositivo a uma conta Bitdefender:

1. Digite o endereço de e-mail e senha da sua conta Bitdefender nos campos correspondentes. Caso não tenha uma conta Bitdefender e deseje criar uma, pressione o link correspondente para criar uma.
2. Pressione **ENTRAR**.

Para entrar usando uma conta do Facebook, Google ou Microsoft, pressione o serviço que deseja usar na área **Ou entrar com**. Você será redirecionado para a página de login do serviço selecionado. Siga as instruções para vincular sua conta ao Bitdefender Mobile Security.

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.

Configurar proteção

Uma vez que você consiga entrar no aplicativo, a janela **Configurar proteção** aparecerá. Nós recomendamos que você realize estes passos para proteger seu dispositivo:

- **Status de assinatura.** Para obter a proteção do Bitdefender Mobile Security, 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.

  Caso tenha um código de ativação, pressione **EU POSSUO UM CÓDIGO** e depois **ATIVAR**.

  Se você tiver entrado com uma nova conta Bitdefender e não tiver um código de ativação, poderá usar o produto por 14 dias gratuitamente.

- **Proteção na web.** Se o seu dispositivo requerer acessibilidade para ativar a proteção na web, pressione **ATIVAR**. Você será redirecionado para o menu de acessibilidade. Pressione Bitdefender Mobile Security e depois ligue o botão correspondente.

- **Verificador de Malware.** Realize uma verificação única do seu dispositivo para que ele esteja livre de ameaças. Para iniciar o processo de verificação, pressione **VERIFICAR AGORA**.

Assim que o processo de verificação começar, o painel aparecerá. Aqui você vê o status de segurança do seu dispositivo.

Painel Geral

Toque no ícone do Bitdefender Mobile Security na gaveta de aplicativos do seu aparelho para abrir a interface do aplicativo.

O Painel fornece informações sobre o status de segurança do seu dispositivo e por meio do Autopilot, ele ajuda a reforçar a segurança do seu dispositivo oferecendo recomendações de recursos.

O cartão de status no topo da janela informa sobre o status de segurança do dispositivo usando mensagens explícitas e cores sugestivas. Se o Bitdefender Mobile Security não tiver alertas, o cartão de status será verde. Quando um problema de segurança é detectado, o cartão de status muda para vermelho.

Para lhe oferecer uma operação efetiva e proteção reforçada enquanto realiza diferentes atividades, o **Bitdefender** Autopilot agirá como o seu consultor de segurança pessoal. Dependendo da atividade que você realizar, o Bitdefender do Autopilot fornecerá recomendações contextuais com base no uso e necessidades do seu dispositivo. Isso irá ajudá-lo a descobrir e se beneficiar das vantagens trazidas pelos recursos inclusos no aplicativo Bitdefender Mobile Security.

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 para navegar facilmente na barra de navegação inferior:

Verificador de Malware
Permite iniciar uma verificação sob demanda e habilitar a Verificação de Armazenamento. Para mais informações, acesse "*Verificador de Malware*" (p. 264).

Proteção na Web
Garante uma navegação segura, alertando sobre páginas da web potencialmente maliciosas. Para mais informações, acesse "*Proteção na Web*" (p. 267).

VPN

Criptografa a comunicação na internet, ajudando-o a manter sua privacidade, não importando a rede à qual você está conectado. Para mais informações, acesse "*VPN*" (p. 269).

Antifurto

Permite que você ative ou desative as características Antifurto e configure os ajustes Antifurto. Para mais informações, acesse "*Recursos Antifurto*" (p. 272).

Privacidade de Conta

Verifica se ocorreu qualquer vazamento de dados nas suas contas online. Para mais informações, acesse "*Privacidade de Conta*" (p. 276).

Bloqueio de Aplicativo

Permite que você proteja seus aplicativos instalados, através da configuração de um código de acesso PIN. Para mais informações, acesse "*Bloqueio de Aplicativo*" (p. 278).

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, acesse "*Relatórios*" (p. 283).

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, acesse "*WearON*" (p. 284).

22. 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 verifica automaticamente se o mesmo utiliza tecnologia nas nuvens. O mesmo processo de verificação se inicia toda vez que aplicativos instalados são atualizados.

  Caso o aplicativo seja considerado malicioso, aparecerá um alerta solicitando que você desinstale-o. Pressione **Desinstalar** para acessar a tela de desinstalação do aplicativo.

- **Análise on-demand**

  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 sob demanda:

  1. Toque em **Verificação de Malware** na barra de navegação inferior.
  2. Pressione **INICIAR ANÁLISE**.

     Nota
     Permissões adicionais são necessárias no Android 6 para a função Verificador de Malware. Após pressionar **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 progresso de verificação será exibido, e você poderá detê-lo em qualquer momento.

Verificação de Malware

O Bitdefender Mobile Security já vem configurado para verificar o armazenamento interno de seu dispositivo, incluindo qualquer cartão SD conectado. a, quaisquer aplicativos perigosos que estejam no cartão podem ser detectados antes de causar danos.

Para desativar as configurações de Verificação de Armazenamento:

1. Toque em **Mais** na barra de navegação inferior.
2. Toque em **Configurações**.
3. Desative o botão de **Verificação de Armazenamento** na área de Verificação de Malware.

Caso sejam detectados quaisquer aplicativos maliciosos, serão exibidas informações sobre eles e você poderá removê-los tocando **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.

Se a sua versão do Android é a 7.1 ou mais nova, você pode acessar um atalho para o Verificador de Malware, para poder executar as verificações de forma mais rápida, sem ter que abrir a interface do Bitdefender Mobile Security. Para isso, mantenha pressionado o ícone do Bitdefender na sua tela de Início ou na gaveta de apps, e depois selecione o ícone .

23. PROTEÇÃO 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 e Dolphin. 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.

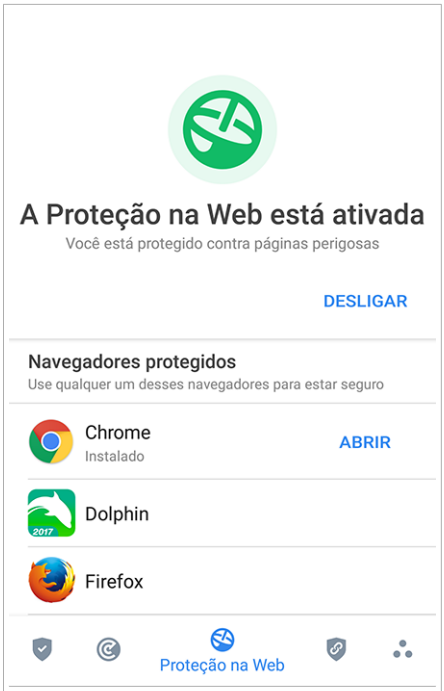
Você poderá então optar por ignorar o alerta e prosseguir à página web ou retornar a uma página segura.

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.

A configuração do Bitdefender Web Protection está programada para notificá-lo(a) para que você use o Bitdefender VPN cada vez que acessar um site de internet banking. A notificação aparece na barra de status. Recomendamos o uso do Bitdefender VPN enquanto você estiver logado(a) na sua conta de internet banking para que seus dados possam continuar protegidos contra possíveis brechas de segurança.

Para desativar a notificação da Proteção na Web:

1. Toque em **Mais** na barra de navegação inferior.
2. Toque em **Configurações**.
3. Desligue o botão correspondente na área de Proteção na Web.



Proteção na Web

24. VPN

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

O VPN funciona como um túnel entre o seu dispositivo e a rede à qual você se conecta, protegendo sua conexão, criptografando seus dados usando criptografia de nível bancário e escondendo seu endereço IP onde quer que esteja. Seu tráfego é redirecionado por meio de um servidor separado, tornando seu dispositivo quase impossível de ser identificado dentre os incontáveis dispositivos que usam nossos serviços. Além disso, enquanto estiver conectado à internet com o Bitdefender VPN, você pode acessar conteúdos que normalmente são restritos em áreas específicas.

Nota
Alguns países censuram a internet e, portanto, o uso de VPNs em seus territórios foi banido por lei. Para evitar consequências legais, uma mensagem de aviso pode aparecer ao tentar usar o aplicativo Bitdefender VPN pela primeira vez. Ao continuar a usar esse aplicativo, você confirma que está ciente das regulamentações aplicáveis e dos riscos aos quais você pode estar exposto.

Há duas formas de ativar ou desativar o Bitdefender VPN:

- Toque em **CONECTAR** no cartão do VPN no Painel de Controle.

  O estado do Bitdefender VPN é exibido.

- Toque em **VPN** na barra de navegação inferior, e então toque em **CONECTAR**.

  Pressione **CONECTAR** sempre que quiser permanecer protegido enquanto estiver conectado a redes sem fio não seguras.

  Pressione **DESCONECTAR** quando desejar desativar a conexão.

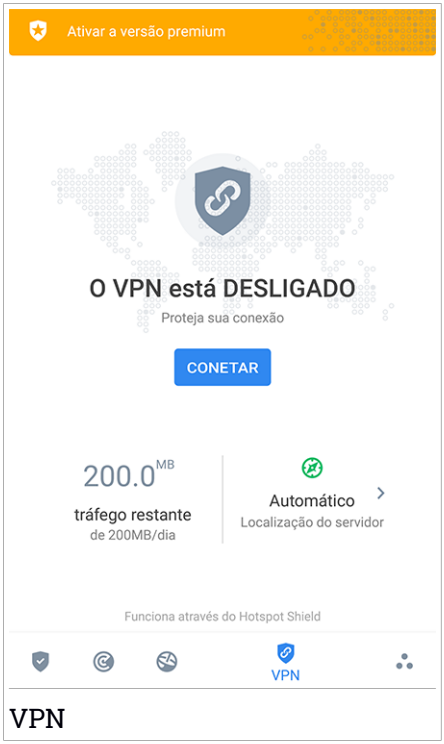
Nota
Na primeira vez que ligar o VPN, você deverá permitir a solicitação do Bitdefender para configurar uma conexão VPN que monitorará o tráfego de rede. Pressione **OK** para continuar.

Se a sua versão do Android é a 7.1 ou mais nova, você pode acessar um atalho para o Bitdefender VPN sem ter que abrir a interface do Bitdefender Mobile Security. Para isso, mantenha pressionado o ícone do Bitdefender na sua tela de Início ou na gaveta de apps, e depois selecione o ícone .

O ícone aparece na barra de status quando o Bitdefender VPN está ativo.

Para economizar bateria, recomendamos que você desligue o VPN quando não precisar usá-lo.

Se você tiver uma assinatura Premium e quiser se conectar a um servidor da sua escolha, pressione **Localização do servidor** na ferramenta de VPN e depois selecione o local desejado. Para detalhes sobre as assinaturas de VPN, acesse “Assinaturas” (p. 271).



VPN

Configurações do VPN

Para uma configuração avançada do seu VPN:

1. Toque em **Mais** na barra de navegação inferior.
2. Toque em **Configurações**.

Na área do VPN você pode ajustar as seguintes opções:

- VPN de acesso rápido - uma notificação aparecerá na barra de status do seu dispositivo permitindo ativar o VPN rapidamente.
- Rede Wi-Fi aberta - toda vez que você se conectar a uma rede Wi-Fi aberta, a barra de status do seu dispositivo vai pedir para você usar o VPN.

Assinaturas

O Bitdefender VPN oferece gratuitamente uma quota de tráfego diário de 200 MB por dispositivo para proteger a conexão sempre que a sua equipe precisar.

Para obter tráfego ilimitado e acesso irrestrito a conteúdos no mundo todo podendo escolher um local de servidor da escolha da sua equipe, atualize para a versão premium.

Você pode atualizar para a versão do Bitdefender Premium VPN em qualquer momento no painel **Minhas assinaturas** disponível na conta do seu Bitdefender.

A assinatura do Bitdefender Premium VPN é independente da assinatura do Bitdefender Small Office Security, ou seja, você poderá usá-lo durante todo o seu período de validade. Caso a assinatura do Bitdefender Premium VPN expire e a do Bitdefender Small Office Security continue ativa, você voltará para o plano gratuito.

O Bitdefender VPN é um produto multiplataforma, disponível nos produtos Bitdefender compatíveis com Windows, macOS, Android e iOS. Quando você atualizar para o plano Premium, poderá usar sua assinatura em todos os seus produtos, desde que faça login com a mesma conta Bitdefender.

25. RECURSOS ANTIFURTO

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.

Bitdefender Mobile Security 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.

Bloqueio Remoto

Bloqueia a tela do seu aparelho e define uma senha para desbloquear o mesmo.

Apagamento Remoto

Remova todos os dados pessoais de seu aparelho roubado.

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 Antifurto

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. Toque em **Mais** na barra de navegação inferior.
2. Toque em **Antifurto**.
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:

   a. Pressione **Ativar Antifurto**, então pressione **LIGAR**.

   b. Permita que o **Antivírus** acesse a localização do seu dispositivo.

   a. **Conceder privilégios de administrador**

      Esses privilégios são essenciais à operação da Antifurto, e devem ser concedidas antes de continuar.

   b. **Definir senha numérica para o aplicativo**

      Você deve estabelecer um código PIN para prevenir acessos não autorizados. Sempre que houver uma tentativa de acesso ao seu dispositivo, primeiro deverá ser inserido o código PIN. 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.

      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.

Na realidade, uma foto será 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 é salva juntamente com um selo com a hora e o motivo, e poderá ser vista quando você abrir o Bitdefender Mobile Security e acessar a janela Antifurto. De forma alternativa, você pode visualizar a foto na sua conta Bitdefender:

i. Acesse: https://central.bitdefender.com.

ii. Acesse sua conta.

iii. Toque em ☰ no canto superior esquerdo da tela, e então selecione **Meus dispositivos**.

iv. Selecione o seu dispositivo Android, e então, a aba **Antifurto**.

v. Toque ⋮ ao lado de **Verificar suas fotos** para ver as últimas fotos tiradas.

Apenas as duas fotos mais recentes são salvas.

Ao ativar o recurso Antifurto, você pode habilitar ou desabilitar os comandos de Controle da Web de maneira individual na janela do Antifurto tocando nas opções correspondentes.

Usando recursos Antifurto da Bitdefender Central

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. Toque em ☰ 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 ··· 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 Antifurto deixam de funcionar.

   EXIBIR IP - exibe o último endereço de IP para o dispositivo selecionado.

Configurações do Antifurto

Se você deseja ativar ou desativar os controles remotos:

1. Toque em **Mais** na barra de navegação inferior.
2. Toque em **Antifurto**.
3. Ativar ou desativar as opções desejadas.

26. PRIVACIDADE DE CONTA

A Privacidade de Conta do Bitdefender detecta se ocorreu qualquer vazamento de dados nas contas que você usa para fazer pagamentos, compras ou assinaturas online em diferentes aplicativos e websites. Os dados que podem ser armazenados em uma conta podem ser senhas, informações de cartão de crédito ou bancárias e, se não forem protegidos adequadamente, pode ocorrer roubo de identidade ou invasão de privacidade.

O status de privacidade de uma conta é exibido logo após a validação.

As verificações automáticas estão configuradas para ocorrer em segundo plano, mas também é possível realizar verificações manuais diariamente.

Notificações serão exibidas sempre que novos vazamentos em qualquer uma das contas de e-mail validadas forem descobertos.

Para começar a proteger suas informações pessoais:

1. Toque em **Mais** na barra de navegação inferior.
2. Toque em **Privacidade de Conta**.
3. Toque em **COMEÇAR A USAR**.
4. Aparecerá o e-mail que você usou para criar sua conta Bitdefender.

   Toque em **ADICIONAR** para continuar.

   O Bitdefender precisa validar esta conta antes de exibir informações pessoais. Portanto, um e-mail com um código de validação é enviado ao endereço de e-mail fornecido.
5. Verifique sua caixa de entrada e depois digite o código recebido na área **Privacidade de Conta** do seu aplicativo. Se você não encontrar o e-mail de validação na caixa de entrada, verifique a pasta de spam.

   O status de privacidade da conta validada é exibido.

   Para adicionar outras contas, toque em **ADICIONAR CONTA** na janela de Privacidade de Conta e siga os passos solicitados.

Se brechas forem encontradas em qualquer uma das suas contas, recomendamos que você altere a senha o mais rápido possível. Para criar uma senha forte e segura, considere estas dicas:

- Faça com que ela tenha ao menos oito caracteres.

- Inclua caracteres minúsculos e maiúsculos.
- Use pelo menos um número ou símbolo, como #, @, % ou !.

Após proteger uma conta que foi vítima de uma exposição de privacidade, você pode confirmar as mudanças marcando a(s) brecha(s) identificadas como **Solucionada(as)**. Para fazer isso:

1. Toque em **Mais** na barra de navegação inferior.
2. Toque em **Privacidade de Conta**.
3. Pulse sobre a conta que acaba de proteger.
4. Toque na brecha solucionada.
5. Toque em **SOLUCIONADO** para informar que a conta está segura.

Quando todas as brechas detectadas estiverem marcadas como **Solucionadas**, a conta não aparecerá mais como exposta, pelo menos até que seja identificada uma nova brecha.

Para parar de receber notificações cada vez que acontecer uma verificação:

1. Toque em **Mais** na barra de navegação inferior.
2. Toque em **Configurações**.
3. Desligue o botão correspondente na área de Privacidade de Conta.

27. 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. Toque em **Mais** na barra de navegação inferior.
2. Toque em **Bloqueio de aplicativos**.
3. Pressione **ATIVAR**.
4. Permitir acesso à utilização de dados para o Bitdefender.

   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.

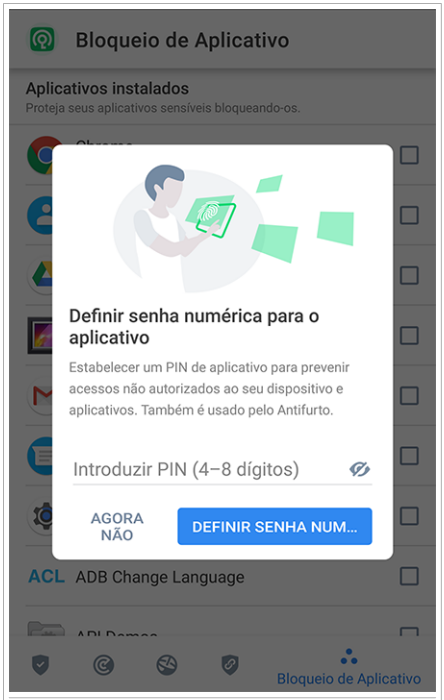
5. Volte para o aplicativo, configure o código de acesso e pressione **DEFINIR PIN**.

   Nota
   Esta etapa somente será necessária se você não tiver configurado o PIN na função Antifurto.

6. Permite que a opção Tirar Foto pegue qualquer intruso que tente acessar seus dados pessoais.
7. Selecione as aplicações você gostaria de proteger:

Usar o PIN ou digital errada cinco vez 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.



Bloqueio de Aplicativo

Modo de bloqueio

A primeira vez que você adicionar um aplicativo ao Bloqueio de Aplicativos, aparecerá a tela de Modo de Bloqueio de Aplicativos. 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:

- **Solicitar desbloqueio sempre** - cada vez que os aplicativos bloqueados forem acessados, o código PIN ou a impressão digital estabelecida terá que ser usada.
- **Manter desbloqueado até a tela apagar** - o acesso aos seus aplicativos será válido até a tela apagar.
- **Bloquear depois de 30 segundos** - você tem 30 segundos para sair e acessar novamente seus aplicativos desbloqueados.

Se você quiser mudar a configuração selecionada:

1. Toque em **Mais** na barra de navegação inferior.
2. Toque em **Configurações**.
3. Toque em **Solicitar desbloqueio sempre** na área de Bloqueio de Aplicativo.
4. Escolha a opção desejada.

Ajustes do Bloqueio de Aplicativo

Para uma configuração avançada do desbloqueio de aplicativos:

1. Toque em **Mais** na barra de navegação inferior.
2. Toque em **Configurações**.

Na área de Desbloqueio de Aplicativos, você pode ajustar as seguintes opções:

- **Sugestão de aplicativo sensível** - receba uma notificação de bloqueio cada vez que você instalar um aplicativo sensível.
- **Solicitar desbloqueio sempre** - escolher uma das opções de bloqueio e desbloqueio disponíveis.
- **Desbloqueio Inteligente** - mantém os aplicativos desbloqueados enquanto você estiver conectado(a) a redes Wi-Fi.
- **Teclado aleatório** - previne a leitura do PIN ao mostrar os números de forma aleatória.

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 e acessar o recurso Bloqueio de Aplicativo.

Nota
Este recurso somente está disponível para telefones que têm uma câmera frontal.

Para configurar o recurso Tirar Foto para o Bloqueio de Aplicativos:

1. Toque em **Mais** na barra de navegação inferior.
2. Toque em **Configurações**.
3. Habilite o botão correspondente na área de Tirar Foto.

As fotos tiradas quando o PIN incorreto for inserido são exibidas na janela 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. Toque em no canto superior esquerdo da tela, e então selecione **Meus dispositivos**.
4. Selecione o seu dispositivo Android, e então, a aba **Antifurto**.
5. Toque ao lado de **Verificar suas fotos** para ver as últimas fotos tiradas.

Apenas as duas fotos mais recentes são salvas.

Para parar de fazer upload das fotos na sua conta Bitdefender:

1. Toque em **Mais** na barra de navegação inferior.

2. Toque em **Configurações**.
3. Desativar **Fazer upload das fotos** na área de Tirar Foto.

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 configurar o recurso Desbloqueio Inteligente:

1. Toque em **Mais** na barra de navegação inferior.
2. Toque em **Bloqueio de aplicativos**.
3. Toque em **ADICIONAR** para estabelecer a conexão Wi-Fi que você está usando como confiável.

Nota
Esta configuração somente estará disponível se o recurso Desbloqueio Inteligente estiver habilitado.

Quando você mudar de opinião, desabilite o recurso, e as redes Wi-Fi que você configurou como confiáveis serão tratadas como não-confiáveis.

28. 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. Toque em **Mais** na barra de navegação inferior.
2. Toque em **Relatórios**.

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.

  Para parar de receber notificações cada vez que for gerado um relatório:

  1. Toque em **Mais** na barra de navegação inferior.
  2. Toque em **Configurações**.
  3. Desativar o botão de **Notificação de novo relatório** na área de Relatórios.

- **REGISTRO DE ATIVIDADES** - aqui você poderá acessar informações detalhadas sobre as atividades do seu aplicativo Bitdefender Mobile Security desde quando foi instalado no seu dispositivo Android.

  Para eliminar o log de atividades:

  1. Toque em **Mais** na barra de navegação inferior.
  2. Toque em **Configurações**.
  3. Toque em **Limpar log de atividades**, e a seguir, toque em **LIMPAR**.

29. 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 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 detectará automaticamente o aplicativo no seu telefone e irá vibrar sempre que estiver muito longe do seu relógio e que o dispositivo perder a conectividade Bluetooth.

   Para habilitar esse recurso, abra o Bitdefender Mobile Security, 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.

30. SOBRE

Para mais informações sobre a versão do Bitdefender Mobile Security que você instalou, acesse e leia o Acordo de Assinatura e a Política de Privacidade e visualize as licenças Open-source:

1. Toque em **Mais** na barra de navegação inferior.
2. Toque em **Configurações**.
3. Toque na opção desejada na área Sobre.

31. 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, acessando https://central.bitdefender.com, ou diretamente pelo aplicativo da Bitdefender Central em dispositivos Android e iOS.

Para instalar o aplicativo da Bitdefender Central nos seus dispositivos:

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

Assim que fizer login, você pode começar a fazer o seguinte:

- Faça o download e instale o Bitdefender nos sistemas operacionais Windows, macOS, iOS e Android. Os produtos disponíveis para download são:
  - Bitdefender Mobile Security
  - Bitdefender Mobile Security para iOS
  - 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.
- Proteja os dispositivos de rede e seus dados contra roubo ou perda com o Antifurto.

Acessar sua conta Bitdefender

Há duas formas de acessar a Bitdefender Central

- No seu navegador da Internet:
  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.

- Em seu dispositivo Android ou iOS:

  Abra o aplicativo da Bitdefender Central que você instalou.

Nota
Com este material, você recebe as opções e instruções disponíveis na plataforma web.

Autenticação de dois fatores

O método de autenticação em 2 fatores adiciona uma camada extra de segurança à sua conta do Bitdefender, ao requerer um código de autenticação além das credenciais de login. Assim, você impedirá o roubo da conta e afugentará diversos tipos de ciberataques, como keyloggers, ataques de força bruta e de dicionário.

Ativar autenticação de dois fatores

Ao permitir a autenticação de dois fatores, você deixará a sua conta Bitdefender muito mais segura. Sua identidade será verificada cada vez que você fizer login em um dispositivo diferente, já seja para instalar um dos produtos Bitdefender, verificar o estado da sua assinatura ou executar tarefas remotamente nos seus dispositivos.

Para ativar a autenticação de dois fatores:

1. Acesse Bitdefender Central.
2. Pressione o ícone no canto superior direito da tela.
3. Clique em **Conta do Bitdefender** no menu deslizante.
4. Selecione a aba **Senha e segurança**.
5. Toque em **Autenticação em dois fatores**.
6. Toque em **COMEÇAR A USAR**.

   Selecione uma das seguintes opções:

   - **Aplicativo de autenticação** - use um aplicativo de autenticação para gerar um código cada vez que você quiser acessar a sua conta Bitdefender.

Caso você queira usar o aplicativo de autenticação, mas você não tem certeza de qual escolher, aparecerá uma lista com os aplicativos de autenticação recomendados.

a. Toque em **USAR APLICATIVO DE AUTENTICAÇÃO** para começar.

b. Para entrar em um dispositivo Android ou iOS, use o seu dispositivo para escanear o código QR.

Para acessar usando um laptop ou computador, você pode adicionar manualmente o código mostrado.

Pressione **CONTINUAR**.

c. Insira o código fornecido pelo aplicativo ou mostrado no passo anterior, e então toque em **ATIVAR**.

- **E-mail** - cada vez que você acessar a sua conta Bitdefender, o código de verificação será enviado à sua caixa de e-mail. Verifique a sua conta de e-mail e então digite o código que você recebeu.

a. Toque em **USAR E-MAIL** para começar.

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

Lembre que você possui cinco minutos para verificar a sua conta de e-mail e digitar o código gerado. Se o tempo expirar, você deverá gerar um novo link seguindo os mesmos passos.

c. Pressione **ATIVAR**.

d. Você receberá dez códigos de ativação. Você pode tanto copiar, baixar ou imprimir a lista e usá-la caso perca o seu endereço de e-mail, caso contrário você não poderá acessar. Cada código pode ser usado apenas uma vez.

e. Pressione **FEITO**.

Caso você queira parar de usar a autenticação de dois fatores:

1. Toque em **DESATIVAR A AUTENTICAÇÃO EM DOIS FATORES**.
2. Verifique o seu aplicativo ou conta de e-mail e digite o código que você recebeu.

   Caso você tenha escolhido receber o código de autenticação por e-mail, você terá cinco minutos para verificar a sua conta de e-mail e digitar o código gerado. Se o tempo expirar, você deverá gerar um novo link seguindo os mesmos passos.

3. Confirme sua escolha.

Adicionando dispositivos confiáveis

Para garantir que apenas você pode acessar a sua conta Bitdefender, pode ser que solicitemos o código de segurança antes. Caso queira pular este passo cada vez que se conectar com o mesmo dispositivo, nós recomendamos cadastrá-lo como um dispositivo confiável.

Para adicionar dispositivos confiáveis:

1. Acesse Bitdefender Central.
2. Pressione o ícone no canto superior direito da tela.
3. Clique em **Conta do Bitdefender** no menu deslizante.
4. Selecione a aba **Senha e segurança**.
5. Pressione **Dispositivos confiáveis**.
6. Será mostrada a lista com os dispositivos Bitdefender instalados. Toque no dispositivo desejado.

Você pode adicionar quantos dispositivos desejar, contanto que eles tenham o Bitdefender instalado e sua assinatura seja válida.

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 do dispositivo mostram o nome do dispositivo, o estado de proteção e se há algum risco de segurança afetando a proteção dos seus dispositivos.

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

1. Acesse Bitdefender Central.
2. Toque em no canto superior esquerdo da tela, e então selecione **Meus dispositivos**.
3. Toque no cartão de dispositivo desejado, e a seguir toque em no canto superior direito na tela.
4. Selecione **Configurações**.

5. Digite um novo nome no campo **Nome do dispositivo**, e logo selecione **SALVAR**.

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

1. Acesse Bitdefender Central.
2. Toque em ☰ no canto superior esquerdo da tela, e então selecione **Meus dispositivos**.
3. Toque no cartão de dispositivo desejado, e a seguir toque em ⋮ no canto superior direito na tela.
4. Selecione **Perfis**.
5. Toque em **Add owner** e, em seguida, preencha os respetivos campos. Customize o perfil adicionando uma foto e selecionando a data de nascimento.
6. Pressione **ADICIONAR** para salvar o perfil.
7. 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 visualizar os detalhes sobre o dispositivo selecionado, verificar seu estado de proteção, o estado do Bitdefender VPN e quantas ameaças foram bloqueadas nos últimos sete dias. O estado de proteção pode estar verde, quando não houver problemas afetando seu dispositivo, amarelo, quando o dispositivo requerer sua atenção, ou vermelho, quando o dispositivo estiver em risco. Quando houver problemas afetando o seu dispositivo, clique a seta suspensa na área de estado acima para saber 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 **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.

- **Antifurto**. 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, acesse "*Recursos Antifurto*" (p. 272).

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 nele, como descrito em "Instalando o Bitdefender Mobile Security" (p. 259).

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.

32. PERGUNTAS MAIS FREQÜENTES

Por que o Bitdefender Mobile Security 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 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 proteção na Web apaga sites maliciosos do seu histórico de navegação.
- Ler o registro de dados -> o Bitdefender Mobile Security detecta traços de atividades de ameaças dos registros Android.
- Localização -> Necessária para localização remota.
- Câmera -> necessária para tirar foto.
- Armazenamento -> usado para permitir que o Verificador de Malware verifique o cartão SD.

Como posso parar de mandar informação para o Bitdefender sobre aplicativos suspeitos?

Segundo a definição padrão, o Bitdefender Mobile Security envia relatórios para servidores do Bitdefender sobre os aplicativos suspeitos que você está instalando. Essas informações são essenciais para melhorar a detecção de ameaças e podem nos ajudar a lhe oferecer uma experiência melhor no futuro. Caso você queira parar de nos enviar informação sobre aplicativos suspeitos:

1. Toque em **Mais** na barra de navegação inferior.
2. Toque em **Configurações**.
3. Desligue a **Detecção na nuvem** na área e Verificação de Malware.

Onde posso ver mais informações sobre a atividade do aplicativo?

O Bitdefender Mobile Security mantém um registro de todas as ações importantes, mudanças de status e outras mensagens críticas relacionadas à sua atividade. Para acessar, veja as atividades do aplicativo:

1. Toque em **Mais** na barra de navegação inferior.
2. Toque em **Relatórios**.

   Na janela de RELATÓRIOS SEMANAIS, você pode acessar os relatórios gerados semanalmente, e na janela de LOG DE ATIVIDADES você pode ver informações sobre as atividades do seu aplicativo Bitdefender.

Esqueci o código PIN que defini para proteger meu aplicativo. What do I do?

1. Acesse Bitdefender Central.
2. Toque em no canto superior esquerdo da tela, e então selecione **Meus dispositivos**.
3. Toque no cartão de dispositivo desejado, e a seguir toque em no canto superior direito na tela.
4. Selecione **Configurações**.
5. Recupere o PIN no campo **PIN de Aplicativo**.

Como posso mudar o código PIN que eu estabeleci para o Bloqueio de Aplicativos e Antifurto?

Se você quiser mudar o código PIN que você estabeleceu para o Bloqueio de Aplicativos e Antifurto:

1. Toque em **Mais** na barra de navegação inferior.
2. Toque em **Configurações**.
3. Toque no **CÓDIGO PIN** de segurança na área de Antifurto.
4. Insira o novo código PIN.
5. Insira o novo código que você quer estabelecer.

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?

Primeiro, você deve conectar seu dispositivo à rede Wi-Fi que você quer estabelecer como confiável. A seguir, siga esses passos:

1. Toque em **Mais** na barra de navegação inferior.
2. Toque em **Bloqueio de aplicativos**.
3. Toque em no canto superior direito.
4. Toque em **ADICIONAR** ao lado da rede que você deseja definir como confiável.

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. Toque em 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**.

Como posso proteger minhas compras online?

Fazer compras online traz altos riscos quando alguns detalhes são ignorados. Para não se tornar uma vítima de fraude, recomendamos as seguintes medidas:

- Mantenha o seu aplicativo de segurança atualizado.
- Faça pagamentos online somente com proteção do comprador.
- Use uma VPN quando se conectar à internet de redes sem fio públicas ou não seguras.
- Preste atenção às senhas que você designou para suas contas online. Elas precisam ser fortes, incluindo letras maiúsculas e minúsculas, números e símbolos (@, !, %, #, etc.).
- Certifique-se de que as informações que você envia são em conexões seguras. A extensão online do website deve ser HTTPS:// e não HTTP://.

Quando devo usar o Bitdefender VPN?

Você precisa ter cuidado quando acessa, baixa ou envia conteúdos na internet. Para garantir que você fique em segurança enquanto navega na web, recomendamos usar o Bitdefender VPN quando você:

- quiser se conectar a redes sem fio públicas
- quiser acessar conteúdos que normalmente são restritos em áreas específicas, não importa se estiver em casa ou fora
- quiser manter seus dados pessoais privados (nomes de usuário, senhas, informações de cartão de crédito, etc.)
- desejar esconder seu endereço IP

O Bitdefender VPN vai ter um impacto negativo na bateria do meu dispositivo?

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

Por que estou encontrando lentidão na internet enquanto uso o Bitdefender VPN?

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

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. Toque em **Mais** na barra de navegação inferior.
2. Toque no seu endereço de e-mail.
3. Toque em **Sair da sua conta**. Se um código PIN tiver sido configurado, será solicitado que você o utilize.

4. Confirme sua escolha.
5. Digite o endereço de e-mail e a senha da sua conta nos campos correspondentes, e então pressione **ENTRAR**.

Como o Bitdefender Mobile Security 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 não roda em plano de fundo quando você liga para amigos, envia mensagens ou joga.

O que é o Administrador de Aparelho?

O Administrador de Aparelhos é um recurso para Android que concede ao Bitdefender Mobile Security 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**.

Como solucionar o erro "Nenhum Token Google" que aparece ao fazer login no Bitdefender Mobile Security.

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 Congigurações > do Android; Aplicativos > Gerenciar Aplicativos > Bitdefender Mobile Security 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.
- Reinicie seu dispositivo e depois tente entrar novamente.

Em que idiomas o Bitdefender Mobile Security está disponível?

O Bitdefender Mobile Security está disponível atualmente nos seguintes idiomas:

- Brasileiro
- Tcheco(a)
- Holandês
- Português
- Francês
- Alemão
- Grego
- Húngaro(a)
- Italiano
- Japonês
- Coreano
- Polonês
- Português
- Romeno
- Russo
- Espanhol
- Sueco
- Tailandês
- Turco
- Vietnamita

Outros idiomas serão adicionados em versões futuras. Para alterar o idioma da interface do Bitdefender Mobile Security, acesse as configurações do seu aparelho **Idioma & teclado** e defina o idioma que deseja usar no aparelho.

CONTATE-NOS

33. 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. 162) fornece as informações necessárias em relação às incidências mais frequentes que poderá encontrar ao utilizar este produto.

Se você não encontrar uma resposta à sua pergunta nos recursos oferecidos, você pode nos contactar ligando para **(+1)800 839 6823**ou enviando um e-mail para soho@bitdefender.com. Ou então, fale conosco diretamente:

- "Contate conosco diretamente no Bitdefender Total Security" (p. 300)
- "Contate-nos através do nosso Centro de Suporte Online" (p. 301)

Contate conosco diretamente no Bitdefender Total Security

Se possuir uma conexão ativa com a Internet, você pode entrar em contato com o suporte do Bitdefender diretamente da interface do produto.

Siga esses passos:

1. Clique em **Suporte** no menu de navegação da interface do Bitdefender.
2. Você tem as seguintes opções:
   - **GUIA DO USUÁRIO**

     Acesse nossa base de dados e procure a informação necessária.
   - **CENTRO DE SUPORTE**

     Acesse nossos artigos e vídeos de tutoriais online.
   - **CONTATAR O SUPORTE**

     Clique em **CONTATAR SUPORTE** para abrir a Ferramenta de Suporte do Bitdefender e entrar em contato com o Departamento de Atendimento ao Cliente.

a. Complete o formulário de envio com os dados necessários:

   i. Selecione o tipo de problema que você encontrou.

   ii. Digite uma descrição do problema encontrado.

   iii. Clique em **TENTAR REPRODUZIR ESSE PROBLEMA** caso você esteja encontrando um problema no produto. Reproduza a incidência, e então, clique em **FINALIZAR** no quadro REPRODUZINDO A INCIDÊNCIA.

   iv. Clique em **CONFIRMAR INCIDÊNCIA**.

b. Continue completando o formulário com os dados necessários:

   i. Digite seu nome completo.

   ii. Digite seu endereço de email.

   iii. Marque a caixa de consenso com o acordo.

   iv. Clique em **CRIAR PACOTE DE DEBUG**.

   Aguarde alguns minutos enquanto o Bitdefender reúne informações relacionadas ao produto. Esta informação irá ajudar os nossos engenheiros a encontrar uma solução para o seu problema.

c. Clique em **FECHAR** para sair do assistente. Um dos nossos representantes entrará em contato com você o mais breve possível.

Contate-nos através do nosso Centro de Suporte Online

Caso não consiga acessar as informações necessárias usando o produto Bitdefender, entre em contato com nosso Centro de Suporte:

1. Vá para https://www.bitdefender.com/support/consumer.html.

   O Centro de Suporte doBitdefender armazena inúmeros artigos que contém soluções para as questões relacionadas ao Bitdefender.

2. Utilize a barra de pesquisa na parte superior da janela para encontrar artigos que possam fornecer uma solução definitiva para seu problema. Para pesquisar, apenas digite o termo na barra de pesquisa e clique em **Pesquisar**.

3. Leia os artigos ou os documentos e experimente as soluções propostas.

4. Se a solução não resolver seu problema, acesse

   https://www.bitdefender.com/support/contact-us.htmle contate nossos representantes de suporte.

34. 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.

34.1. Centro de Suporte Bitdefender

O Centro de Suporte do Bitdefender é um repositóio de informação online sobre os produtos Bitdefender. Armazena, num formato facilmente acessível, 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 ameaças, 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 freqüência. A informção extensiva que ele contêm 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.

34.2. 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 certas ameaças do seu computador ou se tiver alguma questão sobre a forma como opera, coloque o seu problema ou a sua questão no fórum.

Os técnicos de 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, 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.

34.3. 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.

35. INFORMAÇÃO SOBRE CONTATO

A comunicação eficiente é a chave para um negócio de sucesso. Desde 2001, a BITDEFENDER estabeleceu uma reputação sólida ao visar constantemente uma comunicação melhor, excedendo, assim, as expectativas dos nossos clientes e parceiros. Por favor, não hesite em nos contactar sobre quaisquer assuntos ou dúvidas que você possa ter.

35.1. Endereços da Rede

Departamento de Vendas: sales@bitdefender.com
Centro de Suporte:https://www.bitdefender.com/support/consumer.html
Documentação: documentation@bitdefender.com
Distribuidores locais:https://www.bitdefender.com/partners
Programa de parcerias: partners@bitdefender.com
Relações com a mídia: pr@bitdefender.com
Carreiras: jobs@bitdefender.com
Envio sobre ameaças: virus_submission@bitdefender.com
Envio de spam: spam_submission@bitdefender.com
Relato de abuso: abuse@bitdefender.com
Website:https://www.bitdefender.com

35.2. 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 email sales@bitdefender.com. Escreva a sua mensagem em inglês para podermos responder imediatamente.

35.3. 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
Suporte Técnico: https://www.bitdefender.com/support/consumer.html
Página da Web https://www.bitdefender.com

UK e Irlanda

BITDEFENDER LTD
C/O Howsons Winton House, Stoke Road, Stoke on Trent
Staffordshire, United Kindon, ST4 2RW
E-mail: info@bitdefender.co.uk
Telefone: (+44) 2036 080 456
Vendas: sales@bitdefender.co.uk
Suporte Técnico: https://www.bitdefender.co.uk/support/
Página da Web https://www.bitdefender.co.uk

Alemanha

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Escritório: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Vendas: vertrieb@bitdefender.de
Suporte Técnico: https://www.bitdefender.de/support/consumer.html
Página da Web https://www.bitdefender.de

Dinamarca

Bitdefender APS
Agern Alle 24, 2970 Hørsholm, Denmark
Escritório: +45 7020 2282
Suporte Técnico: http://bitdefender-antivirus.dk/
Página da Web http://bitdefender-antivirus.dk/

Espanha

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Telefone: +34 902 19 07 65
Vendas: comercial@bitdefender.es
Suporte Técnico: https://www.bitdefender.es/support/consumer.html
Website: https://www.bitdefender.es

Romênia

BITDEFENDER SRL
Orhideea Towers, 15A Orhideelor Street, Sector 6
Bucharest
Fax: +40 21 2641799
Telefone de Vendas: +40 21 2063470
E-mail de vendas: sales@bitdefender.ro
Suporte Técnico: https://www.bitdefender.ro/support/consumer.html
Website: https://www.bitdefender.ro

Emirados Arabes Unidos

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
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 aplicativo host gratuito enquanto o usuário concordar em aceitar o adware. Não existem implicações penais neste tipo de instalação, pois o usuário concordou com o acordo de licença que afirma o propósito do aplicativo.

No entanto, propagandas do tipo “pop-up” podem se tornar uma inconveniência, e em alguns casos afetar o desempenho do seu sistema. Além disto, as informações que alguns destes programas coletam podem causar problemas de privacidade a usuários que não estão totalmente cientes do funcionamento do programa.

Ameaça

Um programa ou pedaço de código que é carregado no seu computador sem o seu conhecimento e é executado contra a sua vontade. A maioria das ameaças também podem se duplicar. Todos as ameaças de computador são criadas pelo homem. É fácil criar uma simples ameaça que pode se reproduzir uma e outra vez. Mesmo uma simples ameaça é perigosa, porque pode rapidamente usar toda memória disponível e fazer o sistema parar. O tipo de ameaça mais perigoso é aquele que é capaz de transmitir-se através de uma rede ou contornando sistemas de segurança.

Ameaça persistente avançada

A ameaça persistente avançada (APA) explora as vulnerabilidades dos sistemas para roubar informações importantes e fornecê-las à fonte. Grandes grupos como organizações, empresas ou governos são os alvos desta ameaça.

O objetivo de uma ameaça persistente avançada é permanecer não detectada por um longo período, sendo capaz de monitorar e coletar informações importantes sem danificar as máquinas atacadas. O método usado para injetar a ameaça na rede é através de um arquivo PDF ou documento do Office que pareça inofensivo, de forma que todo usuário possa abrir esses arquivos.

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.

Ataque de dicionário

Um ataque de adivinhação de senha foi usado para invadir o sistema de um computador inserindo uma combinação de palavras comuns para gerar possíveis senhas. O mesmo método é usado para adivinhar chaves de criptografia de mensagens ou documentos encriptados. Ataques de dicionário dão certo devido à tendência de muitas pessoas escolherem senhas curtas ou de uma palavra que acabam sendo fáceis de serem adivinhadas.

Ataque de força bruta

Um ataque de adivinhação de senha foi usado para invadir o sistema de um computador inserindo possíveis combinações de senha, começando pelas mais fáceis de se adivinharem.

Atualização da informação sobre a ameaça

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

Atualizações

Uma nova versão de um produto de hardware ou software feita 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 tem o seu recurso próprio de atualização que lhe permite conferir atualizações manualmente, ou deixar que ele atualize o programa automaticamente.

Backdoor

Um furo na segurança do sistema deixado deliberadamente pelos desenvolvedores ou mantenedores. A motivação para tais furos não é sempre sinistra; alguns sistemas operacionais, por exemplo, saem com contas privilegiadas para uso de técnicos ou de programadores de manutenção do distribuidor.

Bandeja do sistema

Introduzido com o Windows 95, a bandeja do sistema está localizada 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 um clique duplo ou clique com o botão direito do mouse sobre o ícone para ver e acessar os detalhes e controles.

Botnet

O termo “botnet” é composto das palavras “robot” (robô) e “network” (rede). Os botnets são dispositivos conectados à internet infectados por ameaças e podem ser usados para enviar e-mails de spam, roubar dados, controlar dispositivos vulneráveis remotamente ou espalhar spyware, ransomware e outros tipos de ameaças. Seu objetivo é infectar o máximo de dispositivos conectados possível, como PCs, servidores, dispositivos móveis ou IoT pertencentes a grandes empresas e indústrias.

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.

Cavalo de Tróia

Um programa destrutivo que se esconde sob um aplicativo benigno. Diferentemente de programas maliciosos e worms, os Cavalos de Troia não se replicam, mas podem ser tão destrutivos quanto eles. Um dos tipos mais traiçoeiros de ameaças do tipo Cavalo de Troia é um programa que promete remover ameaças do seu computador, mas em vez disso, introduz ameaças nele.

O termo vem da história de Ilíada de Homero, na qual os gregos deram um cavalo de madeira gigante a seus inimigos, os troianos, como uma oferta de paz. Mas depois que os 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.

Cliente de e-mail

É um aplicativo que lhe permite enviar e receber emails.

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, 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 declarados. É uma faca de

dois gumes para muitos, porque por um lado é eficiente e pertinente - você só vê anúncios que lhe interessam. Por outro lado, isso envolve "rastrear" e "seguir" aonde você vai e no que você clica. 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 ele é preciso.

Cyberbullying

Quando colegas ou estranhos estão cometendo atos abusivos contra crianças de propósito para feri-las fisicamente. Para causar danos emocionais, os agressores enviam mensagens ou fotos mal-intencionadas, que fazem com que suas vítimas se isolem de outros e se sintam frustradas.

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 do usuário, tais como clicar com um botão do mouse ou pressionar uma tecla, ou ocorrências do sistema, como falta de memória.

Explorações

Trata-se de uma forma de se aproveitar de diferentes bugs e vulnerabilidades presentes num computador (software ou hardware). Assim, os hackers podem ganhar controle de computadores ou redes.

Extensão do arquivo

É a parte do arquivo, após o ponto final, indicando o tipo de dados que estão armazenados no arquivo.

Muitos sistemas operacionais usam extensões de arquivos, ex. Unix, VMS, MS-DOS. Eles consistem geralmente 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 um programa de análise identifica um arquivo infectado quando de fato não está.

Heurística

Um método baseado em regras para identificar novas ameaças. Este método de verificação não utiliza um banco de dados de informações de ameaças específico. A vantagem da verificação heurística é que ela não pode ser enganada por uma nova variante de uma ameaça existente. Entretanto, ela pode relatar um código suspeito em um programa normal, gerando assim um chamado "falso positivo".

IP

Protocolo de Internet - Um protocolo roteável no conjunto do protocolo TCP/IP que é responsável pelo endereçamento IP, roteamento, 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 você digita.

Os keyloggers não são maliciosos por natureza. Eles 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 números de identificação pessoal).

Linha de comando

Na interface de linha de comando, os usuários digitam os comandos em um espaço fornecido diretamente na tela usando linguagem de comando.

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

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

Navegador

Termo simplificado para navegador da web, uma aplicação de software utilizada 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. Além disso, os navegadores mais modernos podem apresentar informações multimídia, como som e vídeo, embora exijam plugins para alguns formatos.

Pasta

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.

Phishing

O ato de enviar um e-mail a um usuário que mente afirmando ser uma empresa legítima e estabelecida, em uma tentativa de convencer o usuário a oferecer informações privadas que serão usadas para fins fraudulentos. O email encaminha o usuário a um website no qual deve atualizar suas informações pessoais, como senhas e números de cartão de crédito, números de identidade e números de contas bancárias que a organização legítima já possui. A página web, no entanto, é falsa e existe apenas para roubar informações do usuário.

Photon

Photon é uma tecnologia inovadora não-intrusiva da Bitdefender, projetado para minimizar o impacto da solução de segurança 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 à 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, mouses e outros dispositivos periféricos.

Em redes TCP/IP e UDP, um endpoint de uma conexão lógica. O número da porta identifica o tipo da porta. Por exemplo, a porta 80 é usada para o 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.

Predadores online

Pessoas que procuram atrair menores de idade ou adolescentes para conversas com o objetivo de envolvê-los em atividades sexuais ilegais. As redes sociais são o foro ideal para caçar e seduzir facilmente crianças vulneráveis para cometer atividades sexuais, tanto online ou cara a cara.

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 email indesejado, baixando anexos de email 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 pela primeira vez nos sistemas operativos UNIX e referia-se a ferramentas recompiladas que proporcionavam direitos de administração aos intrusos, 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 relatórios. Eles também podem interceptar dados dos terminais, ligações de rede ou periféricos, se eles incorporarem o software adequado.

Os rootkits não são maliciosos por natureza. Por exemplo, os sistemas e mesmo alguns aplicativos ocultam arquivos críticos usando rootkits. No entanto, eles são essencialmente utilizados para ocultar ameaças ou para esconder a presença de um intruso no sistema. Quando combinados com ameaças, 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 evitar sua detecção.

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 início de cada disco que identifica a arquitetura do disco (tamanho do setor, tamanho do cluster, e assim por diante). Para discos de inicialização, o setor de boot também contém um programa que carrega o sistema operacional.

Spam

Lixo eletrônico em forma de mensagens. 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 fins 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 também pode coletar informações sobre endereços de e-mail, senhas e números de cartão de crédito.

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 em execução podem levar o sistema ao colapso ou instabilidade geral.

TCP/IP

Transmission Control Protocol/Internet Protocol (Protocolo de Controle de Transmissão/Protocolo de Internet) - 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 normas sobre como os computadores se comunicam e convenções para conectar redes e direcionar o tráfego.

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 espiões. Uma prova de segurança é a autenticação, que pode ser feita somente com o uso de um nome de usuário e senha.

Vírus de boot

Uma ameaça 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 a ameaça se torne ativa na memória. Toda vez que você ligar o seu sistema daquele ponto em diante, você terá uma ameaça ativa na memória.

Vírus de macro

Um tipo de ameaça de computador que é codificada como uma macro dentro de um documento. Muitos aplicativos, como Microsoft Word e Excel, suportam poderosas linguagens de macro.

Esses aplicativos permitem que você coloque uma macro em um documento, e mandam a macro ser executada cada vez que o documento é aberto.

Vírus polimórfico

Uma ameaça que muda sua forma a cada arquivo infectado. Como eles não têm nenhum padrão binário consistente, tais ameaças são difíceis de identificar.

Worm

Um programa que se propaga pela rede, se reproduzindo enquanto avança. Ele não pode se anexar a outros programas.