Bitdefender ANTIVIRUS PLUS

GUIA DO USUÁRIO

Bitdefender Antivirus Plus
Guia do Usuário

Data de Publicação 07/20/2020

Aviso Legal

Bitdefender

Índice

INSTALAÇÃO

1. PREPARANDO A INSTALAÇÃO

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

- Assegure-se de que o dispositivo no qual deseja instalar o Bitdefender tenha os requisitos mínimos de sistema. Caso o dispositivo não atenda aos requisitos 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. 3).
- Acesse o dispositivo utilizando uma conta de Administrador.
- Remova qualquer outro software similar do seu dispositivo. 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.
- Recomenda-se que o seu dispositivo 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.

2. REQUISITOS DE SISTEMA

Você pode instalar o Bitdefender Antivirus Plus apenas nos dispositivos com os seguintes sistemas operacionais:

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

- 2,5 GB de espaço disponível em disco rígido (pelo menos 800 MB no drive do sistema)
- 2 GB de memória (RAM)

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

Nota
Para saber qual é o sistema operacional Windows do seu dispositivo 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.

2.1. Requisitos de Software

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

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

- Google Chrome 34 e superior

3. INSTALANDO SEU PRODUTO BITDEFENDER

Você pode instalar o Bitdefender com o disco de instalação, ou usar o instalador da internet baixado no seu dispositivo na Bitdefender Central.

Se sua compra incluir mais de um dispositivo (por exemplo, você comprou o Bitdefender Antivirus Plus para três computadores), repita o processo de instalação e ative seu produto com a mesma conta em todos os dispositivos. A conta a ser usada deve ser a mesma que contém sua assinatura ativa do Bitdefender.

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 Antivirus Plus é ativado.

Para baixar o Bitdefender Antivirus Plus 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 do sistema para a instalação do Bitdefender, você será informado das áreas que precisam 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 dispositivo para concluir a remoção das soluções de segurança detectadas.

O pacote de instalação do Bitdefender Antivirus Plus 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 Antivirus Plus:

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 Antivirus Plus.

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.

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.

Passo 4 - Verificação do dispositivo

Agora, você será perguntado se deseja realizar uma verificação no seu dispositivo para garantir que ele esteja seguro. Durante este passo, o Bitdefender irá verificar áreas críticas do sistema. Clique em **Iniciar verificação do dispositivo** para começar.

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

Quando a verificação estiver concluída, clique em **Abrir interface do Bitdefender**.

Nota

De forma alternativa, se você não desejar realizar a verificação, você pode simplesmente clicar em **Pular**.

Passo 5 - Introdução

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

Clique em **FINALIZAR** para acessar a interface do Bitdefender Antivirus Plus.

3.2. Instale a partir do disco de instalação.

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

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

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

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

Validando a instalação

O Bitdefender primeiro verificará seu sistema para validar a instalação.

Se o seu sistema não apresenta os requisitos do sistema para a instalação do Bitdefender, você será informado das áreas que precisam 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 dispositivo para concluir a remoção das soluções de segurança detectadas.

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 Antivirus Plus:

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 Antivirus Plus.

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.

Passo 3 - Instalação concluída

É apresentado um resumo da instalação. Se uma ameaça ativa tiver sido detectada e removida durante a instalação, pode ser necessário reiniciar o sistema.

Passo 4 - Verificação do dispositivo

Agora, você será perguntado se deseja realizar uma verificação no seu dispositivo para garantir que ele esteja seguro. Durante este passo, o Bitdefender irá verificar áreas críticas do sistema. Clique em **Iniciar verificação do dispositivo** para começar.

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

Quando a verificação estiver concluída, clique em **Continuar com a criação da conta**.

Nota
De forma alternativa, se você não desejar realizar a verificação, você pode simplesmente clicar em **Pular**.

Passo 5 - conta Bitdefender

Após completar a configuração inicial, aparecerá a janela da Conta do Bitdefender. Uma conta Bitdefender é necessária para ativar o produto e usar suas ferramentas online. Para mais informações, acesse "*Bitdefender Central*" (p. 30).

Proceda de acordo com sua situação.

- **Quero criar uma conta Bitdefender**

  1. Digite as informações necessárias nos campos correspondentes. Os dados que nos fornecer serão mantidos confidenciais. A senha deve ter no mínimo 8 caracteres, incluindo ao menos um número ou símbolo, um caractere minúsculo e um maiúsculo.
  2. 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.
  3. Clique em **CRIAR CONTA**.

Nota
Uma vez criada a conta, você poderá usar o endereço de e-mail e senha fornecidos para entrar na sua conta em https://central.bitdefender.com, ou no aplicativo da Bitdefender Central desde que esteja instalado em um dos seus dispositivos Android ou iOS. Para instalar o app Bitdefender Central no Android, você precisa acessar o Google Play, pesquisar por Bitdefender Central e depois tocar na opção de instalação correspondente. Para instalar o app da Bitdefender Central no iOS, você precisa acessar a App Store, pesquisar por Bitdefender Central e depois tocar na opção de instalação correspondente.

- **Já tenho uma conta Bitdefender**

  1. Clique em **Entrar**.
  2. Digite o endereço de e-mail no campo correspondente e clique em **PRÓXIMO**.
  3. Digite sua senha, depois clique em **ENTRAR**.

     Se tiver esquecido a senha da sua conta ou caso queira redefini-la:

     a. Clique em **Esqueceu a senha?**.

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

     c. 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.

     d. Digite a nova senha que deseja estabelecer, e em seguida digite-a novamente. Clique em **SALVAR**.

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

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

  Para entrar com sua conta Microsoft, Facebook ou Google:

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

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

Etapa 6 - Ative o seu produto

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

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

Proceda conforme sua situação:

- Tenho um código de ativação

  Neste caso, ative o produto seguindo estas etapas:

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

     > **Nota**
     > Você pode encontrar seu código de ativação:
     > - na etiqueta do CD/DVD.
     > - No cartão de registro do produto.
     > - no email da sua compra on-line.

  2. **Desejo avaliar o Bitdefender**

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

Passo 7 - Introdução

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

Clique em **FINALIZAR** para acessar a interface do Bitdefender Antivirus Plus.

INTRODUÇÃO

4. O BÁSICO

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

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. Isso se deve principalmente porque fraudadores podem estar observando suas atividades para 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. 123).

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. 113) carteira. Com uma única senha-mestre você pode proteger sua privacidade de invasores que podem tentar deixá-lo sem dinheiro.

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 Segurança Wi-Fi*" (p. 105).

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. 110).

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. 133).

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. 16).

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 dispositivo e seus dados.

Para usar as ferramentas online do Bitdefender Antivirus Plus e gerenciar suas assinaturas e dispositivos, acesse sua conta Bitdefender. Para mais informações, acesse "*Bitdefender Central*" (p. 30).

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

4.1. Abrindo a janela do Bitdefender

Para acessar a interface principal do Bitdefender Antivirus Plus, clique no ícone no seu desktop.

Se necessário, você também pode seguir os passos abaixo:

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

4.2. Notificações

O Bitdefender mantém um registro detalhado dos eventos relacionados com a sua atividade no seu dispositivo. 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 dispositivo, 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 2.

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.

4.3. 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.

4.3.1. 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.

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

Você pode clicar em **NÃO AGORA** se quiser ativar o recurso mais tarde.

Para permitir que o Bitdefender ative perfis automaticamente:

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

2. Na aba **Perfis**, clique em **Configurações**.
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. Dos primeiros três perfis, apenas um pode ser imediatamente ativado de forma manual.

Para mais informações sobre Perfis, por favor, acesse"*Perfis*" (p. 133)

4.4. Configurações de proteção da senha do Bitdefender

Se você não é a única pessoa a usar esse dispositivo 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.

4.5. 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**.

4.6. 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.

5. INTERFACE BITDEFENDER

Bitdefender Antivirus Plus 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 a área de configurações, notificações e as sessões do Bitdefender para configurações detalhadas e tarefas administrativas avançadas.

Na parte superior da interface principal, você pode acessar a sua conta Bitdefender. E você também pode nos contatar para obter suporte caso tenha perguntas ou algo inesperado apareça.

5.1. 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:

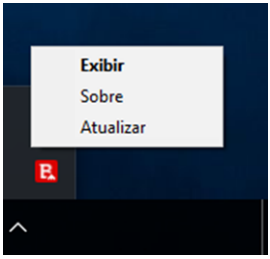
- No **Windows 7, Windows 8 e Windows 8.1**:
  1. Clique na seta no canto inferior direito da tela.
  2. Clique **Personalizar...** para abrir a janela de ícones da Área de Notificação.

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 **Configurações da barra de tarefas**.
2. Role para baixo e clique no link **Selecionar os ícones que aparecem na barra de tarefas** Na **Área de notificações**.
3. 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.



Ícone da área de notificação

- **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.
- **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 dispositivo 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.

5.2. 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 rapidamente problemas de segurança, ver recomendações de acordo com as necessidades do seu sistema e padrões de uso e realizar ações rápidas.
-
- **Proteção**. Aqui, você pode executar e configurar verificações antivírus, recuperar dados criptografados por ransomware e configurar a proteção enquanto você navega na internet.
- **Privacidade**. Aqui, você pode criar gerenciadores de senhas para suas contas online, fazer pagamentos online em um ambiente online e abrir o aplicativo do VPN.
- **Utilidades**. Aqui, você pode gerenciar perfis e acessar o recurso de Proteção de Dados.
- **Notificações**. É possível acessar daqui as notificações geradas.
- **Configurações**. É possível acessar daqui as configurações gerais.

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

- **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 Antivirus Plus.
- **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.

5.3. 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 dispositivo.

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.

5.3.1. Área de status de segurança

O Bitdefender utiliza um sistema de rastreio de problemas para detectar e lheinformar sobre os problemas que podem afetar a segurança do seu dispositivo e dados. 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 dispositivo, 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.

5.3.2. Autopilot

Para lhe oferecer uma operação efetiva e proteção reforçada enquanto realiza diferentes atividades, o Bitdefender Autopilot agirá como o seu consultor de segurança pessoal. Dependendo da atividade que 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**.

5.3.3. Ações rápidas

Usando as ações rápidas você pode executar com rapidez tarefas que considera importantes para manter seu sistema protegido e melhorar sua forma de trabalhar.

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 dispositivo.
- **Verificação do sistema**. Execute uma verificação do sistema para garantir que o dispositivo esteja livre de ameaças.

- **Analisar Vulnerabilidade**. Verifique seu dispositivo para identificar vulnerabilidades e assegurar que todos os aplicativos instalados, além do sistema operacional, estejam atualizados e funcionando corretamente.
- **Consultor de Segurança do Wi-Fi**. Abra a janela do Consultor de Segurança do Wi-Fi no módulo de Vulnerabilidade.
- **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 dispositivo.

Para começar a proteger dispositivos adicionais com o Bitdefender:

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

   Uma nova janela aparecerá na sua tela.

2. Pressione **COMPARTILHAR LINK DE DOWNLOAD**.

3. Siga os passos na tela para instalar o Bitdefender.

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

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

5.4. 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

5.4.1. Proteção

Na seção Proteção, você pode ajustar suas configurações avançadas de segurança, os recursos da Prevenção Contra Ameaças Online, conferir e reparar as vulnerabilidades potenciais do sistema e avaliar a segurança das redes sem fio às quais você 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
- Ambiente de Resgate

Para mais informações sobre tarefas de análise e como configurar a proteção antivírus, consulte "*Proteção Antivírus*" (p. 74).

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 Ameaças Online*" (p. 98).

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 contra Ameaças*" (p. 95).

VULNERABILIDADE

O módulo Vulnerabilidade o ajuda a manter seu sistema operacional e os aplicativos que usa regularmente atualizados, e a identificar as redes sem fio inseguras às quais se conecta. Clique em **Abrir** no módulo de Vulnerabilidade para acessar as suas funcionalidades.

A funcionalidade de **Verificação de Vulnerabilidades** permite identificar atualizações essenciais do Windows, atualizações de aplicativos, senhas fracas pertencentes a contas do Windows e redes sem fio não seguras. Clique em **Iniciar Verificação** para realizar uma verificação no seu dispositivo.

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

Para mais informações sobre como configurar a proteção de vulnerabilidade, consulte "*Vulnerabilidade*" (p. 101).

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. 110).

5.4.2. Privacidade

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

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. 123).

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. 113).

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. 126).

ANTITRACKER

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

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

5.4.3. Utilitários

Proteção de Dados

O Destruidor de Arquivos do Bitdefender o ajuda a apagar dados permanentemente removendo-os fisicamente de seu disco rígido.

Para mais informações, acesse "*Proteção de Dados*" (p. 140).

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.

Para mais informações sobre esse recurso, acesse "*Perfis*" (p. 133).

5.5. 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.

6. 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 dispositivo 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 Plus
  - 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.

6.1. 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.

6.2. Autenticação de dois fatores

O método de autenticação em 2 fatores adiciona uma camada extra de segurança à sua conta do Bitdefender, ao 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 desktop, 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.

6.2.1. 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.

6.3. Minhas assinaturas

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

6.3.1. Verificar assinaturas disponíveis

Para verificar suas assinaturas disponíveis:

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

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

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

Nota
É possível ter uma ou mais assinaturas na sua conta, desde que sejam para plataformas diferentes (Windows, macOS, iOS ou Android).

6.3.2. Adicionar novo dispositivo

Caso sua assinatura cubra mais de um dispositivo, você pode adicionar um novo dispositivo e instalar seu Bitdefender Antivirus Plus 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:

6.3.3. Renove assinatura

Caso você tenha desabilitado a renovação automática da sua assinatura do Bitdefender, você pode renová-la manualmente seguindo esses passos:

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.

6.3.4. 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.

6.4. 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 Seção 13.2.3, "*Executando uma Análise do Sistema*" e "*Executar uma Análise Rápida*" (p. 80).
- **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. 101).

6.5. Atividade

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

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 problemas remotamente nos dispositivos detectados, clique em **Solucionar problemas**, e a seguir, clique em **VERIFICAR E SOLUCIONAR PROBLEMAS**.

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

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

- **Ameaças bloqueadas**. Aqui 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 usuários foram identificadas.
- **Principais dispositivos com ameaças bloqueadas**. Aqui você pode visualizar um ranking mostrando onde a maioria das ameaças para os dispositivos foram identificadas.

6.6. 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.

7. 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 definição padrão, ele verifica se há atualizações quando você liga seu dispositivo e a cada **hora** após isso. Se for detectada uma atualização, esta é automaticamente descarregada e instalada no seu dispositivo.

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 dispositivo 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. 67).
- 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. 40).

7.1. 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.

7.2. 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 dispositivo 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**.

7.3. 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 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.

7.4. 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 definição padrão, se for necessário reiniciar após uma atualização, o Bitdefender continuará a trabalhar com os arquivos antigos até que o usuário

reinicie voluntariamente o dispositivo. 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**.

7.5. 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 2020 instalado.

COMO

8. INSTALAÇÃO

8.1. Como instalar o Bitdefender em um segundo dispositivo?

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

Para instalar o Bitdefender em um segundo dispositivo:

1. Clique no link **Instalar em outro dispositivo** no canto inferior esquerdo da interface do Bitdefender.

   Uma nova janela aparecerá na sua tela.

2. Pressione **COMPARTILHAR LINK DE DOWNLOAD**.
3. Siga as instruções na tela para instalar o Bitdefender.

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

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

8.3. Onde posso baixar meu produto Bitdefender?

Você pode instalar o Bitdefender do disco de instalação, ou utilizando o instalador baixado no seu dispositivo na plataforma da Bitdefender Central.

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

Para instalar o Bitdefender da Bitdefender Central:

1. 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. Execute o Bitdefender que você baixou.

8.4. 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.

8.5. Como utilizar minha assinatura do Bitdefender após uma atualização do Windows?

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

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

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

Há duas possibilidades de caso que podem aparecer:

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

  Nesse caso, você precisa reinstalar o produto seguindo os seguintes passos:

  - No **Windows 7**:

    1. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Programas e Recursos**.
    2. Encontre o **Bitdefender Antivirus Plus** e selecione **Desinstalar**.
    3. Clique em **REINSTALAR** na janela que aparece.
    4. Aguarde o processo de desinstalação ser concluído e depois reinicie o seu sistema.

       Abra a interface do seu novo Bitdefender instalado para ter acesso aos seus recursos.

  - 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 Antivirus Plus** e selecione **Desinstalar**.
    4. Clique em **REINSTALAR** na janela que aparece.
    5. Aguarde o processo de desinstalação ser concluído e depois reinicie o seu sistema.

       Abra a interface do seu novo Bitdefender instalado para ter acesso aos seus recursos.

  - 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 Antivirus Plus** 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 desinstalação ser concluído e depois reinicie o seu sistema.

   Abra a interface do seu novo Bitdefender instalado para ter acesso aos seus recursos.

> **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.

- Você mudou seu sistema e deseja continuar usando a proteção Bitdefender. Portanto, será necessário reinstalar o produto usando a versão mais recente.

  Para resolver este problema:

  1. Baixe o arquivo de instalação:
     a. Acesse Bitdefender Central.
     b. Selecione o painel **Meus Dispositivos**, e clique em **INSTALAR PROTEÇÃO**.
     c. 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.

2. Execute o Bitdefender que você baixou.

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

8.6. 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 2020, 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**. Espere que o dispositivo seja reiniciado.

   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.

9. BITDEFENDER CENTRAL

9.1. 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 no nome da sua conta no canto superior da interface do Bitdefender.
2. Clique no botão **Alterar conta** no canto superior direito da tela para trocar a conta vinculada ao dispositivo.
3. Digite o endereço de e-mail no campo correspondente e clique em **PRÓXIMO**.
4. Digite sua senha, 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. 164).

9.2. 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**.

9.3. 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. Digite seu endereço de e-mail, depois clique em **SEGUINTE**.

     Uma nova janela aparece.
  4. Clique em **Esqueceu a senha?**.
  5. Clique em **SEGUINTE**.
  6. 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.
  7. 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. Clique em **SEGUINTE**.
  6. 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.

9.4. 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 **Sessões** no menu deslizante.
4. Na área **Sessões ativas**, selecione a opção **SAIR** próxima ao dispositivo em que você deseja encerrar sessão.

10. A ANALISAR COM BITDEFENDER

10.1. 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.
- Verificar um compartilhamento de rede antes de copiar os arquivos para o dispositivo.

10.2. 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**, clique em **Abrir**.
3. Clique no botão **Executar Verificação** ao lado de **Verificação do Sistema**.
4. Siga as instruções do assistente de Verificação de Sistema para completar a verificação. O Bitdefender executará automaticamente as ações recomendadas nos arquivos detectados.

   Se ainda houver ameaças não resolvidas, será solicitado que você escolha as ações a serem tomadas com relação às mesmas. Para mais informações, acesse "*Assistente do analisador Antivírus*" (p. 84).

10.3. 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 dispositivo.

Para programar uma verificação:

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

   Você também pode criar um tipo de verificação que atenda às suas necessidades clicando em **+Criar verificação** próximo a **Gerenciar verificações**.
4. Personalize a verificação de acordo com as suas necessidades, depois clique em **Seguinte**.
5. Marque a caixa ao lado de **Escolha quando agendar esta tarefa**.

   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.

10.4. Como posso criar uma tarefa de análise personalizada?

Se você deseja verificar locais específicos no seu dispositivo ou configurar as opções de verificação, configure e execute uma verificação personalizada.

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

1. No painel **ANTIVÍRUS**, clique em **Abrir**.
2. Clique em **+Criar verificação** ao lado de **Gerenciar verificações**.
3. No campo de Nome da tarefa, introduza o nome da verificação e selecione os locais que você deseja verificar, e depois clique em **SEGUINTE**.
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 dispositivo
     - Fechar a janela de análise

5. Se deseja configurar as opções de verificação detalhadamente, clique em **Mostrar opções avançadas**.

   Clique em **Próximo**.

6. Você pode habilitar a opção **Programar tarefa de verificação** e, se quiser, escolher 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.

10.5. 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 **ANTIVÍRUS**, clique em **Abrir**.
3. Clique na barra **Definições** .
4. Clique em **Exceções de gerenciamento**.
5. Clique em **+Adicionar uma exceção**.
6. Introduza no campo correspondente o caminho da pasta que pretende adicionar à lista de exceção da verificação.

   Como alternativa, você pode navegar até a pasta clicando no botão navegar no lado direito da interface, selecioná-la e clicar em **OK**.
7. Ligue o interruptor junto à função de proteção que não deve verificar a pasta. Há três opções:
   - AV
   - Detecção Ameaças Online
   - Defesa contra Ameaças
8. Clique **Salvar** para salvar as alterações e fechar a janela.

10.6. 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 **ANTIVÍRUS**, clique em **Abrir**.
   c. Na janela **Avançada**, 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. 69).
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 **Abrir**.
   c. Vá para a janela **Configurações** e clique em **Gerenciar a quarentena**.
   d. 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. 57).

   Por definição padrão, a Bitdefender adiciona automaticamente arquivos restaurados à lista de exceções.
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. 164).

10.7. 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**.

11. PROTEÇÃO DE PRIVACIDADE

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

Para ter a certeza de que as suas operações online se mantém privadas, 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 **Configurações**.
3. Na janela do **Safepay**, clique em **Abrir Safepay**.
4. Clique no ícone para acessar o **Teclado Virtual**.

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

11.2. 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 dispositivo 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 **Deletar 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.

11.3. 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 **Restaurar localização** e escolha um local no 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;

12. INFORMAÇÕES ÚTEIS

12.1. 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. 164).

12.2. Como eu posso remover o Bitdefender?

Se deseja remover seu Bitdefender Antivirus Plus:

- No **Windows 7**:
  1. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Programas e Recursos**.
  2. Encontre o **Bitdefender Antivirus Plus** e selecione **Desinstalar**.
  3. Clique em **REMOVER** na janela que aparece.

4. Aguarde 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 Antivirus Plus** 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 Antivirus Plus** 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.

12.3. Como removo o Bitdefender VPN?

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

- 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.

12.4. 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 ••• e depois selecione **Remover**.

12.5. Como desligo automaticamente o dispositivo após a verificação?

O Bitdefender oferece múltiplas tarefas de análise que você pode usar para se certificar de que o seu sistema não está infectado com ameaças. Verificar todo o dispositivo 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.

Considere este exemplo: você terminou o seu trabalho e quer ir dormir. Gostaria de ter o seu sistema completamente analisado em busca de ameaças pelo Bitdefender.

Para desligar o dispositivo 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**, clique em **Abrir**.
3. Na janela de **Verificações**, clique em ••• próximo a Verificação Rápida, e então selecione **Editar**.
4. Personalize a verificação de acordo com as suas necessidades e clique em **Seguinte**.
5. Marque a caixa ao lado de **Escolher quando agendar esta tarefa**, e depois 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.

6. Clique em **Guardar**.

Para desligar o dispositivo ao finalizar uma verificação customizada:

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

Se não forem encontradas ameaças, o dispositivo 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. 84).

12.6. Como posso configurar Bitdefender para usar um proxy de conexão à internet?

Se o seu dispositivo 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.

12.7. 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.

12.8. 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**.

12.9. Como posso remover outras soluções de segurança?

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

Quando utiliza mais do que uma solução de segurança no mesmo dispositivo, o sistema torna-se instável. O instalador do Bitdefender Antivirus Plus 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.

12.10. 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 dispositivo.
  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.

GERENCIAR A SUA SEGURANÇA

13. PROTEÇÃO ANTIVÍRUS

O Bitdefender protege o seu dispositivo 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 dispositivo seja infectado por ameaças, mantenha ativada a **verificação 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 verifica automaticamente qualquer mídia removível que esteja conectada ao dispositivo para garantir um acesso seguro. Para mais informações, acesse "*Análise automática de mídia removível*" (p. 88).

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. 90).

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. 93).

Se o seu dispositivo estiver infectado com ameaças, consulte "*Remover ameaças do seu sistema*" (p. 156). Para ajudá-lo a remover as ameaças do dispositivo que não podem ser removidas no sistema operacional Windows, o Bitdefender lhe fornece o"*Ambiente de Resgate*" (p. 156). Este é um ambiente

confiável especialmente concebido para a remoção de ameaças, o que lhe permite inicializar o dispositivo independentemente do Windows. Quando o dispositivo é executado no Ambiente de Resgate, as ameaças do Windows estão inativas, sendo mais fácil removê-las.

13.1. Análise no acesso (proteção em tempo real)

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

13.1.1. Ligar ou desligar a proteção em tempo real

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

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Avançado**, 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.

13.1.2. 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 **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Avançado**, você pode configurar as definições da verificação conforme 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).
- **Verificar scripts.** A funcionalidade de Verificação de scripts permite ao Bitdefender verificar scripts da powershell e documentos de escritório que possam conter malware à base de scripts.
- **Analisar compartilhamentos de rede.** Para acessar uma rede remota com segurança no seu dispositivo, 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 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.
- **Verificação de inicialização antecipada.** 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 **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Avançado**, role a página para baixo até ver a opção **Ações de ameaças**.
4. Configure as definições de análise como necessário.

As seguintes ações podem ser 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. 93).

  > **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. 93).

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

13.1.3. 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 **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Avançado**, role a página para baixo até ver a opção **Restabelecer configurações avançadas**. Selecione essa opção para retornar às configurações de fábrica do antivírus.

13.2. Análise on-demand

O objetivo principal do Bitdefender é manter seu dispositivo livre de ameaças. Isso é feito ao manter novas ameaças fora de seu dispositivo 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 dispositivo contra ameaças residentes após instalar o Bitdefender. E, sem dúvida, é uma boa idéia verificar seu dispositivo 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 verificar o dispositivo sempre que desejar, executando as tarefas de verificação padrão, ou as suas próprias tarefas de verificação (tarefas definidas pelo usuário). Se você deseja verificar locais específicos no seu dispositivo ou configurar as opções de verificação, configure e execute uma verificação personalizada.

13.2.1. 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.

13.2.2. 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 **Abrir**.
3. Na janela **Verificações**, clique no botão **Executar verificação** ao lado de **Verificação Rápida**.
4. Siga o assistente de Análise Antivírus para completar a análise. O Bitdefender 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.

13.2.3. Executando uma Análise do Sistema

A tarefa de Verificação do Sistema procura em todo o dispositivo 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 dispositivo.

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. Verificar o seu dispositivo 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. 39).
- Encerre todos os programas abertos.

Se você deseja verificar locais específicos no seu dispositivo ou configurar as opções de verificação, configure e execute uma verificação personalizada. Para mais informações, acesse "*Configurando uma análise personalizada*" (p. 81).

Para realizar uma verificação do sistema:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Verificações**, clique no botão **Executar Verificação** ao lado de **Verificação do Sistema**.
4. A primeira vez que você executar uma Verificação do Sistema, você verá uma apresentação da função. Clique em **OK, entendi** para continuar.
5. 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.

13.2.4. Configurando uma análise personalizada

Sempre que você achar que seu dispositivo 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.

Para configurar uma nova verificação customizada detalhadamente:

1. Clique em **Proteção** no menu de navegação da interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Nas janelas **Verificações**, clique em **+Criar 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 **Seguinte**.
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 dispositivo
     - 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 **Próximo**.
7. Você pode habilitar a opção **Programar tarefa de verificação** e, se quiser, escolher 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 verificar os cookies armazenados pelos navegadores no seu dispositivo.
- **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.

13.2.5. 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. 93).

  > **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. 156).

13.2.6. 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** .

13.3. Análise automática de mídia removível

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

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.

13.3.1. 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. 156).

13.3.2. 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 **ANTIVÍRUS**, clique em **Abrir**.
3. Selecione a janela **Configurações**.

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.

13.4. 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**.

13.5. 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**.

13.5.1. 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 **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Configurações**, clique em **Gerenciar exceções**.
4. Clique em **+Adicionar uma exceção**.
5. Introduza no campo correspondente o caminho da pasta que pretende adicionar à lista de exceção da verificação.

   Como alternativa, você pode navegar até a pasta clicando no botão navegar no lado direito da interface, selecioná-la e clicar em **OK**.
6. Ligue o interruptor junto à função de proteção que não deve verificar a pasta. Há três opções:
   - AV
   - Detecção Ameaças Online
   - Defesa contra Ameaças
7. Clique **Salvar** para salvar as alterações e fechar a janela.

13.5.2. Excluir extensões de arquivos da análise

Quando exclui uma extensão de arquivo da verificação, o Bitdefender deixará de verificar arquivos com essa extensão, independentemente da sua localização no seu dispositivo. 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 verificação, porque tais exceçãos podem tornar o seu dispositivo 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 **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Configurações**, clique em **Gerenciar exceções**.
4. Clique em **+Adicionar uma exceção**.
5. Digite as extensões que você deseja excluir da verificação com um ponto antes e separando-as por ponto e vírgula (;).

   txt;avi;jpg

6. Ligue o interruptor junto à função de proteção que não deve verificar a extensão.
7. Clique em **Guardar**.

13.5.3. 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 **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Configurações**, clique em **Gerenciar exceções**. Uma lista com todas as suas exceções será exibida.
4. Para remover ou editar excepções da verificação, clique em um dos botões disponíveis. Proceder da seguinte forma:

- Para remover um dado da lista, clique no botão  próximo a ele.
- Para remover um dado da lista, clique no botão **Editar** próximo a ele. Uma nova janela aparece onde você pode alterar a extensão ou o caminho a ser excluído e o recurso de segurança do qual você deseja que eles sejam excluídos, conforme necessário. Faça as alterações necessárias, depois clique em **Modificar**.

13.6. 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 **Abrir**.
3. Selecione a janela **Configurações**.

   Aqui você pode ver o nome dos arquivos em quarentena, sua localização original e o nome das ameaças detectadas.
4. 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.

5. Para eliminar um arquivo da quarentena, selecione-o e clique no botão **Eliminar**. Se pretende restaurar um arquivo da quarentena para a respectiva localização original, selecione-o e clique em **Restaurar**.

14. DEFESA 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 dispositivo, 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.

14.1. 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**, clique clique em **Abrir**.
3. Vá para a janela **Configurações** e clique no botão ao lado de **Defesa contra Ameaças Avançadas da Bitdefender**.

> **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.

14.2. 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 dispositivo 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 clique em **Abrir**.
3. Vá para a janela **Defesa contra Ameaças**.

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.

14.3. 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 clique em **Abrir**.
3. Na janela **Configurações**, clique em **Gerenciar exceções**.
4. Clique em **+Adicionar uma exceção**.
5. Introduza no campo correspondente o caminho da pasta que pretende adicionar à lista de exceção da verificação.

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

14.4. 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 dispositivo 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 clique em **Abrir**.

- Vá para a janela **Configurações** e clique no interruptor ao lado de **Explorar detecção** para ligar ou desligar o recurso.

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

15. DETECÇÃO 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 ativa a opção Verificação da web encriptada.

- Proteção antifraude.
- Proteção contra phishing.

Role para baixo e você chegará à seção **Prevenção de ameaças em rede**. Aqui você tem a opção **Prevenção de ameaças em rede**. Para manter seu dispositivo 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 **Configurações**.
3. Clique em **Gerenciar exceções**.
4. Clique em **+Adicionar uma exceção**.
5. No campo correspondente, digite o nome do site, do domínio ou do endereço IP que você deseja adicionar às excepções.
6. Clique no botão ao lado de **Prevenção de Ameaças Online**.
7. Para remover um dado da lista, clique no botão próximo a ele.

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

15.1. Alertas de Bitdefender no navegador

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

A página contém informações como a URL do site 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.

16. VULNERABILIDADE

Um passo importante na proteção do seu dispositivo 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 dispositivo, 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 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.

16.1. 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 **Abrir**.
3. Na aba **Verificação de vulnerabilidades** clique em **Iniciar verificação**, e então, aguarde até que o Bitdefender verifique seu sistema em busca de vulnerabilidades. As vulnerabilidades detectadas são agrupadas nas três categorias:
   - **SISTEMA OPERATIVO**
     - **Segurança de sistemas operativos**

       Configurações de sistema alteradas que podem comprometer seu dispositivo e dados, como não exibir avisos quando arquivos executados executam alterações em seu sistema sem sua permissão ou quando dispositivos MTP como telefones ou câmeras se conectam e executam operações diferentes sem seu conhecimento.

- **Atualizações Críticas do Windows**

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

- **Contas do Windows fracas**

  Você pode ver a lista das contas de usuário do Windows configuradas no seu dispositivo e o nível de proteção que sua senha fornece. 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 @).

- **APLICAÇÕES**

  - **Segurança do Navegador**

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

  - **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 **Baixar nova versão** para fazer download da última versão.

- **NETWORK**

  - **Rede e credenciais**

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

  - **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.

16.2. 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 **Abrir**.

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

3. Vá para a aba **Configurações**.
4. 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 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.

16.3. Consultor 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

16.3.1. 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 **Abrir**.
3. Vá para a janela **Configurações** e ative ou desative a opção **Consultor de Segurança do Wi-Fi**.

16.3.2. 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 **Abrir**.
3. Vá para a janela **Consultor de Segurança do Wi-Fi** e clique em **Wi-Fi doméstico**.
4. 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.
5. Escolha sua rede doméstica e depois clique em **SELECIONAR**.

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

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

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

16.3.3. 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 **Abrir**.
3. Vá para a janela **Consultor de Segurança do Wi-Fi**, clique em **Wi-Fi do trabalho**.
4. 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.
5. 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**.

16.3.4. 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 Antivirus Plus está configurado para realizar automaticamente os seguintes ajustes:

- A Defesa Avançada Contra Ameaças está ligada
- 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.

16.3.5. 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 **Abrir**.
3. Vá para a janela **Consultor de Segurança do Wi-Fi**.
4. Dependendo das informações que você precisar, selecione uma das três abas, **Wi-Fi doméstico**, **Wi-Fi de escritório** ou **Wi-Fi pública**.
5. Clique em **Ver detalhes**, próximo à rede para a qual você deseja ver mais informações.

Há três tipos de redes sem fio filtradas pela importância, cada tipo indicado por um ícone específico:

Wi-Fi inseguro - indica que o nível de segurança da rede é baixo. Ou seja, é muito arriscado usá-la e não é recomendado fazer pagamentos ou conferir contas bancárias sem uma proteção extra. Em tais situações, recomendamos usar o Bitdefender Safepay™ com a proteção para pontos de acesso de redes não seguras ativada.

Wi-Fi inseguro - indica que o nível de segurança da rede é moderado. Ou seja, ela pode ter vulnerabilidades e não é recomendado fazer pagamentos ou conferir contas bancárias sem uma proteção extra. Em tais situações, recomendamos usar o Bitdefender Safepay™ com a proteção para pontos de acesso de redes não seguras ativada.

Wi-Fi seguro - indica que a rede que você está usando é segura. Neste caso, você pode usar dados sensíveis para fazer operações online.

Ao clicar no link **Ver detalhes** na área de cada rede, os seguintes detalhes são exibidos:

- **Segura** - aqui você pode ver se a rede selecionada é segura ou não. Redes 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.

17. 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.

17.1. 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.

17.2. 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 **Gerenciar**.
3. Na janela Configurações, ative ou desative a **Recuperação automática**.

17.3. 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.

17.4. 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 **Restaurar localização** e escolha um local no 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;

17.5. 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 **Gerenciar**.
3. Na janela **Exceções**, clique em **+Adicionar uma exceção**.

18. PROTEÇÃO DO GERENCIADOR DE SENHAS PARA SUAS CREDENCIAIS

Utilizamos os nossos dispositivos para efetuar compras online ou pagar as contas, para nos ligarmos a plataformas de comunicação social ou para iniciar sessão em 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

18.1. 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 **Configurações**.
3. Na janela **Minhas Carteiras**, clique em **Adicionar carteira**.
4. Clique em **Criar nova**.
5. Digite as informações necessárias nos campos correspondentes.
   - Nome da Carteira - digite um nome único para seu banco de dados da Carteira.
   - Senha Mestre - digite uma senha para sua Carteira.
   - Dica - digite uma dica para lembrar de sua senha.
6. Clique em **Continuar**.
7. Nesta etapa você pode escolher armazenar suas informações na nuvem, ativando o botão ao lado de **Sincronizar em todos os meus dispositivos**. Escolha a opção desejada e então clique em **Continuar**.
8. Selecione o navegador da Internet de onde você deseja importar credenciais.
9. Clique em **Finalizar**.

18.2. 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 **Configurações**.
3. Na janela **Minhas Carteiras**, clique em **Adicionar carteira**.
4. Clique em **Importar um banco de dados existente**.
5. Vá até o local no seu dispositivo onde você deseja salvar o banco de dados da Carteira e selecione-o.

6. Clique em **Abrir**.
7. Dê um nome à sua carteira e digite a senha designada quando ela foi criada.
8. Clique em **Importar**.
9. Selecione os programas de onde deseja que a Carteira importe credenciais, depois o botão **Finalizar**.

18.3. 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 **Configurações**.
3. Vá para a janela **Minhas Carteiras**.
4. Clique no ícone ••• na Carteira desejada, e então selecione **Exportar**.
5. Acesse o local no seu dispositivo onde você deseja salvar o banco de dados da carteira e escolha um nome para ele.
6. Clique em **Guardar**.

> **Nota**
> A Carteira precisa ser aberta para que o botão **Exportar** esteja disponível. Se a Carteira que você precisa exportar estiver bloqueada, clique em **Ativar Carteira** e depois digite a senha designada quando ela foi criada.

18.4. 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 **Configurações**.
3. Vá para a janela **Minhas Carteiras**.
4. Clique no ícone ••• na Carteira desejada, e então selecione **Configurações**.
5. Escolha a opção desejada na janela que aparecer, e então clique em **Salvar**.

Nota
A Carteira precisa ser aberta para que o botão **Exportar** esteja disponível. Se a Carteira que você precisa sincronizar estiver bloqueada, clique em **ATIVAR CARTEIRA** e depois digite a senha designada quando ela foi criada

18.5. 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 **Configurações**.
3. Vá para a janela **Minhas Carteiras**.
4. Selecione o banco de dados da carteira desejado e depois clique em **Ativar Carteira**.
5. Digite a senha mestre e depois clique em **OK**.

Uma nova janela aparece. Selecione a categoria desejada na parte superior da janela:

- Identidade
- páginas web
- Online banking
- E-mails
- Aplicativos
- Redes Wi-Fi

Adicionar/ editar as credenciais

- Para adicionar uma nova senha, escolha a categoria desejada acima, clique em **+ Adicionar item**, insira as informações nos campos correspondentes e clique no botão Salvar.
- Para editar um dado na tabela, selecione-o e clique no botão **Editar** no lado direito.
- Para remover uma entrada da tabela, selecione-a e clique no botão **Eliminar**.

18.6. 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.

18.7. 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 janela **Configurações**.

Na seção **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 dispositivo, 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 janela **Configurações**.

   Ligue o interruptor ao lado de um aplicativo para usar o Administrador de Senhas e melhore a 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. Na janela **Configurações**, vá até 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.

19. 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.

19.1. Interface do Antitracker

Ao ativar a extensão do Antitracker da Bitdefender, o ícone  aparece ao lado da barra de pesquisa no seu navegador. Cada vez que 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.

19.2. 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.

19.3. 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 .

20. 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.

20.1. 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**.

20.2. 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. 125).

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

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

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

  - **Geral**
    - Notificações
    - Inicialização - escolha se executar ou não o Bitdefender VPN ao iniciar
    - Relatórios do produto - envie relatórios de produtos anônimos para nos ajudar a melhorar a sua experiência
    - Modo escuro
    - Idioma
  - **Avançado**
    - Internet Kill-Switch - esta funcionalidade suspende temporariamente todo o tráfego da internet se a conexão VPN cair acidentalmente. Assim que você estiver de volta online, a conexão VPN é restabelecida.
    - Autoconnect - Conecte o Bitdefender VPN automaticamente quando você acessar uma rede Wi-Fi pública/insegura ou quando um aplicativo de compartilhamento de arquivos peer-to-peer for iniciado

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

20.3. Assinaturas

O Bitdefender VPN oferece gratuitamente 200 MB de franquia por dispositivo para proteger sua conexão sempre que você precisar, além de conectá-lo automaticamente ao melhor local de servidor.

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

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

A assinatura do Bitdefender Premium VPN é independente da assinatura do Bitdefender Antivirus Plus, ou seja, você poderá usá-lo por todo o seu período de disponibilidade, sem importar o estado da assinatura da solução antivírus. Caso a assinatura do Bitdefender Premium VPN expire e a do Bitdefender Antivirus Plus 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.

21. 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. 113).

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 dispositivo 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™.

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

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

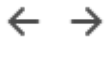
- Na interface do Bitdefender:
  1. Clique em **Privacidade** no menu de navegação da interface do Bitdefender.
  2. No painel do **SAFEPAY**, clique em **Configurações**.
  3. Na janela do **Safepay**, clique em **Abrir Safepay**.
- Do Windows:
  - No **Windows 7**:
    1. Clique **Iniciar** e acesse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

21.2. Configurando definições

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

Aplicar as regras do Bitdefender Safepay para os domínios acessados
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**e siga o assistente para usar os certificados no Bitdefender Safepay™.

Usar teclado virtual

O teclado virtual aparecerá automaticamente quando o campo de senha for selecionado.

Use o botão correspondente para ativar ou desativar a função.

Confirmação de impressão

Ative esta opção se deseja dar sua confirmação antes que o processo de impressão se inicie.

21.3. 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 em • • • e escolha **Barra de endereços** para abrir a barra de endereços.

> **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.

21.4. 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. Na janela **Configurações**, desative o botão ao lado de **Notificações do Safepay**.

21.5. 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. Na janela **Configurações**, ligue o interruptor próximo a **Usar VPN com Safepay**.

22. USB IMMUNIZER

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

Para imunizar um dispositivo USB:

1. Conecte o flash drive ao seu dispositivo.
2. Explore o seu dispositivo 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 dispositivo execute ameaças de dispositivos USB não imunizados, desative a função de media autorun. Para mais informações, acesse "*Usando o monitoramento automático de vulnerabilidade*" (p. 103).

UTILITÁRIOS

23. 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 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 Antivirus Plus é configurado para ajustar automaticamente as seguintes configurações:

- A Defesa Avançada Contra Ameaças está ligada
- As seguintes configurações da Prevenção Contra Ameaças Online são ativadas:
  - Verificação da web criptografada
  - Proteção contra fraudes
  - Proteção contra phishing

23.1. 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 **Utilidades** no menu de navegação da interface do Bitdefender.
2. Na aba **Perfis**, clique em **Configurações**.
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 **Utilidades** no menu de navegação da interface do Bitdefender.
2. Na aba **Perfis**, clique em **Configurações**.
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.

23.2. Perfil de Filme

A exibição de conteúdo de vídeo de alta qualidade, como filmes de alta definição, exige recursos significativos do sistema. O Perfil de Filme ajusta as 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 **Utilidades** no menu de navegação da interface do Bitdefender.
2. Na aba **Perfis**, clique em **Configurações**.
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 **Utilidades** no menu de navegação da interface do Bitdefender.
2. Na aba **Perfis**, clique em **Configurações**.
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.

23.3. 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 **Utilidades** no menu de navegação da interface do Bitdefender.

2. Na aba **Perfis**, clique em **Configurações**.
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 **Utilidades** no menu de navegação da interface do Bitdefender.
2. Na aba **Perfis**, clique em **Configurações**.
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.

23.4. 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 **Utilidades** no menu de navegação da interface do Bitdefender.
2. Na aba **Perfis**, clique em **Configurações**.
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**.

23.5. 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 **Utilidades** no menu de navegação da interface do Bitdefender.
2. Na aba **Perfis**, clique em **Configurações**.
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 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.

23.6. 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 **Utilidades** no menu de navegação da interface do Bitdefender.
2. Na aba **Perfis**, clique em **Configurações**.
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.

24. PROTEÇÃO DE DADOS

24.1. 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 dispositivo 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 **Utilidades** 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 **Deletar 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.

RESOLUÇÃO DE PROBLEMAS

25. 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. 143)
- "*A análise não inicia*" (p. 144)
- "*Não posso mais usar uma app*" (p. 147)
- "*O que fazer quando o Bitdefender bloqueia um site, domínio, endereço IP ou aplicativo online seguro*" (p. 148)
- "*Como atualizar o Bitdefender numa ligação à Internet lenta*" (p. 149)
- "*Os Serviços do Bitdefender não estão respondendo*" (p. 149)
- "*A funcionalidade Preenchimento Automático não funciona na minha Carteira*" (p. 150)
- "*A Remoção do Bitdefender falhou*" (p. 151)
- "*O meu sistema não reinicia após a instalação de Bitdefender*" (p. 152)

Se não conseguir encontrar o seu problema aqui, ou se as soluções apresentadas não resolvem o seu problema, pode contactar os representantes do apoio técnico da Bitdefender como mostrado no capítulo "*Solicite Ajuda*" (p. 164).

25.1. O meu sistema parece estar lento

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

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. 70).

- **Não se cumprem os requisitos do sistema para executar o Bitdefender.**

  Se o seu dispositivo não cumprir os Requisitos do Sistema, ficará lento, especialmente se estiver executando multiplos aplicativos ao mesmo tempo. Para mais informações, acesse "*Requisitos de Sistema*" (p. 3).

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

  Qualquer dispositivo tem programas ou aplicativos que você não usa. 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 dispositivo. 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**, clique em **Abrir**.
  3. Na janela **Verificações**, clique em **Executar Verificação** ao lado de **Verificação do Sistema**.
  4. Siga os passos do assistente.

25.2. A análise não inicia

Este tipo de problema pode ter duas causas principais:

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

Neste caso, reinstale o Bitdefender:

- No **Windows 7**:
  1. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Programas e Recursos**.
  2. Encontre o **Bitdefender Antivirus Plus** e selecione **Desinstalar**.
  3. Clique em **REINSTALAR** na janela que aparece.
  4. Aguarde 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 Antivirus Plus** 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 Antivirus Plus** 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. 70).
  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 Antivirus Plus** 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 Antivirus Plus** 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 Antivirus Plus** 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. 164).

25.3. 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 clique em **Abrir**.
3. Na janela **Configurações**, clique em **Gerenciar exceções**.
4. Clique em **+Adicionar uma exceção**.
5. Digite o caminho do executável que você deseja adicionar à lista de exceção da verificação no campo correspondente.

Como alternativa, você pode navegar para o executável clicando no botão de procurar no lado direito da interface, logo selecioná-lo e clicar em **OK**.

6. Ligue o interruptor ao lado de **Defesa contra Ameaças Avançadas**.
7. Clique em **Guardar**.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção "*Solicite Ajuda*" (p. 164).

25.4. 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 **Configurações**.
3. Clique em **Gerenciar exceções**.
4. Clique em **+Adicionar uma exceção**.
5. No campo correspondente, digite o nome do site, do domínio ou do endereço IP que você deseja adicionar às excepções.
6. Clique no botão ao lado de **Prevenção de Ameaças Online**.
7. Clique **Salvar** para salvar as alterações 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. 164).

25.5. Como atualizar o Bitdefender numa ligação à Internet lenta

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

Para manter 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.

25.6. 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 dispositivo 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 dispositivo e aguarde alguns momentos até que o Bitdefender seja carregado. Abra o Bitdefender para verificar se o erro persiste. Reiniciar o dispositivo 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. 70).

Se o erro persistir, entre em contato com nossos representantes de suporte conforme descrito na seção "*Solicite Ajuda*" (p. 164).

25.7. 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 no botão **Abrir menu** no canto superior direito da tela.
  3. Clique em Add-ons.
  4. Clique em Extensões.
  5. Vá à **Carteira do Bitdefender** e clique no botão próximo a ela.

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

> **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. 164).

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

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

Se instalou o Bitdefender e não consegue reiniciar o seu sistema no modo normal, 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. 71).

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 Antivirus Plus** 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 Antivirus Plus** 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 Antivirus Plus** 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. 71).
  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. 71).
2. Usar a opção de Restauro do Sistema do Windows para restaurar o dispositivo para uma data anterior antes de instalar o produto Bitdefender.
3. Reinicie o sistema no modo normal e contate os nossos representantes do suporte conforme descrito na seção "*Solicite Ajuda*" (p. 164).

26. 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.

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

Se não conseguir encontrar o seu problema aqui, ou se as soluções apresentadas não resolvem o seu problema, pode contactar os representantes do apoio técnico da Bitdefender como mostrado no capítulo "*Solicite Ajuda*" (p. 164).

26.1. Ambiente de Resgate

O **Ambiente de Resgate** é um recurso do Bitdefender que permite verificar e desinfetar todas as partições do disco rígido dentro e fora do seu sistema operacional.

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

Iniciar o seu sistema no Ambiente de Resgate

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 **Abrir**.
3. Clique em **Abrir** ao lado de **Ambiente de Resgate**.
4. Clique em **REINICIAR** na janela que aparece.

   O Ambiente de Resgate do Bitdefender carrega em alguns instantes.

Verificar o seu sistema no Ambiente de Resgate

Para verificar seu sistema no Ambiente de Resgate:

1. Entre no Ambiente de Resgate, como descrito em "Iniciar o seu sistema no Ambiente de Resgate" (p. 157).
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 **Fechar** na janela com os resultados da verificação.

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

Você pode descobrir que há uma ameaça no seu dispositivo de uma dessas formas:

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

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 **ANTIVÍRUS**, clique em **Abrir**.
   c. Na janela **Avançada**, 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. 69).
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. 71).
2. Mostrar objetos ocultos no Windows. Para saber mais sobre como fazer isso, por favor, acesse "*Como posso mostrar objetos ocultos no Windows?*" (p. 69).
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. 164).

26.3. 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 **ANTIVÍRUS**, clique em **Abrir**.
   c. Na janela **Avançada**, desative o **Escudo do Bitdefender**.
3. Vá à localização do arquivo e descomprima-o com uma aplicação de arquivo, como o WinZip.
4. Identifique e elimine o 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. 164).

26.4. 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 **ANTIVÍRUS**, clique em **Abrir**.
   c. Na janela **Avançada**, desative o **Escudo do Bitdefender**.
3. Abra o relatório da análise e utilize a informação de identificação (Assunto, De, Para) das mensagens infectadas para localizá-las no cliente de correio 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. 164).

26.5. 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. 54).
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. 164).

26.6. 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 iria verificá-los automaticamente para manter o seu dispositivo 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.

26.7. 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.

26.8. 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.

26.9. 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.

CONTATE-NOS

27. 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. 143) fornece as informações necessárias em relação às incidências mais frequentes que poderá encontrar ao utilizar este produto.

Se não encontrar a resposta para sua pergunta nos recursos disponibilizados, pode contactar-nos diretamente:

- "Contate conosco diretamente no Bitdefender Antivirus Plus" (p. 164)
- "Contate-nos através do nosso Centro de Suporte Online" (p. 165)

Contate conosco diretamente no Bitdefender Antivirus Plus

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 no botão **Suporte**, representado por um **ponto de interrogação**, na parte superior da interface 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.

28. 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.

28.1. Centro de Suporte Bitdefender

O Centro de Suporte do Bitdefender é um repositóio de informação online sobre os produtos Bitdefender. Armazena, num formato facilmente acessível, 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.

28.2. Fórum de Suporte Bitdefender

O Fórum de Suporte do Bitdefender proporciona aos utilizadores do Bitdefender uma forma fácil de obter ajuda e ajudar os outros.

Se o seu produto Bitdefender não estiver a funcionar correctamente, se não conseguir remover certas ameaças do seu dispositivo ou se tiver alguma questão sobre a forma como opera, coloque o seu problema ou a sua questão no fórum.

Os técnicos de 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.

28.3. Portal HOTforSecurity

HOTforSecurity é uma fonte rica de informações sobre segurança de computadores. Aqui você pode conhecer as várias ameaças as quais seu dispositivo 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.

29. 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.

29.1. 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

29.2. Distribuidores locais

Os distribuidores locais Bitdefender estão preparados para responder a quaisquer dúvidas relacionadas com as suas áreas de operação, quer sejam comerciais ou assuntos gerais.

Para encontrar um distribuidor Bitdefender no seu país:

1. Vá para https://www.bitdefender.com/partners/partner-locator.html.
2. Escolha 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.

29.3. 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 Building, 15A Orhideelor Street, 11th fllor, district 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.