Bitdefender®
PREMIUM SECURITY

MANUAL DO UTILIZADOR

Mac iOS

Bitdefender Premium Security
Manual do Utilizador

Editado 07/19/2020

Aviso Legal

Bitdefender

Índice

Sobre este guia

1. Propósito e público-alvo

A sua subscrição Bitdefender Premium Security pode proteger até 10 PCs, Macs, iOS smartphones e tablets Android diferentes. A gestão dos seus dispositivos protegidos pode ser realizada através de uma conta Bitdefender, que deve estar vinculada a uma subscrição ativa.

Com a nossa subscrição do Bitdefender Premium Security, pode utilizar a versão premium do Bitdefender VPN em todos os dispositivos onde tiver instalado o Bitdefender. Isso significa que obtém tráfego ilimitado e acesso sem restrições a conteúdos a nível mundial escolhendo a localização de servidor da sua preferência.

Este guia auxilia na configuração e utilização dos produtos incluídos no sua subscrição : Bitdefender Total Security (para Windows), Bitdefender Antivirus for Mac (para macOS), Bitdefender Mobile Security (para Android) e Bitdefender Mobile Security for iOS.

Pode descobrir como configurar o Bitdefender em diferentes dispositivos para mantê-los protegidos contra todo o tipo de ameaças.

2. Como utilizar este guia

Este guia está organizado para os quatro produtos incluídos no Bitdefender Premium Security:

- “Total Security para PC” (p. 1)

  Aprenda a utilizar o produto nos seus PCs e portáteis com Windows.

- “Antivirus para Mac” (p. 194)

  Aprenda a utilizar o produto nos seus Macs.

- “Mobile Security para iOS” (p. 241)

  Aprenda a utilizar o produto nos seus smartphones e tablets iOS.

- “Mobile Security para Android” (p. 259)

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

- “Contacte-nos” (p. 301)

  Veja onde procurar por ajuda caso algo inesperado apareça.

TOTAL SECURITY PARA PC

1. INSTALAÇÃO

1.1. A preparar a instalação

Antes de instalar o Bitdefender Total Security, complete estes procedimentos para assegurar uma boa instalação:

- Assegure-se que o dispositivo onde deseja instalar o Bitdefender tem os requisitos de sistema mínimos. Caso o dispositivo não cumpra os requisitos de sistema, o Bitdefender não será instalado ou caso seja instalado, não irá trabalhar de forma apropriada e irá causar lentidão e instabilidade do sistema. Para ver a lista completa dos requisitos mínimos do sistema, consulte o "*Requisitos do sistema*" (p. 2).
- Ligue-se ao dispositivo utilizando uma conta de Administrador.
- Remova quaisquer outros softwares semelhantes do seu dispositivo. Se for detetada qualquer coisa durante o processo de instalação da Bitdefender, será notificado para desinstalar. Executar dois programas de segurança simultaneamente poderá afetar o seu funcionamento e causar grandes problemas no sistema. O Windows Defender será desativado durante a instalação.
- Desativar ou remover qualquer programa de firewall que possa estar em execução no dispositivo. Executar dois programas de firewall simultaneamente poderá afetar o seu funcionamento e causar grandes problemas no sistema. A Firewall do Windows será desativada durante a instalação.
- Recomenda-se que o seu dispositivo esteja ligado à Internet durante a instalação, mesmo quando realizar a instalação a partir de um CD/DVD. Se estiverem disponíveis versões mais recentes dos ficheiros da aplicação incluidos no pacote de instalação, o Bitdefender irá descarregá-las e instalá-las.

1.2. Requisitos do sistema

Só pode instalar o Bitdefender Total Security nos dispositivos que tenham os seguintes sistemas operativos:

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

- Windows 10
- 2,5 GB de espaço disponível em disco rígido (pelo menos 800 MB na unidade do sistema)
- 2 GB de memória (RAM)

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

Nota
Para saber qual é o sistema operativo Windows executado no seu dispositivo e informações do hardware:

- No **Windows 7**, clique com o botão direito em **Computador** no ambiente de trabalho, depois selecione **Propriedades** no menu.
- No **Windows 8**, no ecrã inicial, localize **Computador** (por exemplo, pode começar a escrever "Computador" diretamente no ecrã inicial) e depois clique com o botão direito no seu ícone. No **Windows 8.1**, localize **Este PC**.

  Selecione **Propriedades** no menu inferior. Verifique a área do **Sistema** para encontrar mais informações sobre o sistema.
- No **Windows 10**, digite **Sistema** na caixa de pesquisa da barra de tarefas e clique no seu ícone. Verifique a área do **Sistema** para encontrar mais informações sobre o sistema.

Requisitos de Software

Para conseguir utilizar o Bitdefender e todas as suas funcionalidades, o seu dispositivo deve cumprir os seguintes requisitos de software:

- Microsoft Edge 40 e superior
- Internet Explorer 10 ou superior
- Mozilla Firefox 51 e superior
- Google Chrome 34 e superior
- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 e superior

1.3. Instalação do seu produto Bitdefender

Pode instalar o Bitdefender utilizando o disco de instalação ou através do instalador Web transferido para o seu dispositivo na Bitdefender Central.

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

1.3.1. Instalar da Bitdefender Central

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

Para transferir o Bitdefender Total Security da Bitdefender Central:

1. Aceda Bitdefender Central.
2. Selecione o painel **Os meus dispositivos**, e clique em **INSTALAR PROTEÇÃO**.
3. Escolha uma das duas opções disponíveis:
   - **Proteger este dispositivo**
     a. Selecione esta opção e, em seguida, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique no botão correspondente.
     b. Guarde o ficheiro de instalação.
   - **Proteger outros dispositivos**
     a. Selecione esta opção e, em seguida, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique no botão correspondente.
     b. Clique em **ENVIAR HIPERLIGAÇÃO DE DOWNLOAD**.
     c. Escreva um endereço de email no campo correspondente e clique em **ENVIAR EMAIL**.

        Observe que a hiperligação de download gerada será válida apenas durante as próximas 24 horas. Se a hiperligação expirar, precisará de gerar uma nova seguindo os mesmos passos.

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

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

A validar a instalação

O Bitdefender primeiro verifica o sistema para validar a instalação.

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

Se for detetada uma solução de segurança incompatível ou uma versão anterior do Bitdefender, será solicitado a removê-lo do seu sistema. Por favor siga as instruções para remover o software do seu sistema, evitando assim que ocorram problemas mais tarde. Pode ser necessário reiniciar o dispositivo para concluir a remoção das soluções de segurança detetadas.

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

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

Quando a instalação for validada, o assistente de instalação aparece. Siga os passos para instalar o Bitdefender Total Security.

Passo 1 – instalação do Bitdefender

Antes de concluir o processo de instalação, deve concordar com o Contrato de Subscrição. Leia o Contrato de Subscrição com calma pois contém os termos e condições que regem a utilização do Bitdefender Total Security.

Se não concorda com estes termos, feche a janela. O processo de instalação terminará e sairá do mesmo.

Podem ser realizadas duas tarefas adicionais neste passo:

- Mantenha a opção **Enviar relatórios de produto** ativada. Ao permitir esta opção, os relatórios que contêm informação sobre como usa o produto são enviados para os servidores Bitdefender. Esta informação é essencial para melhorar o produto e pode ajudar-nos a oferecer-lhe uma experiência

melhor no futuro. Tenha em atenção que estes relatórios não contêm dados confidenciais, tais como o seu nome, endereço de IP ou outros, e que não serão usados para fins comerciais.

- Selecione o idioma em que pretende instalar o produto.

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

Passo 2 - Instalação em curso

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

Passo 3 - Instalação concluída

O seu produto Bitdefender foi instalado com sucesso.

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

Passo 4 - Análise do dispositivo

Agora ser-lhe-á perguntado se deseja realizar uma análise do seu dispositivo, para garantir que ele está seguro. Durante este passo, o Bitdefender irá verificar áreas críticas do sistema. Clique em **Iniciar análise de dispositivo** para a iniciar.

Pode ocultar a interface da análise ao clicar em **Executar análise em segundo plano**. Em seguida, escolha se deseja ser informado quando a análise terminar ou não.

Quando a análise estiver concluída, clique em **Abrir Interface do Bitdefender**.

Nota

Como alternativa, se não deseja realizar a análise, basta clicar em **Ignorar**.

Passo 5 - Introdução

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

Clique em **FINALIZAR** para aceder à interface do Bitdefender Total Security.

2. INTRODUÇÃO

2.1. Os básicos

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

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

Ligar-se a redes sem fios públicas de aeroportos, shoppings, cafés ou hotéis sem proteção pode ser perigoso para o seu dispositivo e para os seus dados. A razão principal é porque defraudadores podem estar a assistir às suas atividades e encontrar o melhor momento para roubar os seus dados pessoais, e também porque todos podem ver o seu endereço IP, tornando a sua máquina uma vítima para futuros ciberataques. Para evitar tais situações inoportunas, instale e use a aplicação "*VPN*" (p. 133).

Pode controlar as suas palavras-passe e contas online armazenando-as "*Proteção do Gestor de palavras-passe para as suas credenciais*" (p. 124) numa carteira. Com uma única palavra-passe principal pode proteger a sua privacidade contra intrusos que podem tentar deixá-lo sem dinheiro.

"*Proteção da Webcam*" (p. 118)impede que as aplicações não fidedignas acedam à sua câmara de vídeo, evitando qualquer tentativa de hacking. Com base na escolha dos utilizadores de Bitdefender, o acesso de aplicações populares à sua câmara Web será permitido ou bloqueado.

Para o proteger contra possíveis bisbilhoteiros e espiões quando o dispositivo está ligado a uma rede sem fios não protegida, Bitdefender analisa o nível de segurança e, quando necessário, fornece recomendações para aumentar a segurança das suas atividades online. Para instruções sobre como manter os seus dados pessoais seguros, aceda o "*Consultor de Segurança Wi-Fi*" (p. 114).

Agora ficheiros encriptados por ransomware podem ser recuperados sem que precise de gastar dinheiro para qualquer resgate exigido. Para

informações sobre como recuperar ficheiros encriptados, veja "*Remediação de Ransomware*" (p. 122).

Enquanto trabalha, joga ou vê filmes, Bitdefender pode oferecer-lhe uma experiência de utilizador contínua, adiando as tarefas de manutenção, eliminando as interrupções e ajustando os efeitos visuais do sistema. Pode beneficiar de tudo isto ao ativar e configurar os "*Perfis*" (p. 157).

Bitdefender tomará por si a maioria das decisões relacionadas com segurança e raramente surgirão alertas pop-up. Os detalhes sobre as ações tomadas e informações sobre a operação de programas estão disponíveis na janela de Notificações. Para mais informação, dirija-se a "*Notificações*" (p. 9).

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

Para utilizar as funcionalidades online do Bitdefender Total Security, gerir as suas subscrições e os dispositivos, aceda à sua conta Bitdefender. Para mais informação, dirija-se a "*Bitdefender Central*" (p. 24).

A "*Como*" (p. 37) secção é onde vai encontrar instruções passo-a-passo sobre como levar a cabo as tarefas mais comuns. Se experimentar incidências durante o uso do Bitdefender, consulte a "*Resolver incidências comuns*" (p. 166) secção de possíveis soluções para os problemas mais comuns.

A abrir a janela do Bitdefender

Para aceder à interface principal do Bitdefender Total Security, clique no ícone no seu ambiente de trabalho.

Se necessário, também pode seguir os passos abaixo:

- No **Windows 7**:
  1. Clique em **Iniciar** e vá para **Todos os Programas**.
  2. Clique em **Bitdefender**.
  3. Clique em **Bitdefender Total Security** ou, mais rápido, clique duas vezes no ícone do Bitdefender no tabuleiro do sistema.
- No **Windows 8 e Windows 8.1**:

Localize o Bitdefender no ecrã inicial do Windows (por exemplo, pode começar a digitar "Bitdefender" diretamente no ecrã inicial) e depois clique no seu ícone. De forma alternativa, abra a aplicação do ambiente de trabalho, clique duas vezes no ícone Bitdefender no tabuleiro do sistema.

- No **Windows 10**:

  Digite "Bitdefender" na caixa de pesquisa da barra de tarefas, depois clique no seu ícone. Alternativamente, clique duas vezes no ícone do Bitdefender no tabuleiro do sistema.

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

2.1.1. Notificações

O Bitdefender mantém um registo detalhado dos eventos relacionados com a sua atividade no seu dispositivo. Sempre que ocorrer algo relevante para a segurança do seu sistema ou dados, será adicionada uma nova mensagem às Notificações do Bitdefender, de forma semelhante a um novo e-mail surgir na sua caixa de entrada.

As notificações são uma ferramenta importante na monitorização e gestão da proteção do seu Bitdefender. Por exemplo, pode verificar com facilidade se a atualização foi realizada com sucesso, se foram encontradas ameaças ou vulnerabilidades no seu dispositivo, etc. Adicionalmente, pode realizar outras ações, se necessário, ou alterar ações tomadas pelo Bitdefender.

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

.

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

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

Clique em cada separador para ver mais detalhes sobre os eventos gerados. São apresentados breves detalhes com um único clique em cada título de evento, como uma descrição curta, a ação tomada pelo Bitdefender quando

o evento ocorreu e a data e hora do evento. Pode ser fornecidas opções para tomar mais ações, caso seja necessário.

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

2.1.2. Perfis

Algumas atividades do computador, tais como os jogos online ou apresentações de vídeo, requerem uma maior capacidade de resposta, elevado desempenho e nenhuma interrupção do sistema. Quando o seu computador portátil está ligado apenas com a bateria, é melhor que operações desnecessárias, que consomem mais energia, sejam adiadas até que o portátil esteja ligado á corrente.

Os Perfis do Bitdefender atribuem mais recursos do sistema às aplicações em execução, modificando temporariamente as definições de proteção e ajustando a configuração do sistema. Consequentemente, o impacto do sistema na sua atividade é minimizado.

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

Perfil Trabalho
: Otimiza a sua eficiência de trabalho ao identificar e ajustar as definições do produto e do sistema.

Perfil de Filme
: Melhora os efeitos visuais e elimina as interrupções ao ver filmes.

Perfil de Jogo
: Melhora os efeitos visuais e elimina as interrupções ao jogar.

Perfil Wi-Fi Público
: Aplica definições do produto para beneficiar da proteção completa enquanto está ligado a uma rede sem fios insegura.

Perfil do Modo de Bateria
: Aplica definições de produto e coloca em pausa as atividades em segundo plano para economizar bateria.

Configure a ativação automática de perfis

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

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

Pode clicar em **AGORA NÃO** se quiser ativar a funcionalidade mais tarde.

Para permitir que o Bitdefender ative perfis automaticamente:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Perfis**, clique em **Definições**.
3. Utilize o botão correspondente para ligar **Ativar perfis automaticamente**.

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

Para ativar manualmente um perfil, ligue o botão correspondente. Dos primeiros três perfis, apenas um pode ser manualmente ativado imediatamente.

Para mais informações sobre Perfis, aceda a"*Perfis*" (p. 157)

2.1.3. Definições de proteção da palavra-passe de Bitdefender

Se não for a única pessoa a utilizar este dispositivo, recomendamos que proteja as suas definições do Bitdefender com uma palavra-passe.

Para configurar a proteção por palavra-passe para as definições do Bitdefender:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. Na janela **Geral**, ative a **Proteção por palavra-passe**.
3. Digite a palavra-passe nos dois campos e, em seguida, clique em **OK**. A palavra-passe tem de ter pelo menos 8 caracteres.

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

Importante

Não se esqueça da sua palavra-passe e registe-a num local seguro. Se esquecer a palavra-passe, terá de reinstalar o programa ou contactar o apoio do Bitdefender.

Para remover a proteção por palavra-passe:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. Na janela **Geral**, desative a **Proteção por palavra-passe**.
3. Digite a palavra-passe e, em seguida, clique em **OK**.

Nota

Para alterar a palavra-passe do seu produto, clique em **Alterar palavra-passe**. Digite a palavra-passe atual e, de seguida, clique **OK**. Na nova janela que aparece, digite a palavra-passe que pretende utilizar a partir deste momento para restringir o acesso às definições do seu Bitdefender.

2.1.4. Relatórios do produto

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

Tenha em atenção que estes relatórios não contêm dados confidenciais, tais como o seu nome, endereço de IP ou outros, e que não serão usados para fins comerciais.

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

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. Selecione o separador **Avançado**.
3. Desligue **Relatórios do produto**.

2.1.5. Notificações de ofertas especiais

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

Para ativar ou desativar notificações de ofertas especiais:

1. Clique em **Definições** 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 do produto estão ativadas por defeito.

2.2. Interface Bitdefender

O Bitdefender Total Security vai de encontro às necessidades quer dos principiantes quer dos utilizadores mais técnicos. Assim, o interface gráfico do utilizador foi desenhado para servir quer uns quer outros.

Vá à interface do Bitdefender, encontra-se exibido no canto superior esquerdo um assistente de introdução que contém detalhes sobre como interagir com o produto e como o configurar. Selecione o ícone do ângulo direito para continuar a ser guiado ou **Ignorar** para fechar o assistente.

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

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

No menu de navegação do lado esquerdo, pode aceder à área de definições, notificações e as sessões do Bitdefender para definições detalhadas e tarefas administrativas avançadas.

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

2.2.1. Ícone na área de notificação

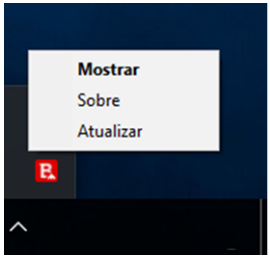
Para gerir todo o produto mais rapidamente, pode usar o ícone da Bitdefender que se encontra na barra de tarefas.

Nota
O ícone do Bitdefender poderá não estar visível a toda a hora. Para fazer o ícone aparecer permanentemente:

- No **Windows 7, Windows 8 e Windows 8.1**:
  1. Clique na seta no canto inferior direito do écran.
  2. Clique **Personalizar...** para abrir a janela de ícones da Área de Notificação.
  3. Selecione a opção **Mostrar ícones e notificações** para o ícone do **Agente do Bitdefender**.
- No **Windows 10**:
  1. Clique com o botão direito do rato na barra de tarefas e seleccione **Definições da barra de tarefas**.
  2. Desça e clique na hiperligação **Selecione os ícones que aparecem na barra de tarefas** sob **Área de notificações**.
  3. Ative o botão ao lado do **Agente do Bitdefender**.

Se fizer duplo-clique neste ícone, o Bitdefender irá abrir. Também clicando com o botão direito do rato sobre ele aparecerá um menu contextual que lhe permitirá uma administração rápida do Bitdefender.

- **Mostrar** - abre a janela principal do Bitdefender.
- **Informação** - abre uma janela na qual poderá consultar informação sobre o Bitdefender, onde procurar ajuda se acontecer algo inesperado, onde aceder e visualizar o Acordo de Subscrição, os Componentes de Terceiros e a Política de Privacidade.
- **Atualizar agora** - executa uma atualização imediata. Pode seguir o estado das atualizações no painel de Atualizações da janela principal do Bitdefender.



Tray Icon

O ícone do Bitdefender na área de notificação do sistema, informa quando há incidências a afetar o seu dispositivo ou a forma como o produto funciona, ao exibir um símbolo especial, como o que se segue:

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

Se o Bitdefender não estiver a funcionar, o ícone da áea de notificação do sistema fica com uma cor de fundo cinzenta . Isto normalmente acontece quando a a assinatura expira. Também pode ocorrer quando os serviços da

Bitdefender não estão a responder ou quando outros erros afectam a actuação normal da Bitdefender.

2.2.2. Menu de navegação

No lado esquerdo da interface do Bitdefender está o menu de navegação, que lhe permite aceder rapidamente aos recursos e ferramentas do Bitdefender que precisa para utilizar o seu produto. Os separadores disponíveis nesta área são:

- **Painel**. Daqui, pode reparar rapidamente problemas de segurança, ver recomendações de acordo com as necessidades do seu sistema, realizar ações rápidas e instalar Bitdefender noutros dispositivos.
- **Proteção**. Daqui, pode executar e configurar análises antivírus, aceder às definições do Firewall, recuperar dados encriptados por ransomware e configurar a proteção enquanto navega na internet.
- **Privacidade**. Daqui, é possível criar gestores de palavras-passe para as suas contas online, proteger o acesso à sua webcam contra espiões, fazer pagamentos online num ambiente online, abrir a aplicação VPN e proteger os seus filhos ao visualizar e restringir a sua atividade online.
- **Utilidades**. Daqui é possível melhorar a velocidade do sistema e configurar a função Antirroubo para os seus dispositivos.
- **Notificações**. A partir daqui pode aceder às notificações geradas.
- **Definições**. A partir daqui pode aceder às definições gerais.

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

- **Suporte**. Aqui é possível entrar em contato com o departamento de Suporte Técnico da Bitdefender sempre que for necessária assistência para resolver um problema com seu Bitdefender Total Security.
- **A minha conta**. Daqui, pode aceder à sua conta Bitdefender para verificar as suas subscrições e realizar tarefas de segurança nos dispositivos que controla. Detalhes sobre a conta Bitdefender e subscrição em utilização também estão disponíveis.

2.2.3. Painel

A janela do painel permite-lhe realizar tarefas comuns, corrigir rapidamente problemas de segurança, visualizar informações sobre o funcionamento do produto e aceder a painéis de onde configurar as definições do produto.

Tudo se encontra a apenas uns cliques de distância.

A janela é organizada em três áreas principais:

Área de estado de segurança
: É aqui que pode conferir o estado de segurança do seu dispositivo.

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

Ações rápidas
: Aqui pode executar diferentes tarefas para manter o seu sistema protegido e a funcionar na velocidade ideal. Também pode instalar Bitdefender noutros dispositivos, uma vez que a sua subscrição tem entradas disponíveis suficientes.

Área de estado de segurança

O Bitdefender utiliza um sistema de emissão de monitorização para detetar e informá-lo sobre os problemas que podem afetar a segurança do seu dispositivo e dos seus dados. As incidências detetadas incluem definições de proteção importantes que estão desligadas e outras condições que podem representar um risco de segurança.

Sempre que problemas afetarem a segurança do seu dispositivo, o estado que aparece na parte superior da Interface do Bitdefender muda para vermelho. O estado exibido indica a natureza do problema a afetar o seu sistema. Além disso, o ícone na bandeja do sistema muda para e se mover o cursor sobre o ícone, 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 esteja atento e os repare o mais depressa possível. Para reparar um problema, clique no botão próximo ao problema detetado.

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 realizar, seja trabalhar, fazer pagamentos online, ver filmes ou jogar, o Bitdefender Autopilot fornecerá recomendações contextuais com base na utilização e necessidades do seu dispositivo. As recomendações propostas também podem estar relacionadas às ações que precisa de executar para manter o seu produto a funcionar na capacidade máxima.

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

Desligar as notificações do Autopilot

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

Para desligar as notificações do Autopilot:

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

Ações rápidas

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

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

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

As tarefas que pode adicionar à interface principal são:

- **Análise Rápida**. Realizar uma verificação rápida para detetar imediatamente as possíveis ameaças que podem estar presentes no seu dispositivo.
- **Análise do Sistema**. Execute uma análise do sistema para garantir que o dispositivo está livre de ameaças.

- **Ver Vulnerabilidades**. Verifique o seu dispositivo para identificar vulnerabilidades e assegurar que todos as aplicações instaladas, além do sistema operacional, estão atualizadas e a funcionar corretamente.
- **Consultor de Segurança do Wi-Fi**. Abra a janela do Consultor de Segurança do Wi-Fi no módulo de Vulnerabilidade.
- **Carteiras**. Veja e administre as suas carteiras.
- **Abrir Safepay**. Abra o Bitdefender Safepay™ para proteger os seus dados pessoais enquanto efetua transações online.
- **Abrir a VPN**. Abra o Bitdefender VPN para adicionar uma camada extra de proteção enquanto está ligado à Internet.
- **Destruidor de Ficheiros**. Abra o Destruidor de Ficheiros para remover os traços de dados sensíveis do seu dispositivo.
- **Abrir o Otimizador de Um Clique**. Liberte espaço no disco, corrija erros de registo e proteja a sua privacidade ao eliminar ficheiros que já não são úteis com um simples clicar no botão.

Para começar a proteger dispositivos adicionais com o Bitdefender:

1. Clique em **Instalar noutro dispositivo**.

   Aparece uma nova janela no seu ecrã.

2. Clique em **PARTILHAR HIPERLIGAÇÃO DE TRANSFERÊNCIA**.

3. Siga os passos no ecrã para instalar o Bitdefender.

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

- Bitdefender Total Security nos dispositivos Windows.
- Bitdefender Antivirus for Mac em dispositivos macOS.
- Bitdefender Mobile Security nos dispositivos Android.
- Bitdefender Mobile Security em dispositivos iOS.

2.2.4. As secções do Bitdefender

O Bitdefender tem três secções diferentes divididas em funcionalidades úteis para ajudá-lo a permanecer protegido enquanto trabalha, navega na Internet, realiza pagamentos online, além de melhorar a velocidade do seu sistema, etc.

Sempre que pretender aceder às funcionalidades para uma secção específica ou para começar a configurar o seu produto, clique nos seguintes ícones localizados no menu de navegação da interface do Bitdefender:

-  Proteção
-  Privacidade
-  Utilitários

Proteção

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

As funcionalidades que pode gerir na secção Proteção são:

ANTIVIRUS

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

A partir da funcionalidade Antivírus, pode aceder facilmente às seguintes tarefas de análise:

- Análise Rápida
- Análise do Sistema
- Gerir Análises
- Ambiente de Resgate

Para mais informações sobre tarefas de análise e como configurar a proteção antivírus, consulte "*Proteção Antivírus*" (p. 71).

PREVENÇÃO CONTRA AMEAÇAS ONLINE

A Prevenção contra ameaças online ajuda-lhe a manter-se protegido contra ataques de phishing, tentativas de fraude e fugas de dados pessoais enquanto navega na internet.

Para mais informações sobre como configurar o Bitdefender para proteger a sua atividade Web, consulte "*Prevenção de Ameaças Online*" (p. 93).

FIREWALL

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

Para mais informações sobre configuração de firewall, consulte "*Firewall*" (p. 104).

ADVANCED THREAT DEFENSE

O Advanced Threat Defense protege ativamente o sistema contra ameaças tal como ransomware, spyware e cavalos de Tróia ao analisar o comportamento de todas as aplicações instaladas. Os processos suspeitos são identificados e, quando necessário, bloqueados.

Para mais informações sobre como manter o sistema protegido contra ameaças, consulte "*Advanced Threat Defense*" (p. 91).

ANTISPAM

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

Para mais informações sobre a proteção antispam, consulte "*Antispam*" (p. 95).

VULNERABILIDADE

O módulo Vulnerabilidade ajuda a manter o seu sistema operativo e as aplicações que utiliza regularmente atualizados e a identificar as redes sem fio inseguras às quais se liga. Clique em **Abrir** no módulo de Vulnerabilidade para aceder às suas funcionalidades.

A funcionalidade de **Análise de Vulnerabilidades** permite identificar atualizações essenciais do Windows, atualizações de aplicações, palavras-passe fracas pertencentes a contas do Windows e redes sem fios que não são seguras. Clique em **Iniciar Análise** para realizar uma análise no seu dispositivo.

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

Para mais informações sobre como configurar a proteção de vulnerabilidade, consulte "*Vulnerabilidade*" (p. 110).

REMEDIAÇÃO DE RANSOMWARE

A ferramenta de Remediação de Ransomware ajuda a recuperar ficheiros caso eles sejam encriptados por ransomware.

Para informações sobre como recuperar ficheiros encriptados, veja "*Remediação de Ransomware*" (p. 122).

Privacidade

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

As funcionalidades que pode gerir na secção Privacidade são:

VPN

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

Para mais informações sobre esta funcionalidade, consulte "*VPN*" (p. 133).

PROTEÇÃO DE VÍDEO E ÁUDIO

A Proteção de Vídeo e Áudio mantém a sua webcam segura bloqueando o acesso a aplicações não confiáveis e notificando-o(a) quando uma aplicação tentar aceder ao seu microfone.

Para saber mais sobre como manter a sua webcam protegida contra acessos indesejados e como configurar o Bitdefender para o(a) notificar sobre a atividade do seu microfone, consulte "*Proteção de Vídeo e Áudio*" (p. 118).

PASSWORD MANAGER

O Gestor de palavras-passe do Bitdefender ajuda-o a controlar as suas palavras-passe, protege a sua privacidade e proporciona uma experiência de navegação segura.

Para mais informações sobre como configurar o Gestor de palavras-passe, consulte "*Proteção do Gestor de palavras-passe para as suas credenciais*" (p. 124).

SAFEPAY

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

Para mais informações sobre o Bitdefender Safepay™, consulte "*Segurança Safepay para transações online*" (p. 135).

CONTROLO PARENTAL

O Controlo Parental do Bitdefender permite monitorizar o que os seus filhos fazem no dispositivo. Caso haja conteúdo inapropriado, pode decidir restringir o seu acesso à Internet ou às aplicações específicas.

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

Para mais informações sobre a configuração do Controlo Parental, aceda a "*Controlo Parental* " (p. 140).

ANTITRACKER

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

Para obter mais informações sobre a funcionalidade Antitracker, consulte "*Antitracker*" (p. 131).

Utilitários

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

Otimizador de Um Clique

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

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

Para mais informações, dirija-se a "*Otimizador de Um Clique*" (p. 163).

Anti-Theft

O Antirroubo do Bitdefender protege o seu dispositivo e os seus dados contra roubo ou perda. No caso de tal evento, isto permite-lhe localizar

remotamente ou bloquear o seu dispositivo. Pode também limpar todos os dados presentes no seu sistema.

O Antirroubo do Bitdefender oferece as seguintes funcionalidades:
- Localização Remota
- Bloqueio Remoto
- Limpeza Remota
- Alerta Remoto

Para mais informações sobre como pode manter o seu sistema longe das mãos erradas, consulte "*Dispositivo Anti-Roubo*" (p. 153).

Proteção de dados

O Destruidor de Ficheiros do Bitdefender ajuda a eliminar permanentemente dados removendo-os fisicamente do seu disco rígido.

Para mais informações, dirija-se a "*Proteção de dados*" (p. 164).

Perfis

Atividades de trabalho diárias, ver filmes ou jogar podem provocar lentidão no sistema, especialmente se estes estiverem a ser executados simultaneamente com os processos de atualização do Windows e as tarefas de manutenção.

Com o Bitdefender, pode agora escolher e aplicar o seu perfil preferido; o que irá ajustar o sistema a melhorar o desempenho de aplicações específicas.

Para mais informações sobre esta funcionalidade, consulte "*Perfis*" (p. 157).

2.2.5. Mude o idioma do produto

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

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

2.3. Bitdefender Central

Bitdefender Central é a plataforma onde tem acesso às funções e serviços online do produto, e pode realizar remotamente tarefas importantes nos dispositivos em que o Bitdefender estiver instalado. Pode aceder à sua conta Bitdefender desde qualquer dispositivo ligado à internet, indo para https://central.bitdefender.com, ou diretamente pela aplicação da Bitdefender Central em dispositivos Android e iOS.

Para instalar a aplicação da Bitdefender Central nos seus dispositivos:

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

Assim que iniciar sessão, pode começar a fazer o seguinte:

- Transfira e instale o Bitdefender nos sistemas operativos Windows, macOS, iOS e Android. Os produtos disponíveis para download são:
  - Bitdefender Total Security
  - O Antivírus Bitdefender para Mac
  - Bitdefender Mobile Security para Android
  - Bitdefender Mobile Security for iOS
  - Bitdefender - Controlo Parental
- Gerir e renovar as suas subscrições do Bitdefender.
- Adicionar novos dispositivos à sua rede e gerir as suas funcionalidades onde quer que esteja.
- Proteja os dispositivos de rede e os seus dados contra roubo ou perda com o Anti-Roubo.
- Configurar as definições do Parental Control para as contas das suas crianças e monitorizar a sua atividade onde quer que eles estejam.

A aceder Bitdefender Central

Existem diversas formas de aceder à Bitdefender Central:

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

  Abra a aplicação da Bitdefender Central que instalou.

Nota
Neste material, recebe as opções e instruções disponíveis na plataforma web.

2.3.1. Autenticação de dois fatores

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

Ativar autenticação de dois fatores

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

Para ativar a autenticação de dois fatores:

1. Aceda Bitdefender Central.
2. Clique no ícone no canto superior direito do ecrã.

3. Clique em **Conta da Bitdefender** no menu deslizante.
4. Selecione o separador **Palavra-passe e segurança**.
5. Clique em **Autenticação de dois fatores**.
6. Clique em **COMEÇAR**.

   Selecione uma das seguintes opções:

   - **Aplicação de autenticação** - utilize uma apliação de autenticação para gerar um código sempre que quiser aceder à sua conta Bitdefender.

     Caso queira utilizar a aplicação de autenticação, mas não tem a certeza de qual escolher, aparecerá uma lista com as aplicações de autenticação recomendadas.

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

     b. Para uniciar sessão num dispositivo Android ou iOS, utilize o seu dispositivo para digitalizar o código QR.

        Para iniciar sessão utilizando um portátil ou um ambiente de trabalho, pode adicionar manualmente o código apresentado.

        Clique em **CONTINUAR**.

     c. Insira o código fornecido pela aplicação ou o apresentado no passo anterior e, em seguida, clique em **ATIVAR**.

   - **E-mail** - sempre que iniciar sessão na sua conta Bitdefender, o código de verificação será enviado para a sua caixa de e-mail. Verifique a sua conta de e-mail e introduza o código fornecido.

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

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

        Lembre que tem cinco minutos para verificar a sua conta de e-mail e introduzir o código gerado. Se o tempo expirar, deverá gerar uma nova hiperligação seguindo os mesmos passos.

     c. Clique em **ATIVAR**.

     d. Receberá dez códigos de ativação. Pode copiar, transferir ou imprimir a lista e usá-la caso perca o seu endereço de e-mail, caso contrário não poderá iniciar sessão. Cada código pode ser utilizado apenas uma vez.

     e. Clique em **TERMINADO**.

Caso queira deixar de utilizar a autenticação de dois fatores:

1. Clique em **DESATIVAR A AUTENTICAÇÃO EM DOIS FATORES**.
2. Verifique a sua aplicação ou conta de e-mail e introduza o código que recebeu.

   Caso tenha escolhido receber o código de autenticação por e-mail, terá cinco minutos para verificar a sua conta de e-mail e introduzir o código gerado. Se o tempo expirar, deverá gerar uma nova hiperligação seguindo os mesmos passos.
3. Confirme a sua escolha.

Adicionar dispositivos fiáveis

Para garantir que apenas pode aceder à sua conta Bitdefender, poderemos solicitar o código de segurança primeiro. Caso pretenda ignorar este passo sempre que se ligar com o mesmo dispositivo, recomendamos identificá-lo como um dispositivo fiável.

Para adicionar dispositivos como dispositivos fiáveis:

1. Aceda Bitdefender Central.
2. Clique no ícone no canto superior direito do ecrã.
3. Clique em **Conta da Bitdefender** no menu deslizante.
4. Selecione o separador **Palavra-passe e segurança**.
5. Clique em **Dispositivos fiáveis**.
6. Será mostrada a lista com os dispositivos Bitdefender instalados. Clique no dispositivo desejado.

Pode adicionar os dispositivos que pretender, desde que tenham o Bitdefender instalado e a sua subscrição seja válida.

2.3.2. As minhas subscrições

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

Verificar subscrições disponíveis

Para verificar as suas subscrições disponíveis:

1. Aceda Bitdefender Central.

2. Selecione o painel **As Minhas Subscrições**.

Aqui pode aceder às informações sobre a disponibilidade das subscrições que possui e o número de dispositivos a utilizar cada uma delas.

Pode adicionar um novo dispositivo a uma subscrição ou renová-la selecionando um cartão de subscrição.

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

Adicionar um novo dispositivo

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

1. Aceda Bitdefender Central.
2. Selecione o painel **Os meus dispositivos**, e clique em **INSTALAR PROTEÇÃO**.
3. Escolha uma das duas opções disponíveis:

   - **Proteger este dispositivo**

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

   - **Proteger outros dispositivos**

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

     Clique em **ENVIAR HIPERLIGAÇÃO DE DOWNLOAD**. Escreva um endereço de email no campo correspondente e clique em **ENVIAR EMAIL**. Observe que a hiperligação de download gerada será válida apenas durante as próximas 24 horas. Se a hiperligação expirar, precisará de gerar uma nova seguindo os mesmos passos.

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

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

Renew subscription

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

1. Aceda Bitdefender Central.
2. Selecione o painel **As Minhas Subscrições**.
3. Selecione o cartão de subscrição pretendido.
4. Clique em **RENOVAR** para continuar.

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

Ativar subscrição

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

Caso tenha adquirido um código de ativação de um dos nossos revendedores ou ganho como presente, poderá prolongar a duração de qualquer subscrição do Bitdefender existente disponível na conta, desde que sejam do mesmo produto.

Para ativar uma assinatura utilizando um código de ativação:

1. Aceda Bitdefender Central.
2. Selecione o painel **As Minhas Subscrições**.
3. Clique no botão **CÓDIGO DE ATIVAÇÃO** e, em seguida, escreva o código no campo correspondente.
4. Clique em **ATIVAR** para continuar.

A subscrição está ativada agora. Vá ao painel **Os Meus Dispositivos** e selecione **INSTALAR PROTEÇÃO** para instalar o produto num de seus dispositivos.

2.3.3. Meus dispositivos

A área **Os Meus Dispositivos** na Bitdefender Central dá-lhe a possibilidade de instalar, gerir e realizar ações remotas no seu produto Bitdefender em

qualquer dispositivo, desde que esteja ligado e com ligação à Internet. Os cartões de dispositivos exibem o nome do dispositivo, o estado da proteção e se há algum risco de segurança afetando a proteção dos seus dispositivos.

Para ver uma lista dos seus dispositivos ordenados de acordo com o seu estado ou utilizadores, clique na seta pendente no canto superior direito do ecrã.

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

1. Aceda Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.
3. Clique no cartão de dispositivo pretendido e, em seguida, o ícone ⋮ no canto superior direito do ecrã.
4. Selecione **Definições**.
5. Digite um novo nome no campo **Nome do dispositivo** e clique **GUARDAR**.

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

1. Aceda Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.
3. Clique no cartão de dispositivo pretendido e, em seguida, o ícone ⋮ no canto superior direito do ecrã.
4. Selecione **Perfil**.
5. Clique em **Add owner** e, em seguida, preencha os respetivos campos. Personalize o perfil adicionando uma fotografia e selecionando a data de nascimento.
6. Clique em **ADICIONAR** para guardar o perfil.
7. Selecione o proprietário pretendido na lista **Proprietário do dispositivo** e, em seguida, clique em **ATRIBUIR**.

Para atualizar o Bitdefender remotamente no seu dispositivo Windows:

1. Aceda Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.

3. Clique no cartão de dispositivo pretendido e, em seguida, o ícone ⋮ no canto superior direito do ecrã.
4. Selecione **Atualizar**.

Para mais ações remotas e informações sobre o seu produto Bitdefender num dispositivo específico, clique no cartão de dispositivo pretendido.

Quando clicar no cartão de dispositivo, ficam disponíveis os seguintes separadores:

- **Painel**. Nesta janela, pode visualizar os detalhes sobre o dispositivo selecionado, verificar o seu estado de proteção, o estado do Bitdefender VPN e quantas ameaças foram bloqueadas nos últimos sete dias. O estado de proteção pode estar verde, quando não houver problemas a afetar o seu dispositivo, amarelo, quando o dispositivo exigir a sua atenção, ou vermelho, quando o dispositivo estiver em risco. Quando houver problemas a afetar o seu dispositivo, clique no seta pendente na área de estado acima para saber mais detalhes. A partir daqui poderá resolver manualmente os problemas que afetam a segurança dos seus dispositivos.
- **Proteção**. Desta janela pode executar uma Verificação Rápida ou do Sistema remotamente nos seus dispositivos. Clique no botão **VERIFICAR** para iniciar o processo. Também pode conferir quando é que a última verificação foi realizada no dispositivo e aceder a um relatório da última verificação, contendo as informações mais importantes.Para mais informações sobre estes dois processos de verificação, consulte "*Executar uma Análise do Sistema*" e "*Executar uma Análise Rápida*" (p. 77).
- **Otimizador**. Aqui pode melhorar remotamente o desempenho de um dispositivo com a verificação, deteção e limpeza remota de ficheiros inúteis. Clique no botão **INICIAR** e, em seguida, selecione as áreas que deseja otimizar. Clique novamente no botão **INICIAR** para iniciar o processo de otimização. Clique em **Mais detalhes** para aceder a um relatório detalhado sobre os problemas resolvidos.
- **Antirroubo**. Em caso de deslocação, roubo ou perda, pode localizar e realizar ações remotas no seu dispositivo com a função Anti-furto. Clique em **LOCALIZAR** para descobrir a localização do seu dispositivo. A última localização conhecida será exibida, juntamente com a hora e com a data. Para mais detalhes sobre esta função, aceda a "*Dispositivo Anti-Roubo*" (p. 153).

- **Vulnerabilidade**. Para verificar um dispositivo e identificar vulnerabilidades, como a falta de atualizações do Windows, aplicações desatualizadas ou palavras-passe fracas, clique no botão **VERIFICAR** no separador Vulnerabilidade. Vulnerabilidades não podem ser corrigidas remotamente. Caso qualquer vulnerabilidade seja detetada, é necessário executar uma nova verificação no dispositivo e, em seguida, tomar as providências recomendadas. Clique em **Mais detalhes** para aceder a um relatório detalhado sobre os problemas encontrados. Para mais detalhes sobre esta função, aceda a "*Vulnerabilidade*" (p. 110).

2.3.4. Actividade

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

Ao aceder a janela **Atividade**, os seguintes cartões são disponibilizados:

- **Meus dispositivos**. Aqui pode visualizar o número de dispositivos ligados e o seu estado de proteção. Para resolver problemas remotamente nos dispositivos detectados, clique em **Resolver problemas** e, em seguida, clique em **ANALISAR E RESOLVER PROBLEMAS**.

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

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

- **Ameaças bloqueadas**. Aqui pode visualizar um gráfico que mostra uma estatística geral que inclui informação sobre as ameaças bloqueadas nas últimas 24 horas e nos últimos sete dias. A informação exibida vai depender do comportamento malicioso detectado e os ficheiros, aplicações e URLs acedidos.

- **Utilizadores principais com ameaças bloqueadas**. Aqui pode visualizar uma lista que mostra onde o maior número ameaças para os utilizadores foram identificadas.

- **Dispositivos principais com ameaças bloqueadas**. Aqui pode visualizar uma lista mostrando onde foram encontrados os dispositivos com o maior número de ameaças.

2.3.5. Notificações

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

2.4. Mantenha o seu Bitdefender atualizado.

Todos os dias são encontradas e identificadas novas ameaças. Por isso é muito importante manter o Bitdefender atualizado com a base de dados de informações de ameaças mais recente.

Se está ligado à Internet através de banda larga ou ADSL, o Bitdefender executa esta operação sozinho. Por predefinição, ele verifica se há atualizações quando liga o seu dispositivo e todas as **horas** após isso. Se for detetada uma atualização, esta é automaticamente descarregada e instalada no seu dispositivo.

O processo de actualização é executado "on the fly", o que significa que os ficheiros são substituídos progressivamente. Desta forma, o processo de atualização não afetará a operação do produto, e ao mesmo tempo, qualquer vulnerabilidade será eliminada.

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

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

- Se o seu dispositivo se ligar a Internet através de um servidor proxy, deve configurar as definições do proxy conforme escrito em *"Como posso configurar Bitdefender para usar um proxy de ligação à Internet?"* (p. 65).
- Se está ligado à Internet através de uma ligação dial-up, então é uma boa ideia adquirir o hábito de atualizar o Bitdefender a seu pedido. Para mais informação, dirija-se a *"A efetuar uma atualização"* (p. 34).

2.4.1. Verifique se o Bitdefender está atualizado

Para verificar quando foi a última atualização do seu Bitdefender:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Todas**, selecione a notificação referente à última atualização.

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

2.4.2. A efetuar uma atualização

Para realizar actualizações, é necessária uma ligação à Internet.

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

A funcionalidade Atualização irá ligar-se ao servidor de atualização de Bitdefender e verificará se existem atualizações. Se uma atualização é detetada, poderá ser notificado para confirmar a atualização ou a mesma é realizada automaticamente, dependendo das definições de atualização.

Importante
Poderá ser necessário reiniciar o dispositivo quando a atualização tiver terminado. Recomendamos que o faça assim que seja possível.

Também pode realizar atualizações remotamente nos seus dispositivos, desde que estejam ativados e ligados à Internet.

Para atualizar o Bitdefender remotamente no seu dispositivo Windows:

1. Aceda Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.
3. Clique no cartão de dispositivo pretendido e, em seguida, o ícone no canto superior direito do ecrã.
4. Selecione **Atualizar**.

2.4.3. Ligar ou desligar a atualização automática

Para desativar a atualização automática:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. Selecione o separador **Atualizar**.

3. Ative ou desative o botão correspondente.
4. Aparece uma janela de aviso. Tem de confirmar a sua escolha selecionando no menu durante quanto tempo pretende desativar a atualização automática. Pode desativar as atualizações automáticas por 5, 15 ou 30 minutos, por uma hora ou até à próxima reinicialização do sistema.

Atenção
Esta é uma incidência de segurança critica. Recomendamos que desative a atualização automática o menos tempo possível. Se o Bitdefender não for atualizado regularmente, não será capaz de o proteger contra as ameaças mais recentes.

2.4.4. Ajuste das configurações da atualização

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

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

Para ajustar as definições de atualização:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. Selecione o separador **Atualizar** e ajuste as definições de acordo com suas preferências.

Frequência de atualização

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

Regras de atualização

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

Algumas atualizações exigem o reinício para concluir a instalação.

Por defeito, se for necessário reiniciar após uma actualização, o Bitdefender continuará a trabalhar com os ficheiros antigos até que o utilizador reinicie voluntariamente o dispositivo. Isto serve para evitar que o processo de actualização de Bitdefender interfira com o trabalho do utilizador.

Se quiser ser notificado quando uma atualização precisar de reiniciar, ative a **Notificação de reinicialização**.

2.4.5. Atualizações contínuas

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

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

Nota
As atualizações que incluem novas funcionalidades e melhorias serão entregues apenas aos utilizadores com o Bitdefender 2020 instalado.

3. COMO

3.1. Instalação

3.1.1. Como instalar o Bitdefender num segundo dispositivo?

Caso a subscrição que comprou cubra mais do que um dispositivo, pode utilizar a sua conta Bitdefender para ativar um segundo PC.

Para instalar o Bitdefender num segundo dispositivo:

1. Clique na hiperligação **Instalar noutro dispositivo** no canto inferior esquerdo da interface do Bitdefender.

   Aparece uma nova janela no seu ecrã.

2. Clique em **PARTILHAR HIPERLIGAÇÃO DE TRANSFERÊNCIA**.
3. Siga as instruções no ecrã para instalar o Bitdefender.

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

3.1.2. Como posso reinstalar Bitdefender?

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

- você reinstalou o sistema operativo.
- pretende corrigir problemas que causaram abrandamentos e falhas.
- o seu produto Bitdefender não começa ou funciona corretamente.

Caso uma das situações mencionadas seja o seu caso, siga estes passos:

- No **Windows 7**:
  1. Clique em **Iniciar** e vá para **Todos os Programas**.
  2. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
  3. Clique em **REINSTALAR** na janela que aparece.
  4. Precisa de reiniciar o dispositivo para concluir o processo.
- No **Windows 8 e Windows 8.1**:

1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
2. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
4. Clique em **REINSTALAR** na janela que aparece.
5. Precisa de reiniciar o dispositivo para concluir o processo.

- No **Windows 10**:

1. Clique em **Iniciar**, em seguida, clique em Definições.
2. Clique no ícone **Sistema** na área das Definições, em seguida, selecione **Aplicações e funcionalidades**.
3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
4. Clique em **Desinstalar** novamente para confirmar a sua escolha.
5. Clique em **REINSTALAR**.
6. Precisa de reiniciar o dispositivo para concluir o processo.

Nota
Ao seguir este procedimento de reinstalação, as definições personalizadas são guardadas e estão disponíveis no novo produto instalado. As outras definições podem ser alteradas novamente para a configuração predefinida.

3.1.3. Onde posso transferir o meu produto Bitdefender?

Pode instalar o Bitdefender do disco de instalação ou através do instalador transferido no seu dispositivo da plataforma Bitdefender Central.

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

Para instalar o Bitdefender da Bitdefender Central:

1. Aceda Bitdefender Central.
2. Selecione o painel **Os meus dispositivos**, e clique em **INSTALAR PROTEÇÃO**.

3. Escolha uma das duas opções disponíveis:

   - **Proteger este dispositivo**

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

   - **Proteger outros dispositivos**

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

     Clique em **ENVIAR HIPERLIGAÇÃO DE DOWNLOAD**. Escreva um endereço de email no campo correspondente e clique em **ENVIAR EMAIL**. Observe que a hiperligação de download gerada será válida apenas durante as próximas 24 horas. Se a hiperligação expirar, precisará de gerar uma nova seguindo os mesmos passos.

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

4. Execute o Bitdefender que transferiu.

3.1.4. Como é que posso alterar o idioma do meu produto Bitdefender?

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

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

3.1.5. Como utilizo a minha subscrição do Bitdefender após uma atualização do Windows?

Esta situação ocorre quando atualiza o sistema operativo e pretende continuar a utilizar a subscrição do Bitdefender.

Se estiver a utilizar uma versão anterior do Bitdefender, 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.

Existem dois casos que podem aparecer:

- Atualizou o sistema operativo utilizando o Windows Update e constata que o Bitdefender já não funciona.

  Neste caso, é necessário reinstalar o produto ao seguir estes passos:

  - No **Windows 7**:

    1. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
    2. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
    3. Clique em **REINSTALAR** na janela que aparece.
    4. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

       Abra a interface do produto Bitdefender recentemente instalado para ter acesso às respetivas funcionalidades.

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

    1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
    2. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
    3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
    4. Clique em **REINSTALAR** na janela que aparece.
    5. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

       Abra a interface do produto Bitdefender recentemente instalado para ter acesso às respetivas funcionalidades.

- No **Windows 10**:

  1. Clique em **Iniciar**, em seguida, clique em Definições.
  2. Clique no ícone **Sistema** na área de Configurações e, em seguida, selecione **Aplicações**.
  3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
  4. Clique em **Desinstalar** novamente para confirmar a sua escolha.
  5. Clique em **REINSTALAR** na janela que aparece.
  6. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

     Abra a interface do produto Bitdefender recentemente instalado para ter acesso às respetivas funcionalidades.

> **Nota**
> Ao seguir este procedimento de reinstalação, as definições personalizadas são guardadas e estão disponíveis no novo produto instalado. As outras definições podem ser alteradas novamente para a configuração predefinida.

- Alterou o seu sistema e pretende continuar a utilizar a proteção Bitdefender. Portanto, será necessário reinstalar o produto utilizando a versão mais recente.

  Para resolver este problema:

  1. Transfira o ficheiro de instalação:
     a. Aceda Bitdefender Central.
     b. Selecione o painel **Os meus dispositivos**, e clique em **INSTALAR PROTEÇÃO**.
     c. Escolha uma das duas opções disponíveis:
        - **Proteger este dispositivo**

          Selecione esta opção e, em seguida, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique no botão correspondente.
        - **Proteger outros dispositivos**

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

Clique em **ENVIAR HIPERLIGAÇÃO DE DOWNLOAD**. Escreva um endereço de email no campo correspondente e clique em **ENVIAR EMAIL**. Observe que a hiperligação de download gerada será válida apenas durante as próximas 24 horas. Se a hiperligação expirar, precisará de gerar uma nova seguindo os mesmos passos.

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

2. Execute o Bitdefender que transferiu.

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

3.1.6. Como posso atualizar para a mais recente versão de Bitdefender?

A partir de agora, a atualização para a versão mais recente é possível sem seguir o procedimento manual de desinstalação e reinstalação. Mais exatamente, o novo produto que inclui novas funcionalidades e melhorias de produto importantes é fornecido por atualização do produto e, se já tiver uma subscrição de Bitdefender ativa, o produto é ativado automaticamente.

Se estiver a utilizar a versão de 2020, é possível atualizar para a versão mais recente ao seguir estes passos:

1. Clique em **REINICIAR AGORA** na notificação recebida com as informações sobre a atualização. Se a perder, aceda à janela Notificações, aponte para a atualização mais recente e clique no botão **REINICIAR AGORA**. Espere que o dispositivo seja reiniciado.

   É apresentada a janela **Novidades** com informações sobre as novas e melhoradas funcionalidades.

2. Clique nas hiperligações **Ler mais** para ser redirecionado para a nossa página dedicada com mais detalhes e artigos úteis.

3. Feche a janela **Novidades** para aceder à interface da nova versão instalada.

Os utilizadores que pretendem atualizar gratuitamente do Bitdefender 2016 ou uma versão inferior para a versão mais recente do Bitdefender têm de

remover a versão atual do Painel de Controlo e transferir o ficheiro de instalação mais recente do site Web do Bitdefender no seguinte endereço: https://www.bitdefender.com/Downloads/. A ativação só é possível com uma subscrição válida.

3.2. Bitdefender Central

3.2.1. Como faço para iniciar sessão na conta da Bitdefender com outra conta?

Criou uma nova conta Bitdefender e pretende utilizá-la de agora em diante.

Para iniciar sessão com outra conta da Bitdefender:

1. Clique no nome da sua conta no canto superior da Interface do Bitdefender.
2. Clique em **Alterar Conta** no canto superior direito do ecrã para trocar a conta vinculada ao dispositivo.
3. Introduza o endereço de e-mail no campo correspondente e clique em **PRÓXIMO**.
4. Introduza a sua palavra-passe e depois clique em **ENTRAR**.

> **Nota**
> O produto Bitdefender do seu dispositivo muda automaticamente de acordo com a subscrição associada à nova conta Bitdefender.
> Se não houver uma subscrição associada à nova conta Bitdefender ou caso pretenda transferi-la da conta anterior, pode contatar o Bitdefender para obter suporte, como descrito na secção "*Pedir Ajuda*" (p. 302).

3.2.2. Como é que desativo as mensagens de ajuda da Bitdefender Central?

As mensagens de ajuda são exibidas no painel para ajudá-lo a entender como cada opção na Bitdefender Central é útil.

Se pretender deixar de ver este tipo de mensagens:

1. Aceda Bitdefender Central.
2. Clique no ícone no canto superior direito do ecrã.
3. Clique em **A Minha Conta** no menu deslizante.

4. Clique em **Definições** no menu deslizante.
5. Desative a opção **Ativar/desativar mensagens de ajuda**.

3.2.3. Esqueci-me da palavra-passe que defini para a minha conta Bitdefender. Como é que a reponho?

Existem duas possibilidades para definir uma nova palavra-passe para a sua conta do Bitdefender:

- A partir da 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 do ecrã.

     Aparece uma nova janela.
  3. Introduza o seu endereço de e-mail e clique em **PRÓXIMO**.

     Aparece uma nova janela.
  4. Clique em **Esqueceu a palavra-passe?**.
  5. Clique em **SEGUINTE**.
  6. Verifique a sua conta de e-mail, introduza o código de segurança que recebeu e depois clique em **PRÓXIMO**.

     Ou pode clicar em **Alterar palavra-passe** no e-mail que recebeu.
  7. Introduza a nova palavra-passe que pretende definir e, em seguida, introduza-a novamente. Clique em **GUARDAR**.
- Do seu navegador Web:
  1. Vá para: https://central.bitdefender.com.
  2. Clique em **INICIAR SESSÃO**.
  3. Introduza o seu endereço de e-mail e depois clique em **PRÓXIMO**.
  4. Clique em **Esqueceu a palavra-passe?**.
  5. Clique em **SEGUINTE**.
  6. Verifique a sua conta de e-mail e siga as instruções fornecidas para definir a nova palavra-passe da sua conta Bitdefender.

A partir de agora, para aceder à sua conta Bitdefender, escreva o seu endereço de e-mail e a nova palavra-passe que acabou de definir.

3.2.4. Como posso gerir os inícios de sessão associados à minha conta do Bitdefender?

Na sua conta do Bitdefender tem a possibilidade de ver os últimos inícios de sessão inativos e ativos a funcionar em dispositivos associados à sua conta. Além disso, pode terminar sessão remotamente seguindo os seguintes passos:

1. Aceda Bitdefender Central.
2. Clique no ícone no canto superior direito do ecrã.
3. Clique em **Sessões** no menu deslizante.
4. Na área **Sessões ativas**, selecione a opção **TERMINAR SESSÃO** junto ao dispositivo que pretende terminar a sessão.

3.3. A analisar com Bitdefender

3.3.1. Como posso analisar um ficheiro ou uma pasta?

A forma mais fácil para analisar um ficheiro ou pasta é clicar com o botão direito do rato no objeto a 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 tomará automaticamente as ações recomendadas nos ficheiros detetados.

Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas.

Situações típicas em que deve de usar este método de análise são as seguintes:

- Suspeita que um determinado ficheiro ou pasta está infectado.
- Sempre que descarrega ficheiros da Internet que julga serem perigosos.
- Verifique uma partilha de rede antes de copiar os ficheiros para o seu dispositivo.

3.3.2. Como posso analisar o seu sistema?

Para realizar uma análise completa no sistema:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Clique no botão **Executar Análise** ao lado de **Análise do Sistema**.
4. Siga as instruções do assistente de Verificação do Sistema para concluir a verificação. O Bitdefender tomará automaticamente as ações recomendadas nos ficheiros detetados.

   Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas. Para mais informação, dirija-se a "*Assistente de Análise Antivírus*" (p. 81).

3.3.3. Como programar uma verificação?

Pode configurar o seu produto Bitdefender para iniciar a verificação de locais importantes do sistema quando não estiver a utilizar o dispositivo.

Para agendar uma análise:

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

   Como alternativa, pode criar um tipo de verificação que corresponda às suas necessidades clicando em **+Criar análise** ao lado de **Gerir análises**.
4. Personalize a análise de acordo com as suas necessidades e, em seguida, clique em **Seguinte**.
5. Marque a caixa ao lado de **Escolha quando agendar esta tarefa**.

   Selecione uma das opções correspondentes para definir uma agenda:

   - No iniciar do sistema
   - Diária
   - Semanal

- Mensal

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

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

3.3.4. Como posso criar uma tarefa de análise personalizada?

Se quer analisar localizações específicas no seu dispositivo ou configurar as opções de análise, pode configurar e executar uma tarefa personalizada.

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

1. No painel **ANTIVÍRUS**, clique em **Abrir**.
2. Clique em **+Criar análise** ao lado de **Gerir análises**.
3. No campo de nome da tarefa, introduza o nome da verificação e selecione os locais que deseja analisar e, em seguida, clique em **SEGUINTE**.
4. Configure as seguintes opções gerais:
   - **Analisar apenas aplicações**. Você pode configurar o Bitdefender para só analisar as aplicações acedidas.
   - **Verificar prioridade de tarefa**. Pode escolher o impacto que o processo de análise deve ter no desempenho do seu sistema.
     - Automática - A prioridade do processo de análise dependerá da atividade do sistema. Para que o processo de análise não afete a atividade do sistema, o Bitdefender decide se o processo de análise deve ser executado com prioridade alta ou baixa.
     - Alta - A prioridade do processo de análise será alta. Ao escolher esta opção, permite que outros programas sejam executados mais devagar, diminuindo o tempo necessário para o processo de análise ser concluído.
     - Baixa - A prioridade do processo de análise será baixa. Ao escolher essa opção, permite que outros programas sejam executados mais rápido, aumentando o tempo necessário para o processo de análise ser concluído.

- **Ações pós-verificação**. Escolha a ação que o Bitdefender deve realizar se não forem encontradas ameaças:
  - Mostrar janela de resumo
  - Desligar dispositivo
  - Fechar janela da Análise

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

   Clique **Seguinte**.

6. Pode ativar a opção **Programar tarefa de análise** e, se quiser, escolha quando a análise personalizada que criou deve começar.
   - No iniciar do sistema
   - Diária
   - Mensal
   - Semanal

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

7. Clique em **Guardar** para guardar as definições e fechar a janela de configuração.

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

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

3.3.5. Como excluir uma pasta da análise?

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

As exceções devem ser usadas pelos utilizadores que possuem conhecimento informáticos avançados e apenas nas seguintes situações:

- Você tem uma pasta grande no seu sistema onde guarda filmes e música.
- Você tem um ficheiro grande no seu sistema onde guarda diferentes dados.

- Você tem uma pasta onde instala diferentes tipos de software e aplicações para testar. A análise da pasta pode resultar na perda de alguns dados.

Para adicionar uma pasta à lista de Exceções:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Clique na barra **Definições** .
4. Clique em **Gerir Exceções**.
5. Clique em **+Adicionar uma Exceção**.
6. Introduza no campo correspondente o caminho da pasta que pretende adicionar à lista de exceção da análise.

   Como alternativa, pode navegar até a pasta ao clicar no botão navegar no lado direito da interface, selecioná-la e clicar em **OK**.
7. Ligue o interruptor junto à funcionalidade de proteção que não deve analisar a pasta. Há três opções:
   - Antivírus
   - Prevenção de Ameaças Online
   - Advanced Threat Defense
8. Clique em **Guardar** para guardar as alterações e fechar a janela.

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

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

1. Desative a proteção antivírus em tempo real do Bitdefender:
   a. Clique em **Definições** no menu de navegação na interface do Bitdefender.
   b. No painel **ANTIVÍRUS**, clique em **Abrir**.
   c. Na janela **Avançada**, desative o **Escudo do Bitdefender**.

      Aparece uma janela de aviso. Tem de confirmar a sua escolha seleccionando no menu durante quanto tempo pretende desactivar a

protecção em tempo real. Pode desativar a sua proteção em tempo real durante 5, 15 ou 30 minutos, por uma hora, permanentemente ou até ao reinício do sistema.

2. Mostrar objetos ocultos no Windows. Para saber como o fazer, consulte "*Como posso mostrar objetos ocultos no Windows?*" (p. 67).
3. Restaurar o ficheiro da área de Quarentena:
   a. Clique em **Definições** no menu de navegação na interface do Bitdefender.
   b. No painel **ANTIVÍRUS**, clique em **Abrir**.
   c. Vá para a janela **Definições** e clique em **Gerir a quarentena**.
   d. Selecione o ficheiro e, em seguida, clique em **Restaurar**.
4. Adicionar o ficheiro à lista de Exceções. Para saber como o fazer, consulte "*Como excluir uma pasta da análise?*" (p. 48).

   Por predefinição, a Bitdefender adiciona automaticamente ficheiros restaurados à lista de exceções.
5. Ligue a proteção antivírus em tempo real do Bitdefender.
6. Contacte os nossos representantes do suporte para que possamos remover a deteção de atualizações de informações sobre ameaças. Para saber como o fazer, consulte "*Pedir Ajuda*" (p. 302).

3.3.7. Como posso saber que ameaças o Bitdefender detetou?

Cada vez que uma análise é levada a cabo, um registo de análise é criado e o Bitdefender regista as incidências detetadas.

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

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

Para verificar um registo de análise ou qualquer infeção detetada posteriormente:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Todas**, selecione a notificação referente à última análise.

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

3. Na lista de notificações, pode ver as análises que foram recentemente efectuadas. Clique numa notificação para visualizar detalhes sobre o mesmo.
4. Para abrir um relatório da análise, clique em **Ver Relatório**.

3.4. Controlo Parental

3.4.1. Como posso proteger os meus filhos de ameaças online?

O Controlo Parental do Bitdefender permite que limite o acesso à Internet e a aplicações específicas, prevenindo que seus filhos visualizem conteúdos inapropriados quando não estiver por perto.

Para configurar o Controlo Parental:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **CONTROLO PARENTAL**, clique em **Configurar**.

   Será redirecionado para a página Web da conta Bitdefender. Certifique-se de que tem sessão iniciada com as suas credênciais
3. O painel do Controlo Parental abre. Áqui é o local onde poderá verificar e configurar as definições do Controlo Parental.
4. Clique em **ADICIONAR UM PERFIL INFANTIL**.
5. Estabelecer informações específicas como nome, data de nascimento ou sexo. Para adicionar uma foto ao perfil da sua criança, clique no ícone no canto inferior direito da opção **Foto de perfil**. Clique em **GUARDAR** para continuar.

   Com base no desenvolvimento infantil, definir a idade da criança carrega automaticamente as definições para pesquisar na Web consideradas apropriadas para a sua faixa etária.
6. Clique em **VAMOS ADICIONAR UM DISPOSITIVO**.

7. Se o dispositivo da sua criança já tiver a Bitdefender instalado, selecione o seu dispositivo na lista disponível e, em seguida, selecione a conta que deseja monitorizar. Clique em **ATRIBUIR**.

   Se a sua criança não tem o produto Bitdefender instalado no dispositivo que ele utiliza, clique em **Instalar um novo dispositivo** e, em seguida, clique em **Enviar link de transferência**. Escreva um endereço de email no campo correspondente e clique em **ENVIAR EMAIL**. Observe que a hiperligação de download gerada será válida apenas durante as próximas 24 horas. Se a hiperligação expirar, precisará de gerar uma nova seguindo os mesmos passos.

   No dispositivo em que deseja instalar a Bitdefender, verifique a conta de e-mail que escreveu e clique no botão de transferência correspondente.

Importante
Em dispositivos do Windows ou macOS sem o produto Bitdefender instalado, o monitorizador de verificação do Controlo Parental da Bitdefender será instalado para monitorizar as atividades online das suas crianças.
Em dispositivos Android e iOS, será feita a transferência e instalada a aplicação de Controlo Parental da Bitdefender.

3.4.2. Como bloqueio o acesso do meu filho a um website?

O Controlo Parental do Bitdefender permite que controle o conteúdo acedido pelos seus filhos nos seus dispositivos, e também lhe permite que bloqueie o acesso a determinados sites.

Para bloquear o acesso a um site, precisa de adicioná-lo à lista de Exceções, conforme se segue:

1. Vá para: https://central.bitdefender.com.
2. Inicie sessão na sua conta Bitdefender utilizando o seu endereço de e-mail e palavra-passe.
3. Clique em **Controlo Parental** para aceder ao painel.
4. Selecione o perfil da sua criança.
5. Clique no separador de **OPÇÕES** e, em seguida, clique em **Websites**.
6. Clique em **GERIR**.
7. Escreva o site que deseja bloquear no campo correspondente.
8. Selecione **Bloquear**.

9. Clique no ícone para guardar as alterações e, em seguida, clique em **FEITO**.

Nota
Podem ser configuradas restrições apenas para dispositivos Android, macOS e Windows.

3.4.3. Como evito que os meus filhos utilizem certas aplicações?

O Controlo Parental da Bitdefender permite controlar o conteúdo acedido pelas suas crianças ao utilizar os seus dispositivos.

Para bloquear o acesso a uma aplicação:

1. Vá para: https://central.bitdefender.com.
2. Inicie sessão na sua conta Bitdefender utilizando o seu endereço de e-mail e palavra-passe.
3. Clique em **Controlo Parental** para aceder ao painel.
4. Selecione um perfil infantil.
5. Clique em **OPÇÕES** e selecione **Aplicações**.
6. Será exibida uma lista com os dispositivos atribuídos.

   Selecione o cartão com o dispositivo cujo acesso a aplicações deseja limitar.
7. Clique em **Gerir aplicações utilizadas por...**.

   Será exibida uma lista das aplicações instaladas.
8. Selecione **Bloqueado** próximo às aplicações que deseja que o seu filho pare de utilizar.
9. Clique em **GUARDAR** para aplicar as novas definições.

Nota
Podem ser configuradas restrições apenas para dispositivos Android, macOS e Windows.

3.4.4. Como posso definir um local como seguro ou restrito para o meu filho?

O Controlo Parental do Bitdefender permite definir um local como seguro ou restrito para o seu filho.

Para definir uma localização:

1. Vá para: https://central.bitdefender.com.
2. Inicie sessão na sua conta Bitdefender utilizando o seu endereço de e-mail e palavra-passe.
3. Clique em **Controlo Parental** para aceder ao painel.
4. Selecione o perfil da sua criança.
5. Clique em **OPÇÕES** e selecione **Localização da criança**.
6. Clique em **Dispositivos** dentro da janela **Localização da criança**.
7. Clique no dispositivo que deseja configurar.
8. Na janela **Áreas**, clique no botão **ADICIONAR ÁREA**.
9. Escolha o tipo de local, **SEGURO** ou **RESTRITO**.
10. Escreva um nome válido para a área onde o seu filho tenha ou não permissão para aceder.
11. Defina a distância que deverá ser utilizada para monitorização na barra **Raio**.
12. Clique em **ADICIONAR ÁREA** para guardar as suas definições.

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

3.4.5. Como posso bloquear o acesso do meu filho aos dispositivos atribuídos durante as atividades diárias?

O Controlo Parental da Bitdefender permite limitar o acesso do seu filho aos dispositivos atribuídos durante atividades diárias, como as horas de escola, quando ele tiver que fazer os trabalhos de casa ou depois da hora de ir dormir.

Para configurar as restrições de tempo:

1. Vá para: https://central.bitdefender.com.
2. Inicie sessão na sua conta Bitdefender utilizando o seu endereço de e-mail e palavra-passe.
3. Clique em **Controlo Parental** para aceder ao painel.
4. Selecione o perfil da criança que pretenda estabelecer restrições.
5. Clique em **OPÇÕES** e selecione **Tempo de ecrã**.
6. Na área de **Agendamentos**, clique em **Adicionar agendamento**.
7. Dê um nome à restrição que deseja definir (por exemplo, hora de ir para a cama, trabalho de casa, aulas de ténis, etc.).
8. Defina um período de tempo no qual as restrições devem ser aplicadas e, em seguida, clique em **ADICIONAR AGENDAMENTO** para guardar as definições.

3.4.6. Como bloqueio o acesso do meu filho aos dispositivos atribuídos durante o dia ou a noite?

O Controlo Parental da Bitdefender permite limitar o acesso do seu filho aos dispositivos atribuídos a horas diferentes horas durante um dia.

Para configurar um limite de utilização diária:

1. Vá para: https://central.bitdefender.com.
2. Inicie sessão na sua conta Bitdefender utilizando o seu endereço de e-mail e palavra-passe.
3. Clique em **Controlo Parental** para aceder ao painel.
4. Selecione o perfil da criança que pretenda estabelecer restrições.
5. Clique em **OPÇÕES** e selecione **Tempo de ecrã**.
6. Na área **Limites de tempo diários**, clique em **DEFINIR LIMITE DE TEMPO DIÁRIO**.
7. Defina a hora e o dia nos quais as restrições devem ser aplicadas e, em seguida, clique em **GUARDAR ALTERAÇÕES** para guardar as definições.

3.4.7. Como remover um perfil de criança

Se pretender remover um perfil infantil existente:

1. Vá para: https://central.bitdefender.com.
2. Inicie sessão na sua conta Bitdefender utilizando o seu endereço de e-mail e palavra-passe.
3. Clique em **Controlo Parental** para aceder ao painel.
4. Selecione o perfil infantil que deseja eliminar.
5. Clique em **OPÇÕES** e selecione **Eliminar perfil**.
6. Confirme a sua escolha.

3.5. Protecção de Privacidade

3.5.1. 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, pode usar o browser fornecido pelo Bitdefender para proteger as suas transações e as suas aplicações bancárias.

O Bitdefender Safepay™ é um navegador desenhado para proteger as informações do seu cartão de crédito, número de conta ou qualquer outro dado pessoal que possa utilizar enquanto acede a diferentes localizações online.

Para manter a sua atividade online segura e privada:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel do **SAFEPAY**, clique em **Definições**.
3. Na janela do **Safepay**, clique em **Iniciar Safepay**.
4. Clique no ícone  para aceder ao **Teclado Virtual**.

   Use o **Teclado Virtual** quando inserir informação sensível tal como palavras-passe.

3.5.2. O que posso fazer se o meu dispositivo tiver sido roubado?

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

O Anti-Roubo do Bitdefender permite não só localizar e bloquear o dispositivo roubado, como também apagar todos os dados para garantir que não será utilizado pelo ladrão.

Para aceder às funções anti-furto da sua conta:

1. Aceda Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.
3. Clique no cartão do dispositivo pretendido e, em seguida, selecione **Anti-furto**.
4. Selecione a funcionalidade que deseja usar:
   - **LOCALIZAR** - exibe a localização do seu dispositivo no Google Maps.
   - **Alerta** - emite um alerta no dispositivo.
   - **Bloquear** - bloqueie o seu dispositivo e defina um código numérico PIN para o desbloquear. Alternativamente, ative a opção correspondente para permitir que o Bitdefender tire fotos da pessoa que está a tentar aceder ao seu dispositivo.
   - **Limpar** - eliminar todos os dados do seu dispositivo.

     Importante
     Após apagar toda a informação de um dispositivo, todas as funcionalidades Anti-Roubo deixam de funcionar.

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

3.5.3. Como removo um ficheiro permanentemente com o Bitdefender?

Se deseja remover um ficheiro permanentemente do seu sistema, necessita de apagar a informação fisicamente do seu disco duro.

O Destruidor de Ficheiros do Bitdefender pode ajudá-lo a rapidamente destruir ficheiros ou pastas do seu dispositivo utilizando o menu contextual Windows ao seguir os seguintes passos:

1. Clique com o botão direito do rato no ficheiro ou pasta que deseja apagar permanentemente, aponte para o Bitdefender e selecione **Destruidor de Ficheiros**.
2. Clique em **Eliminar permanentemente** e, em seguida, confirme que deseja continuar com o processo.

   Aguarde que o Bitdefender termine a destruição dos ficheiros.
3. Os resultados são apresentados. Clique em **TERMINAR** para sair do assistente.

3.5.4. Como protejo a minha câmara Web contra hacking?

Pode configurar o produto Bitdefender para permitir ou negar o acesso das aplicações instaladas à sua câmara Web ao seguir estes passos:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel de **PROTEÇÃO DE VÍDEO E ÁUDIO**, clique em **Definições**.
3. Vá para a janela **Proteção da Webcam** e verá a lista com as aplicações que solicitaram acesso à sua câmara.
4. Indique a aplicação cujo acesso deseja permitir ou proibir e, em seguida, clique no botão representado por uma câmara de vídeo, situada ao lado dele.

   Para ver o que os outros utilizadores do Bitdefender optaram por fazer com a aplicação selecionada, clique no ícone . Você será notificado sempre que uma dos aplicativções listadas for bloqueada por utilizadores do Bitdefender.

Para adicionar aplicações manualmente a esta lista, clique no botão **Adicionar aplicação** e selecione uma das duas opções.

- Da Windows Store

- Das suas aplicações

3.5.5. Como posso restaurar manualmente ficheiros encriptados quando o processo de restauração falhar?

Caso ficheiros encriptados não possam ser automaticamente restaurados, pode restaurá-los manualmente seguindo estes passos:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador**Todas**, selecione a notificação referente ao último comportamento de ransomware detectado e, em seguida, clique em **Ficheiros Encriptados**.
3. Será exibida a lista dos ficheiros encriptados.

   Clique em **Recuperar ficheiros** para continuar.
4. Caso o processo de recuperação falhe inteira ou parcialmente, deve escolher o local em que os ficheiros encriptados devem ser guardados. Clique em **Restaurar localização** e, em seguida, escolha uma localização no seu PC.
5. Aparece uma janela de confirmação.

   Clique em **Finalizar** para terminar o processo de restauração.

Ficheiros com as seguintes extensões podem ser restaurados caso sejam encriptados:

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

3.6. Ferramentas de Otimização

3.6.1. Como posso usar melhorar o desempenho do meu sistema?

O desempenho do sistema não depende apenas das características do hardware, tais como a capacidade do CPU, a memória disponível e o espaço

no disco rígido. Está, também, diretamente relacionada com a configuração do software e com a gestão dos dados.

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

- "*Otimize o desempenho do seu sistema com um único clique*" (p. 60)
- "*Analise o seu sistema periodicamente*" (p. 60)

Otimize o desempenho do seu sistema com um único clique

A opção Otimizador de Um Clique poupa-lhe quando quer uma maneira rápida de melhorar o desempenho do sistema ao analisar, detectar e limpar rapidamente ficheiros inúteis.

Para iniciar o processo do OneClick Optimizer:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. Clique no botão **Otimizar**.
3. Deixe que o Bitdefender procure ficheiros que possam ser eliminados, depois clique no botão **Otimizar** para concluir o processo.

Analise o seu sistema periodicamente

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

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

Recomenda-se a utilização da Análise do Sistema pois a mesma analisa todos os tipos de ameaças que prejudicam a segurança do seu sistema e também analisa dentro dos ficheiros.

Para iniciar a Verificação do Sistema:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Clique em **Executar análise** ao lado de **Análise do sistema**.
4. Siga os passos do assistente.

3.7. Informações Úteis

3.7.1. Como posso testar a minha solução de segurança?

Para garantir que o seu produto Bitdefender está a funcionar corretamente, recomendamos a utilização do teste Eicar.

O teste Eicar permite que verifique a sua solução de segurança utilizando um ficheiro de segurança desenvolvido para este fim.

Para testar a sua solução de segurança:

1. Transfira o teste da página Web oficial da organização EICAR http://www.eicar.org/.
2. Clique no separador **Ficheiro de teste antimalware**.
3. Clique em **Transferir** no menu do lado esquerdo.
4. A partir da **área de transferência utilizando o protocolo padrão http** clique no ficheiro de teste **eicar.com**.
5. Receberá informações de que a página a que está a tentar aceder contém o Ficheiro de Teste EICAR (não é uma ameaça).

   Caso clique em **Compreendo os riscos, leve-me até lá mesmo assim**, a transferência do teste irá iniciar e um pop-up do Bitdefender irá informá-lo da deteção de uma ameaça.

   Clique em **Mais Detalhes** para obter mais informações sobre esta ação.

Caso não receba qualquer alerta de Bitdefender, recomendamos que entre em contacto com Bitdefender para suporte conforme descrito na secção "*Pedir Ajuda*" (p. 302).

3.7.2. Como posso remover o Bitdefender?

Se pretender remover o seu Bitdefender Total Security:

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

4. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

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

1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
2. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
4. Clique em **REMOVER** na janela que aparece.
5. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

- No **Windows 10**:

1. Clique em **Iniciar**, em seguida, clique em Definições.
2. Clique no ícone **Sistema** na área de Configurações e, em seguida, selecione **Aplicações**.
3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
4. Clique em **Desinstalar** novamente para confirmar a sua escolha.
5. Clique em **REMOVER** na janela que aparece.
6. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

Nota
Este procedimento de reinstalação irá eliminar permanentemente as definições personalizadas.

3.7.3. Como removo o Bitdefender VPN?

O procedimento de remoção do Bitdefender VPN é semelhante ao que utiliza para remover outros programas do seu dispositivo:

- No **Windows 7**:

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

Aguarde até que o processo de desinstalação seja concluído.

- No **Windows 8 e Windows 8.1**:
  1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
  2. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
  3. Encontre **Bitdefender VPN** e selecione **Desinstalar**.

     Aguarde até que o processo de desinstalação seja concluído.
- No **Windows 10**:
  1. Clique em **Iniciar**, em seguida, clique em Definições.
  2. Clique no ícone **Sistema** na área das Definições, em seguida, selecione **Aplicações instaladas**.
  3. Encontre **Bitdefender VPN** e selecione **Desinstalar**.
  4. Clique em **Desinstalar** novamente para confirmar a sua escolha.

     Aguarde até que o processo de desinstalação seja concluído.

3.7.4. Como é que removo a extensão Antitracker da Bitdefender?

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

- Internet Explorer
  1. Clique em  ao lado da barra de pesquisa e, em seguida, selecione Gerir suplementos.

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

Será exibida a lista das extensões instaladas.

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

- Mozilla Firefox

1. Clique em  ao lado da barra de pesquisa.
2. Selecione **Suplementos** e, em seguida, selecione **Extensões**.

   Será exibida a lista das extensões instaladas.

3. Clique em e, em seguida, selecione **Remover**.

3.7.5. Como desligo automaticamente o meu dispositivo após terminar a análise?

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

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

Considere este exemplo: terminou o seu trabalho e quer ir dormir. Gostaria que o seu sistema fosse completamente analisado quanto a ameaças pelo Bitdefender.

Para desligar o dispositivo uma vez finalizada a Análise Rápida ou a Análise de Sistema:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela de **Análises**, clique em próximo para Análise Rápida e, em seguida, selecione **Editar**.
4. Personalize a análise de acordo com as suas necessidades e clique em **Seguinte**.
5. Marque a caixa ao lado de **Escolher quando agendar esta tarefa** e, em seguida, escolha quando a tarefa deve começar.

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

6. Clique em **Guardar**.

Para desligar o dispositivo ao finalizar uma análise personalizada:

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

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

Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas. Para mais informação, dirija-se a "*Assistente de Análise Antivírus*" (p. 81).

3.7.6. Como posso configurar Bitdefender para usar um proxy de ligação à Internet?

Se o seu dispositivo se ligar à Internet através de um servidor proxy, deve configurar as definições do proxy do Bitdefender. Normalmente, o Bitdefender deteta e importa automaticamente as definições proxy do seu sistema.

> **Importante**
> As ligações à Internet domésticas normalmente não usam um servidor proxy. Como regra de ouro, verifique e configure as definições da ligação proxy do seu programa Bitdefender quando as atualizações não funcionam. Se o Bitdefender atualizar, então está corretamente configurado à Internet.

Para gerir as definições de proxy:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. Selecione o separador **Avançado**.
3. Ative o **Servidor proxy**.
4. Clique em **Mudança de proxy**.
5. Existem duas opções para as definições do proxy:

- **Importe as definições de proxy do navegador por defeito** - as definições de proxy do utilizador actual, extraídas do explorador por defeito. Se o servidor proxy requer um nome de utilizador e uma palavra-passe, deverá inseri-los nos campos correspondentes.

  Nota
  O Bitdefender pode importar definições de proxy dos browsers mais populares, incluindo as mais recentes versões do Microsoft Edge, Internet Explorer, Mozilla Firefox e Google Chrome.

- **Definições de proxy personalizadas** - definições de proxy que você pode configurar. As seguintes definições devem ser especificadas:
  - **Endereço** - introduza o IP do servidor proxy.
  - **Porta** - insira a porta que o Bitdefender usa para se ligar ao servidor proxy.
  - **Nome de Utilizador** - introduza um nome de utilizador reconhecido pelo proxy.
  - **Palavra-passe** - introduza uma palavra-passe válida para o utilizador previamente definido.

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

O Bitdefender usará as definições de proxy disponíveis até conseguir ligar à Internet.

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

Para descobrir se possui sistema operativo 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 do ecrã Iniciar do Windows, localize **Computador** (por exemplo, pode começar a digitar "Computador" diretamente no menu Iniciar) e, em seguida, clique com o botão direito do rato no seu ícone.

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

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

- No **Windows 10**:

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

3.7.8. Como posso mostrar objetos ocultos no Windows?

Estes passos são úteis nos casos de ameaças e se tiver de encontrar e remover os ficheiros infectados, que poderão estar ocultos.

Siga os seguintes passos para mostrar objetos ocultos no Windows:

1. Clique em **Iniciar**, aceda ao **Painel de Controlo**.

   No **Windows 8 e Windows 8.1**: a partir do ecrã Iniciar do Windows, localize o **Painel de Controlo** (por exemplo, introduza "Painel de Controlo" no ecrã Iniciar) e, em seguida, clique no ícone correspondente.
2. Selecione **Opções de Pastas**.
3. Abra o separador **Ver**.
4. Selecione **Mostrar ficheiros e pastas ocultos**.
5. Desmarque **Ocultar extensões nos tipos de ficheiro conhecidos**.
6. Desmarque **Ocultar ficheiros protegidos do sistema operativo**.
7. Clique em **Aplicar**, em seguida, clique em **OK**.

No **Windows 10**:

1. Introduza "Mostrar ficheiros e pastas ocultos" na caixa de pesquisa da barra de tarefas e, em seguida, clique no ícone correspondente.
2. Selecione **Mostrar ficheiros, pastas e unidades ocultos**.
3. Desmarque **Ocultar extensões nos tipos de ficheiro conhecidos**.
4. Desmarque **Ocultar ficheiros protegidos do sistema operativo**.
5. Clique em **Aplicar**, em seguida, clique em **OK**.

3.7.9. 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 Total Security deteta automaticamente outros programas de segurança e oferece-lhe a opção de os desinstalar.

Se não tiver removido as outras soluções de segurança durante a instalação inicial:

- No **Windows 7**:
  1. Clique em **Iniciar**, vá ao **Painel de Controlo** 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 pela conclusão do processo de desinstalação e reinicie o sistema.
- No **Windows 8 e Windows 8.1**:
  1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
  2. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
  3. 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 pela conclusão do processo de desinstalação e reinicie o sistema.
- No **Windows 10**:
  1. Clique em **Iniciar**, em seguida, clique em Definições.

2. Clique no ícone **Sistema** na área de Configurações e, em seguida, selecione **Aplicações**.
3. Encontre o nome do programa que pretende remover e selecione **Desinstalar**.
4. Clique em **Desinstalar** novamente para confirmar a sua escolha.
5. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

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

3.7.10. Como posso reiniciar no Modo de Segurança?

O Modo de Segurança é um modo operativo de diagnóstico, utilizado principalmente para detetar e resolver problemas que estejam a afetar o funcionamento normal do Windows. As causas destes problemas vão desde a incompatibilidade de controladores a ameaças que impedem o arranque normal do Windows. No Modo de Segurança funcionam apenas algumas aplicações e o Windows só carrega os controladores básicos e os componentes mínimos do sistema operativo. É por isso que a maioria das ameaças está inativa quando o Windows está no Modo de Segurança e podem ser facilmente removidos.

Para iniciar o Windows no Modo de Segurança:

- No **Windows 7**:
  1. Reinicie o dispositivo.
  2. Prima a tecla **F8** várias vezes antes de o Windows iniciar para aceder ao menu de arranque.
  3. Selecione **Modo Seguro** no menu de inicialização ou **Modo Seguro com Rede** se quiser ter acesso à Internet.
  4. Prima em **Enter** e aguarde enquanto o Windows carrega o Modo Seguro.
  5. Este processo termina com uma mensagem de confirmação. Clique em **OK** para 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. Escreva **msconfig**na caixa de diálogo **Abrir** ,depois clique em **OK**.
3. Selecione o separador **Arranque**.
4. Na área **Opções de arranque** selecione a caixa **Arranque seguro**.
5. Clique em **Rede** e depois em **OK**.
6. Clique em **OK** na janela **Configuração do Sistema**, que o informa de que o sistema necessita de ser reiniciado para as mudanças serem aplicadsa.

   O seu sistema será reiniciado no Modo Seguro com rede.

Para reiniciar no modo normal, reverta as definições executando novamente a **Operação do Sistema** e desmarcando a caixa **Arranque seguro**. Clique em **OK** e depois em **Reiniciar**. Aguarde para que as novas definições sejam aplicadas.

4. GERIR A SUA SEGURANÇA

4.1. Proteção Antivírus

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

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

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

  > **Importante**
  > Para prevenir a infeção de ameaças no seu dispositivo, mantenha ativada a **análise no acesso**.

- Análise a pedido - permite detetar e remover ameaças que já se encontram no sistema. Esta é uma análise clássica iniciada pelo utilizador – você escolhe qual a drive, pasta ou ficheiro o Bitdefender deverá analisar, e o mesmo é analisado – a-pedido.

O Bitdefender analisa automaticamente qualquer media removível que esteja ligado ao dispositivo para garantir um acesso em segurança. Para mais informação, dirija-se a "*Análise automática de média removíveis*" (p. 85).

Os utilizadores avançados poderão configurar excepções se não desejarem que ficheiros ou tipos de ficheiros específicos sejam analisados. Para mais informação, dirija-se a "*A configurar exceções de análise*" (p. 87).

Quando deteta uma ameaça, o Bitdefender irá tentar remover automaticamente o código malicioso do ficheiro e reconstruir o ficheiro original. Esta operação é designada por desinfecção. Os ficheiros que não podem ser desinfectados são movidos para a quarentena de modo a conter a infecção. Para mais informação, dirija-se a "*Gerir ficheiros da quarentena*" (p. 90).

Se o seu dispositivo estiver infetado com ameaças, consulte "*Remover ameaças do seu sistema*" (p. 186). Para o ajudar a limpar as ameaças do dispositivo que não podem ser removidas no sistema operativo Windows, o Bitdefender proporciona-lhe o "*Ambiente de Resgate*" (p. 187). Este é um ambiente fiável, concebido sobretudo para a remoção de ameaças, que lhe permite arrancar o seu dispositivo independentemente do Windows. Quando o dispositivo é executado no Ambiente de Resgate, as ameaças do Windows estão inativas, tornando-as mais fáceis de remover.

4.1.1. Análise no acesso (proteção em tempo real)

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

Ligar ou desligar a proteção em tempo real

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

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Avançada**, ative ou desative o **Escudo do Bitdefender**.
4. Se pretender desativar a proteção em tempo real, aparece uma janela de aviso. Tem de confirmar a sua escolha seleccionando no menu durante quanto tempo pretende desactivar a protecção em tempo real. Pode desativar a sua proteção em tempo real durante 5, 15 ou 30 minutos, por uma hora, permanentemente ou até ao reinício 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 desactive a protecção em tempo-real o menos tempo possível. Quando a mesma está desactivada você deixa de estar protegido contra as ameaças.

Configuração das definições avançadas de proteção em tempo real

Os utilizadores avançados podem aproveitar as definições que o Bitdefender oferece. Pode configurar as definições da proteção em tempo real criando um nível de proteção personalizado.

Para configurar as definições avançadas de proteção em tempo real:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Avançado**, pode configurar as definições da verificação conforme necessário.

Informação sobre as opções de análise

Poderá achar esta informação útil:

- **Analisar apenas aplicações.** Você pode configurar o Bitdefender para só analisar as aplicações acedidas.
- **Analisar aplicações potencialmente indesejadas.** Selecione esta opção para analisar aplicações indesejadas. Uma aplicação potencialmente indesejada (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 vários anúncios. Esses programas podem ser instalados sem o seu consentimento (também chamados de adware) ou serão incluídos por defeito no seu kit de instalação expresso (apoiado por anúncios).
- **Analisar scripts.** A funcionalidade de análise de scripts permite ao Bitdefender analisar scripts da powershell e documentos de escritório que podem conter malware à base de scripts.
- **Analisar partilhas de rede.** Para aceder a uma rede remota com segurança desde o seu dispositivo, recomendamos que mantenha a opção de Analisar partilhas de rede ativa.
- **Analisar arquivos.** Analisar o interior de arquivos é um processo lento e que consome muitos recursos, não sendo, por isso recomendado para a proteção em tempo real. Os arquivos que contém ficheiros infectados não são uma ameaça imediata à segurança do seu sistema. A ameaça só pode

afetar o seu sistema se o ficheiro infetado for extraído do arquivo e executado sem que a proteção em tempo real esteja ativada.

Se escolher esta opção, ative-a e, em seguida, arraste o marcador pela escala para excluir da análise ficheiros mais longos do que um valor dado em MB (Megabites).

- **Analisar sectores de arranque.** Pode definir o Bitdefenderpara analisar os sectores de saída do seu disco rígido. Este sector do disco rígido contém o código do computadores necessário para iniciar o processo de reinício. Quando uma ameaça infe ta o setor de saída, a unidade pode tornar-se inacessível ou poderá não conseguir iniciar o seu sistema e aceder aos seus dados.
- **Verificar apenas ficheiros novos e modificados.** Ao verificar apenas ficheiros novos e modificados, pode melhorar significativamente a resposta geral do sistema com um sacrifício mínimo da segurança.
- **Analisar em busca de keyloggers.** Selecione esta opção para analisar o seu sistema em busca de aplicações 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 palavras-passe, e usá-las em benefício pessoal.
- **Verificação de arranque antecipado.** Selecione a opção **Verificação de inicialização antecipada** para verificar o seu sistema na inicialização assim que todos os serviços essenciais tenham sido carregados. A finalidade desta funcionalidade é melhorar a deteção de ameaças no arranque do sistema e o tempo de inicialização do sistema.

Ações tomadas em ameaças detetadas

Pode configurar as ações a serem levadas a cabo pela proteção em tempo-real seguindo estes passos:

1. Clique em **Definições** no menu de navegação na 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 levadas a cabo pela proteção em tempo real do Bitdefender:

Tomar acções adequadas

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

- **Ficheiros infectados.** Os ficheiros detetados como infetados correspondem a parte das informações de ameaças encontrada na Base de Dados de Informações de Ameaças do Bitdefender. Bitdefender tentará automaticamente remover o código malicioso do ficheiro infetado e reconstruir o ficheiro original. Esta operação é designada por desinfecção.

  Os ficheiros que não podem ser desinfectados são movidos para a quarentena de modo a conter a infecção. O ficheiros em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece. Para mais informação, dirija-se a "*Gerir ficheiros da quarentena*" (p. 90).

  > **Importante**
  > Para determinados tipos de ameaças, a desinfeção não é possível por o ficheiro detetado ser totalmente malicioso. Nestes casos, o ficheiro infectado é eliminado do disco.

- **Ficheiros suspeitos.** Os ficheiros são detectados como suspeitos pela análise heurística. Não foi possível desinfectar os ficheiros suspeitos por não estar disponível uma rotina de desinfecção. Serão movidos para a quarentena para evitar uma potencial infeção.

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

- **Aquivos que contêm ficheiros infetados.**
  - Os arquivos que contêm apenas ficheiros infectados são eliminados automaticamente.
  - Se um arquivo tiver ficheiros infectados e limpos, o Bitdefender tentará eliminar os ficheiros infectados desde que possa reconstruir o arquivo com os ficheiros limpos. Se não for possível a

reconstrução do arquivo, será informado de que não pode ser tomada qualquer ação, de forma a evitar perder ficheiros limpos.

Mover para a quarentena
Move os ficheiros infectados para a quarentena. O ficheiros em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece. Para mais informação, dirija-se a "*Gerir ficheiros da quarentena*" (p. 90).

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

Restaurar as predefinições

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

Para restaurar as definições da protecção em tempo real:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Avançado**, role a página para baixo até ver a opção **Repor as definições avançadas**. Selecione esta opção para repor as predefinições do antivírus.

4.1.2. Verificação por ordem

O objetivo principal do Bitdefender é manter o seu dispositivo livre de ameaças. Isto é feito ao manter as novas ameaças fora do seu dispositivo e ao analisar as suas mensagens de e-mail e quaisquer novos ficheiros transferidos ou copiados para o seu sistema.

Há o risco de a ameaça já ter acedido ao seu sistema, antes mesmo de ter instalado o Bitdefender. Este é o motivo pelo qual é uma excelente ideia verificar ameaças residentes no seu dispositivo depois de instalar o Bitdefender. E é definitivamente uma boa ideia analisar frequentemente o seu dispositivo quanto a ameaças.

A análise a-pedido está baseada em tarefas de análise. As tarefas de análise especificam as opções de análise e os objectos a serem analisados. Pode analisar o dispositivo sempre que quiser executar as tarefas por defeito ou as suas próprias tarefas de análise (tarefas definidas pelo utilizador). Se

quer analisar localizações específicas no seu dispositivo ou configurar as opções de análise, pode configurar e executar uma análise personalizada.

Procurar ameaças num ficheiro ou pasta

Deve analisar os ficheiros e as pastas sempre que suspeitar de uma infecção. Clique com o botão direito do rato sobre o ficheiro ou pasta que pretende analisar, aponte para o **Bitdefender** e selecione **Analisar com o Bitdefender**. O Assistente de Análise Antivírus irá surgir e guiá-lo através do processo de análise. No final da análise, será notificado para escolher as ações que devem ser tomadas nos ficheiros detetados, caso os haja.

Executar uma Análise Rápida

A Análise Rápida utiliza a análise nas nuvens para detetar ameaças em execução no seu sistema. Normalmente, a realização de uma Análise Rápida demora menos de um minuto e utiliza uma fração dos recursos do sistema necessários para uma análise antivírus normal.

Para realizar uma análise rápida:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Análises**, clique no botão **Executar análise** ao lado de **Análise rápida**.
4. Siga o assistente de Análise Antivírus para completar a análise. O Bitdefender tomará automaticamente as ações recomendadas nos ficheiros detetados. Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas.

Executar uma Análise do Sistema

A tarefa de Análise do Sistema procura em todo o dispositivo todos os tipos de ameaças que prejudicam a sua segurança, tais como malware, spyware, adware, rookits, etc.

Nota

Porque a **Análise do Sistema** leva a cabo uma análise minuciosa de todo o seu computador, a mesma poderá levar algum tempo. Portanto, recomenda-se que execute esta tarefa quando não estiver a utilizar o seu dispositivo.

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

- Certifique-se de que o Bitdefender está atualizado com a sua base de dados de informações de ameaças. Verificar o seu dispositivo utilizando bases de dados de informação de ameaças desatualizadas pode impedir que o Bitdefender detecte novas ameaças criadas desde a última atualização. Para mais informação, dirija-se a "*Mantenha o seu Bitdefender atualizado.*" (p. 33).
- Encerre todos os programas abertos.

Se quer analisar localizações específicas no seu dispositivo ou configurar as opções de análise, pode configurar e executar uma análise personalizada. Para mais informação, dirija-se a "*Configurar uma análise personalizada*" (p. 78).

Para realizar uma análise do sistema:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Análises**, clique no botão **Executar Análise** ao lado de **Análise do Sistema**.
4. A primeira vez que executar uma Análise do Sistema, verá uma apresentação da função. Clique em **OK, entendi** para continuar.
5. Siga o assistente de Análise Antivírus para completar a análise. O Bitdefender tomará automaticamente as ações recomendadas nos ficheiros detetados. Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas.

Configurar uma análise personalizada

Sempre que achar que o seu dispositivo precisar de ser analisado quanto a ameaças potenciais, pode configurar a Bitdefender para realizar análises utilizando a janela **Gerir análises**. Pode programar uma Análise de Sistema, uma Análise Rápida, ou pode criar uma análise personalizada segundo as suas necessidades.

Para configurar uma nova análise personalizada detalhadamente:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Nas janelas **Análises**, clique em **+Criar análise**.

4. No campo **Nome da tarefa**, introduza o nome da análise e, em seguida, selecione os locais que deseja analisar e, em seguida, clique em **Seguinte**.
5. Configure as seguintes opções gerais:
   - **Analisar apenas aplicações**. Você pode configurar o Bitdefender para só analisar as aplicações acedidas.
   - **Verificar prioridade de tarefa**. Pode escolher o impacto que o processo de análise deve ter no desempenho do seu sistema.
     - Automática - A prioridade do processo de análise dependerá da atividade do sistema. Para que o processo de análise não afete a atividade do sistema, o Bitdefender decide se o processo de análise deve ser executado com prioridade alta ou baixa.
     - Alta - A prioridade do processo de análise será alta. Ao escolher esta opção, permite que outros programas sejam executados mais devagar, diminuindo o tempo necessário para o processo de análise ser concluído.
     - Baixa - A prioridade do processo de análise será baixa. Ao escolher essa opção, permite que outros programas sejam executados mais rápido, aumentando o tempo necessário para o processo de análise ser concluído.
   - **Ações pós-verificação**. Escolha a ação que o Bitdefender deve realizar se não forem encontradas ameaças:
     - Mostrar janela de resumo
     - Desligar dispositivo
     - Fechar janela da Análise
6. Se deseja configurar as opções de análise detalhadamente, clique em **Mostrar opções avançadas**. Poderá encontrará informações sobre as análises listadas no final desta seção.

   Clique **Seguinte**.
7. Pode ativar a opção **Programar tarefa de análise** se quiser e, em seguida, escolha quando a análise personalizada que criou deve começar.
   - No iniciar do sistema
   - Diária
   - Mensal

- Semanal

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

8. Clique em **Guardar** para guardar as definições e fechar a janela de configuração.

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

Informação sobre as opções de análise

Poderá achar esta informação útil:

- Se não está familiarizado com alguns dos termos, procure-os no glossário. Pode também encontrar informação útil pesquisando a Internet.
- **Analisar aplicações potencialmente indesejadas.** Selecione esta opção para analisar aplicações indesejadas. Uma aplicação potencialmente indesejada (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 vários anúncios. Esses programas podem ser instalados sem o seu consentimento (também chamados de adware) ou serão incluídos por defeito no seu kit de instalação expresso (apoiado por anúncios).
- **Analisar arquivos.** Os arquivos que contém ficheiros infectados não são uma ameaça imediata à segurança do seu sistema. A ameaça só pode afetar o seu sistema se o ficheiro infetado for extraído do arquivo e executado sem que a proteção em tempo real esteja ativada. No entanto, é recomendado que utilize esta opção para detetar e remover qualquer ameaça potencial, mesmo se não for imediata.

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

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

- **Verificar apenas ficheiros novos e modificados.** Ao verificar apenas ficheiros novos e modificados, pode melhorar significativamente a resposta geral do sistema com um sacrifício mínimo da segurança.
- **Analisar sectores de arranque.** Pode definir o Bitdefenderpara analisar os sectores de saída do seu disco rígido. Este sector do disco rígido contém o código do computadores necessário para iniciar o processo de reinício. Quando uma ameaça infe ta o setor de saída, a unidade pode tornar-se inacessível ou poderá não conseguir iniciar o seu sistema e aceder aos seus dados.
- **Analisar memória.** Selecione esta opção para analisar programas executados na memória do seu sistema.
- **Analisar registo.** Selecione esta opção para analisar as chaves de registo. O Registo do Windows é uma base de dados que armazena as definições da configuração e as opções para os componentes do sistema operativo Windows, bem como para as aplicações instaladas.
- **Analisar cookies.** Selecione esta opção para analisar os cookies armazenados pelos navegadores no seu dispositivo.
- **Analisar em busca de keyloggers.** Selecione esta opção para analisar o seu sistema em busca de aplicações 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 palavras-passe, e usá-las em benefício pessoal.

Assistente de Análise Antivírus

Sempre que inicie 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 surgir, a análise poderá estar configurada para correr silenciosamente, em segundo plano. Procure pelo ícone do progresso da análise na área de notificação. Pode clicar nesse ícone para abrir a janela da análise e ver o seu progresso.

Passo 1 - Realizar Análise

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

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

Parar ou pausar a análise. Pode interromper a análise a qualquer altura que quiser clicando em **PARAR**. Irá directamente para o último passo do assistente. Para parar temporariamente o processo de análise, clique em **PAUSA**. Terá de clicar em**RETOMAR** para retomar a análise.

Arquivos protegidos com palavra-passe. Quando é detectado um arquivo protegido por palavra-passe, dependendo das definições da análise, poderá ter de indicar a palavra-passe. Os arquivos protegidos por palavra-passe não podem ser analisados a não ser que forneça a palavra-passe. Estão disponíveis as seguintes opções:

- **Palavra-passe.** Se quer que o Bitdefender analise o arquivo, selecione esta opção e insira a palavra-passe. Se não sabe a palavra-passe, escolha uma das outras opções.
- **Não pergunte pela palavra-passe e não analise este objeto.** Selecione esta opção para saltar a análise deste arquivo.
- **Skip all password-protected items without scanning them.** Selecione esta opção se não deseja ser incomodado acerca de arquivos protegidos por palavra-passe. O Bitdefender não será capaz de os analisar, mas um registo dos mesmos será mantido no relatório da análise.

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

Passo 2 - Escolher Ações

No final da análise, será notificado para escolher as ações que devem ser tomadas nos ficheiros detetados, caso os haja.

Nota

Quando realiza uma verificação rápida ou do sistema, o Bitdefender automaticamente aplica as ações recomendadas nos ficheiros detetados durante a verificação. Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas.

Os objetos infetados são apresentados em grupos, baseados no tipo de ameaças com que estão infetados. Clique no link correspondente a uma ameaça para descobrir mais informação acerca dos objetos infectados.

Pode escolher uma ação geral a ser levada a cabo para todas as incidências ou pode escolher ações separadas para cada grupo de incidências. Uma ou várias das seguintes opções poderão aparecer no menu:

Tomar acções adequadas

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

- **Ficheiros infectados.** Os ficheiros detetados como infetados correspondem a parte das informações de ameaças encontrada na Base de Dados de Informações de Ameaças do Bitdefender. Bitdefender tentará automaticamente remover o código malicioso do ficheiro infetado e reconstruir o ficheiro original. Esta operação é designada por desinfecção.

  Os ficheiros que não podem ser desinfectados são movidos para a quarentena de modo a conter a infecção. O ficheiros em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece. Para mais informação, dirija-se a "*Gerir ficheiros da quarentena*" (p. 90).

  > **Importante**
  > Para determinados tipos de ameaças, a desinfeção não é possível por o ficheiro detetado ser totalmente malicioso. Nestes casos, o ficheiro infectado é eliminado do disco.

- **Ficheiros suspeitos.** Os ficheiros são detectados como suspeitos pela análise heurística. Não foi possível desinfectar os ficheiros suspeitos por não estar disponível uma rotina de desinfecção. Serão movidos para a quarentena para evitar uma potencial infeção.

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

- **Aquivos que contêm ficheiros infetados.**

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

Apagar
Remove os ficheiros detectados do disco.

Se os ficheiros infectados estiverem armazenados num arquivo junto com ficheiros limpos, o Bitdefender tentará eliminar os ficheiros infectados e reconstruir o arquivo com ficheiros limpos. Se não for possível a reconstrução do arquivo, será informado de que não pode ser tomada qualquer ação, de forma a evitar perder ficheiros limpos.

Não Tomar Acção
Nenhuma acção será levada a cabo sobre os ficheiros detectados. Após a analisar terminar, pode abrir o relatório da análise para ver informação sobres esses ficheiros.

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

Passo 3 - Resumo

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

Importante

Na maioria dos casos o Bitdefender desinfecta com sucesso o ficheiro infectado ou isola a infecção. No entanto, há incidências que não podem ser automaticamente resolvidas. Se necessário, ser-lhe-à solicitado que reinicie o seu computador, para que o processo de limpeza seja completado. Para mais informações e instruções sobre como remover manualmente uma ameaça, consulte "*Remover ameaças do seu sistema*" (p. 186).

Ver os relatórios da análise

Sempre que uma análise for efetuada, é criado um registo de análise e o Bitdefender regista as incidências detectadas na janela Antivírus. O relatório

da análise contém informação detalhada acerca dos processos de análise registados, tal como as opções da análise, o alvo da análise, as ameaças encontradas e as acções tomadas sobre essas ameaças.

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

Para verificar um registo de análise ou qualquer infeção detetada posteriormente:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Todas**, selecione a notificação referente à última análise.

   Aqui poderá encontrar todos os eventos de análise de ameaças, incluindo ameaças detectadas na análise no acesso, análises iniciadas pelo utilizador e alterações de estado para as análises automáticas.
3. Na lista de notificações, pode ver as análises que foram recentemente efectuadas. Clique numa notificação para visualizar detalhes sobre o mesmo.
4. Para abrir o relatório da análise, clique em **Ver Relatório**.

4.1.3. Análise automática de média removíveis

O Bitdefender deteta automaticamente quando um dispositivo de armazenamento removível é ligado ao dispositivo e analisa-o em segundo plano quando a opção de Análise automática está ativada. Isto é recomendado para evitar que ameaças infetem o seu dispositivo.

Os dispositivos detetados encaixam-se numa destas categorias:

- CDs/DVDs
- Dispositivos de armazenamento externos como pen USB e discos rígidos externos
- Unidades de Rede Mapeadas (remotas)

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

Como funciona?

Ao detectar um dispositivo de armazenamento removível, o Bitdefender começa a analisá-lo à procura de ameaças (desde que a análise automática

esteja ativa para esse tipo de dispositivo). Será notificado através de uma janela de pop-up que um novo dispositivo foi detetado e está a ser analisado.

Um ícone de análise do Bitdefender irá aparecer no tabuleiro do sistema Pode clicar nesse ícone para abrir a janela da análise e ver o seu progresso.

Quando a análise estiver concluída, é apresentada a janela dos resultados da análise para o informar se pode aceder em segurança aos ficheiros nos dispositivos removíveis.

Na maioria dos casos, o Bitdefender remove automaticamente as ameaças detetadas ou isola os ficheiros infetados na quarentena. Se houver ameaças não resolvidas depois da análise, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas.

Nota

Leve em consideração que não pode ser tomada qualquer acção em ficheiros infectados ou suspeitos detectados em CDs/DVDs. Da mesma forma, não pode ser tomada qualquer acção em ficheiros infectados ou suspeitos detectados em drives de rede mapeadas, caso não tenha os privilégios adequados.

Esta informação pode ser útil para si:

- Tenha cuidado ao utilizar um CD/DVD infetado com ameaças porque as ameaças não podem ser removidas do disco (é apenas de leitura). Certifique-se que a proteção em tempo real está ativada para evitar que as ameaças se propaguem no seu sistema. É recomendado copiar quaisquer dados valiosos do disco no seu sistema e depois descartar o disco.
- Em alguns casos, o Bitdefender poderá não conseguir remover as ameaças de ficheiros específicos devido a restrições legais ou técnicas. Exemplo disso são os ficheiros guardados usando uma tecnologia proprietária (isto acontece porque o ficheiro não pode ser correctamente recriado).

  Para saber mais sobre como lidar com ameaças, consulte "*Remover ameaças do seu sistema*" (p. 186).

Gerir análise de média removível

Para gerir a verificação automática de dispositivos multimédia amovíveis:

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

2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Selecione a janela **Definições**.

As opções de análise estão pré-configuradas para obter os melhores resultados de deteção. Se forem detctados ficheiros infetados, o Bitdefender tentará desinfetá-los (remover o código malicioso) ou movê-los para a quarentena. Se ambas as acções falharem, o assistente da Análise Antivírus permite especificar outras acções a serem tomadas com ficheiros infectados. As opções de análise são padronizadas e não as pode alterar.

Para uma melhor proteção, recomenda-se que deixe a opção **Análise automática** selecionada para todos os tipos de dispositivos de armazenamento removíveis.

4.1.4. Analisar ficheiro hosts

Os ficheiros anfitrião são fornecidos por predefinição com a instalação do seu sistema operativo e são utilizados para mapear os nomes de anfitrião nos endereços IP sempre que acede a uma nova página Web, ligue um FTP ou outros servidores de Internet. É um ficheiro de texto simples e os programas maliciosos podem modificá-lo. Os utilizadores avançados sabem como utilizá-lo para bloquear anúncios incómodos, separadores, cookies de terceiros ou hijackers.

Para configurar o ficheiro anfitrião de verificação:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. Selecione o separador **Avançado**.
3. Ligue ou desligue a **Análise do ficheiro do host**.

4.1.5. A configurar exceções de análise

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

Pode configurar excepções para que sejam realizadas análises somente após acesso ou por demanda ou até mesmo ambas. Os objetos excetuados

da análise após acesso não serão analisados, mesmo se forem acedidos por si ou por uma aplicação.

Nota

As exceções NÃO serão aplicadas à análise contextual. Análise Contextual é um tipo de análise a-pedido: você clica com o botão direito de rato sobre o ficheiro ou pasta que quer analisar e seleciona **Analisar com Bitdefender**.

Excluindo ficheiros e pastas da análise

Para excluir ficheiros e pastas específicas da análise:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Definições**, clique em **Gerir exceções**.
4. Clique em **+Adicionar uma Exceção**.
5. Introduza no campo correspondente o caminho da pasta que pretende adicionar à lista de exceção da análise.

   Como alternativa, pode navegar até a pasta ao clicar no botão navegar no lado direito da interface, selecioná-la e clicar em **OK**.
6. Ligue o interruptor junto à funcionalidade de proteção que não deve analisar a pasta. Há três opções:
   - Antivírus
   - Prevenção de Ameaças Online
   - Advanced Threat Defense
7. Clique em **Guardar** para guardar as alterações e fechar a janela.

Excluir extensões de ficheiros da análise

Quando exclui uma extensão de ficheiro da análise, o Bitdefender deixará de analisar ficheiros com essa extensão, independentemente da sua localização no seu dispositivo. A exceção também se aplica a ficheiros em meios removíveis, tais como CDs, DVDs, dispositivos de armazenamento USB ou unidades de rede.

Importante
Tenha cuidado ao excluir as extensões da análise, porque essas exceções podem deixar o seu dispositivo vulnerável a ameaças.

Para excluir extensões de ficheiros da análise:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Definições**, clique em **Gerir exceções**.
4. Clique em **+Adicionar uma Exceção**.
5. Escreva as extensões que deseja excluir da análise com um ponto antes e separando-as por ponto e vírgula (;).

   txt;avi;jpg
6. Ligue o interruptor junto à funcionalidade de proteção que não deve analisar a extensão.
7. Clique em **Guardar**.

Ativar exceções de análise

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

Para gerir exceções da análise:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Na janela **Definições**, clique em **Gerir exceções**. Uma lista com todas as suas exceções será exibida.
4. Para remover ou editar exceções da análise, clique num dos botões disponíveis. Proceder da seguinte forma:

   - Para remover uma entrada da lista, clique no botão ao lado dela.
   - Para editar uma entrada da tabela, clique no botão **Editar** ao lado dela. Uma nova janela aparece onde pode alterar a extensão ou o caminho a ser excluído e a funcionalidade de segurança do qual deseja que eles sejam excluídos, conforme necessário. Faça as alterações necessárias e, em seguida, clique em **MODIFICAR**.

4.1.6. Gerir ficheiros da quarentena

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

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

Além disso, o Bitdefender analisa os ficheiros em quarentena sempre que a base de dados de informações de ameaças é atualizada. Os ficheiros limpos são automaticamente repostos no seu local de origem.

Para verificar e gerir os ficheiros em quarentena:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTIVÍRUS**, clique em **Abrir**.
3. Vá para a janela **Definições**.

   Aqui pode ver o nome dos ficheiros em quarentena, a sua localização original e o nome das ameaças detetadas.
4. Os ficheiros da quarentena são geridos automaticamente pelo Bitdefender de acordo com as predefinições da quarentena.

   Embora não seja recomendado, pode ajustar as definições de quarentena de acordo com as suas preferências clicando em **Ver Definições**.

   Clique nos botões para ligar ou desligar:

   Verifique novamente a quarentena depois de atualizações às informações sobre ameaças
   Mantenha esta opção ligada para analisar automaticamente os ficheiros da quarentena após cada atualização da base de dados das informações de ameaças. Os ficheiros limpos são automaticamente repostos no seu local de origem.

   Apagar conteúdo com mais de 30 dias
   Os ficheiros em quarentena com mais de 30 dias são eliminados automaticamente.

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

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

4.2. Advanced Threat Defense

Bitdefender Advanced Threat Defense é uma tecnologia de deteção proativa inovadora que utiliza métodos heurísticos avançados para detetar ransomware e outras novas ameaças potenciais em tempo real.

Advanced Threat Defense monitoriza continuamente as aplicações executadas no dispositivo, procurando ações tipo ameaças. Cada uma destas acções é classificada e é calculada uma pontuação geral para cada processo.

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

Ativar ou desativar o Advanced Threat Defense

Para ativar ou desativar o Advanced Threat Defense:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ADVANCED THREAT DEFENSE**, clique em **Abrir**.
3. Vá para a janela **Definições** e clique no botão ao lado de **Defesa contra Ameaças Avançadas da Bitdefender**.

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

A verificar ataques maliciosos detectados

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

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ADVANCED THREAT DEFENSE**, clique em **Abrir**.
3. Vá para a janela **Defesa contra Ameaças**.

   São apresentados os ataques detetados nos últimos 90 dias. Para obter informações sobre o tipo de um ransomware detetado, o caminho do processo malicioso ou se a desinfeção foi bem-sucedida, basta clicar neste.

A adicionar processos a exceções

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

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

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ADVANCED THREAT DEFENSE**, clique em **Abrir**.
3. Na janela **Definições**, clique em **Gerir exceções**.
4. Clique em **+Adicionar uma Exceção**.
5. Introduza no campo correspondente o caminho da pasta que pretende adicionar à lista de exceção da análise.

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

Deteção de exploits

Uma forma utilizada pelos hackers para invadir sistemas é aproveitarem-se de certos bugs ou vulnerabilidades no software (aplicações e plug-ins) e hardware dos computadores. O Bitdefender utiliza a mais moderna tecnologia antiexploit para evitar que o seu dispositivo seja vítima de um desses ataques, que se costumam espalhar muito rapidamente.

Ativar ou desativar a deteção de exploits

Para ativar ou desativar a deteção de exploits:

- Clique em **Definições** no menu de navegação na interface do Bitdefender.
- No painel **ADVANCED THREAT DEFENSE**, clique em **Abrir**.
- Vá para a janela **Definições** e clique no interruptor ao lado de **Explorar deteção** para ligar ou desligar a funcionalidade.

Nota
A opção de Deteção de exploits está ativa por predefinição.

4.3. Prevenção de Ameaças Online

A Prevenção contra ameaças online do Bitdefender garante uma navegação segura ao alertá-lo sobre páginas 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 **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **PREVENÇÃO CONTRA AMEAÇAS ONLINE**, clique em **Definições**.

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

- A prevenção contra ataques da web bloqueia ameaças provenientes da internet, incluindo downloads não autorizados.
- Consultor de pesquisa, um componente que qualifica os resultados do seu motor de pesquisa e dos links colocados nos websites das redes sociais ao colocar um icone ao lado de cada resultado:

  Não deveria visitar esta página web.

Esta página web pode conter conteúdo perigoso. Tenha cuidado se decidir 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 das redes sociais:

- Facebook
- 123

- Encrypted web scan.

  Ataques mais sofisticados podem usar tráfego da web seguro para enganar as suas vítimas. Logo, recomendamos que mantenha ativa a opção Análise da web encriptada.

- Proteção antifraude.

- Proteção Phishing.

Role para baixo e chegará à seção **Prevenção de ameaças em rede**. Aqui tem a opção **Prevenção de ameaças em rede**. Para manter o seu dispositivo longe de ataques feitos por malware complexos (como ransomware) através da exploração de vulnerabilidades, mantenha a opção ativada.

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

Para configurar e gerir sites, domínios e endereços de IP utilizando a Prevenção Contra Ameaças Online fornecida pelo Bitdefender:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **PREVENÇÃO CONTRA AMEAÇAS ONLINE**, clique em **Definições**.
3. Clique em **Gerir exceções**.
4. Clique em **+Adicionar uma Exceção**.

5. No campo correspondente, escreva o nome do site, do domínio ou do endereço IP que deseja adicionar às excepções.
6. Clique no botão ao lado de **Prevenção de Ameaças Online**.
7. Para remover uma entrada da lista, clique no botão ao lado dela.

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

Alertas de Bitdefender no navegador

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

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

Tem de decidir o que fazer a seguir. Estão disponíveis as seguintes opções:

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

4.4. Antispam

Spam é o termo utilizado para descrever mensagens eletrónicas não solicitadas. O Spam é um problema crescente, tanto para indíviduos como para organizações. Não é bonito, não desejaria que os seus filhos o vissem, pode fazer com que seja despedido (por desperdiçar muito tempo, ou por receber pornografia no seu mail de trabalho) e não pode impedir que as pessoas o enviem. O melhor a fazer para impedir isso, é, obviamente, parar de o receber. Infelizmente, o Spam vem em muitos formatos e feitios, e é muito abundante.

O Bitdefender Antispam emprega inovações tecnológicas surpreendentes e um conjunto de filtros de antispam standard para limpar o spam antes de o mesmo chegar à caixa de correio A receber do utilizador. Para mais informação, dirija-se a "*Compreender o Antispam*" (p. 96).

A proteção de Antispam do Bitdefender está disponível apenas para clientes de correio eletrónico configurado para receber mensagens de e-mail via protocolo POP3. POP3 é um dos protocolos mais utilizados para fazer o download de mensagens de e-mail a partir de um servidor de correio.

Nota
O Bitdefender não proporciona proteção antispam para contas de correio eletrónico a que acede através de sites Internet (webmail).

As mensagens não solicitadas detetadas pelo Bitdefender são marcadas com o prefixo [SPAM] no campo do assunto. O Bitdefender move automaticamente as mensagens de spam para uma determinada pasta, da seguinte forma:

- No Microsoft Outlook, as mensagens de spam são movidas para a pasta **Spam**, localizada na pasta **Itens Eliminados**. A pasta **Spam** fé criada quando um e-mail é indicado como spam.
- No Mozilla Thunderbird, as mensagens de spam são movidas para a pasta **Spam**, localizada na pasta **Lixo**. A pasta **Spam** fé criada quando um e-mail é indicado como spam.

Se usa outros cliente de e-mail, tem de criar uma regra para mover os e-mails marcados como [spam] pelo Bitdefender para uma pasta de quarentena personalizada. Se os itens Eliminar ou as pastas Lixo forem eliminados, a pasta Spam também é eliminada. Contudo, é criada uma nova pasta Spam assim que um e-mail for indicado como spam.

4.4.1. Compreender o Antispam

Filtros impeditivos da entrada de mails indesejados

O Motor Antispam do Bitdefender inclui proteção na nuvem e outros filtros diferenciados que garantem que a sua Caixa de Entrada fique livre de SPAM, como a Lista de Amigos, Lista de Spammers e Filtro de Carateres.

Lista de Amigos / Lista de Spammers

A maioria das pessoas comunica regularmente com um grupo de pessoas, ou até mesmo recebe mensagens de empresas ou organizações no mesmo domínio. Ao utilizar as **listas de amigos ou spammers**, pode facilmente decidir de quem pretende receber e-mails (amigos) independentemente do conteúdo das mensagens, ou de quem nem sequer pretende ouvir falar novamente (spammers).

Nota
Recomendamos que adicone os nomes e endereços de e-mail dos seus amigos à **Lista de Amigos**. O Bitdefendernão bloqueia mensagens das pessoas dessa

lista; logo, adicionar amigos ajuda a que as mensagens legítimas cheguem a si.

Filtro caracteres

Muitas mensagens de spam estão escritas em Cirílico e/ou caracteres Asiáticos. O filtro de Caracteres detecta este tipo de mensagens e marca-os como SPAM.

Operação Antispam

O Motor Bitdefender Antispam usa todos os filtros antispam combinados para determinar se um determinado e-mail deve de chegar à pasta **A Receber** ou não.

Todo o e-mail proveniente da Internet é inicialmente verificado pelo filtro da Lista Amigos / Lista Spammers. Se o endereço do remetente se encontrar na Lista Amigos, o e-mail é movido directamente para a sua **Caixa de Entrada**.

Caso contrário, o filtro da Lista de Spammers irá apoderar-se do seu correio electrónico para verificar se o endereço do remetente se encontra na lista. Se for encontrada uma correspondência, a mensagem será marcada como SPAM e movida para a pasta de **Spam**.

Ainda, o Filtro caracteres irá verificar se o e-mail está escrito em caracteres Cirílicos ou Asiáticos. Se assim for, e-mail será marcado com Indesejado e movido para a pasta de **Spam**.

Nota
Se o e-mail for marcado com SEXUALLY EXPLICIT na linha do sujeito, o Bitdefender irá considerá-lo como SPAM.

Clientes de email e protocolos suportados

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

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

4.4.2. Ligar ou desligar a proteção antispam

A proteção AntiSpam está ativada por defeito.

Para ligar ou desligar a ferramenta Antispam:

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

4.4.3. Utilizar a barra de ferramentas Antispam na janela do seu cliente de email

No lado superior da janela do seu cliente de mail pode ver a barra de ferramentas do Antispam. A barra de ferramentas do Antispam ajuda-o a gerir a proteção antispam diretamente do seu cliente de e-mail. Pode facilmente corrigir o Bitdefender se ele marcar uma mensagem legítima como SPAM.

Importante

O BiDefender integra uma barra antispam de facil utilização, nos clientes de email mais comuns. Para ver a lista completa de clientes de e-mail suportados, por favor consulte o "*Clientes de email e protocolos suportados*" (p. 97).

Cada botão é explicado abaixo:

Definições - abre uma janela onde pode configurar as definições da barra de ferramentas e dos filtros antispam.
É Spam - indica que o email selecionado é spam. O email será movido imediatamente para a pasta **Spam**. Se os serviços da nuvem antispam estiverem ativados, a mensagem é enviada para a Nuvem do Bitdefender para análise mais aprofundada.
Não Spam - indica que o email selecionado não é spam e o Bitdefender não o deveria ter identificado. Este e-mail será movido da pasta **Spam** para o diretório **Caixa de Entrada**. Se os serviços da nuvem antispam estiverem ativados, a mensagem é enviada para a Nuvem do Bitdefender para análise mais aprofundada.

Importante

O botão **Não Spam** fica ativo quando selecionar uma mensagem marcada como SPAM pelo Bitdefender (normalmente estas mensagens localizam-se na pasta de **Spam**).

Adicionar Spammer - adiciona o remetente da mensagem de e-mail à lista de Spammers. Pode necessitar de clicar em **OK** para confirmar. As

mensagens de e-mail recebidas dos endereços na lista de Spammers são automaticamente marcadas como [spam].

Adicionar Amigo - adiciona o remetente da mensagem de e-mail à lista de Amigos. Pode necessitar de clicar em **OK** para confirmar. Irá sempre receber mensagens de e-mail destes endereços, independentemente do conteúdo da mensagem.

Spammers- abre a **Lista de Spammers** que contém todos os endereços de e-mail, dos quais não quer receber mensagens, independentemente do seu conteúdo. Para mais informação, dirija-se a *"Configurar a lista de Spammers"* (p. 101).

Amigos - abre a **Lista de amigos** que contém todos os endereços de e-mail dos quais deseja receber mensagens de e-mail, independentemente do seu conteúdo. Para mais informação, dirija-se a *"Configurar a Lista de Amigos"* (p. 100).

Indicar os erros de deteção

Se estiver a usar um cliente de e-mail suportado, pode facilmente corrigir o filtro antispam (indicando mensagens de correio eletrónico que não deveriam ter sido marcadas como[spam]). Se o fizer, ajuda a melhorar a eficiência do filtro antispam. Siga os seguintes passos:

1. Abra o mail de cliente.
2. Vá à pasta de lixo eletrónico, para onde são movidas as mensagens.
3. Selecione a mensagem legítima incorretamente marcada como [spam] pelo Bitdefender.
4. Clique no botão **Adicionar Amigos** da barra de tarefas antispam do Bitdefender para adicionar o remetente à lista de Amigos. Pode necessitar de clicar em **OK** para confirmar. Irá sempre receber mensagens de e-mail destes endereços, independentemente do conteúdo da mensagem.
5. Clique no botão **Não Spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de mail do cliente). A mensagem de email será movida para a pasta de Entrada.

Indicar mensagens de spam não detetadas

Se estiver a utilizar um cliente de e-mail suportado, pode facilmente indicar quais as mensagens de e-mail que devem ser detectadas como spam. Se o fizer, ajuda a melhorar a eficiência do filtro antispam. Siga os seguintes passos:

1. Abra o mail de cliente.
2. Vá à pasta Caixa de Entrada.
3. Selecione as mensagens spam não detetadas
4. Clique no botão **É Spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de email do cliente). São imediatamente marcadas como [spam] e movidas para a pasta de lixo electrónico.

Configurar definições da barra de ferramentas

Para configurar as definições da barra de ferramentas antispam do seu cliente de email, clique no botão **Definições** na barra e depois no separador **Definições da Barra de Ferramentas**.

Tem as seguintes opções:

- **Marque as mensagens de e-mail indesejadas como 'ler'** - marca as mensagens indesejadas como ler automaticamente, para que não seja perturbador quando chegarem.
- Pode optar por visualizar janelas de confirmação quando clica nos botões **Adicionar Spammer** e **Adicionar Amigo** na barra de ferramentas antispam.

  As janelas de confirmação pode evitar a adição acidental de destinatários de email à lista de Amigos / Spammers.

4.4.4. Configurar a Lista de Amigos

A **Lista de Amigos** é uma lista de todos os endereços de e-mail dos quais deseja sempre receber mensagens, independentemente do seu conteúdo. As mensagens dos seus amigos não são marcadas como spam, mesmo que o conteúdo se assemelhe a spam.

> **Nota**
> Qualquer mail proveniente de um endereço presente na **Lista de amigos**, será automaticamente entregue na sua Caixa de Entrada, sem mais demora.

Para configurar e gerir a lista de Amigos:

- Se estiver a utilizar o Microsoft Outlook ou Thunderbird, clique no botão **Amigos** na barra de ferramentas antispam do Bitdefender.
- Alternativa:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTISPAM**, clique em **Definições**.
3. Aceda à janela **Gerir amigos**.

Para adicionar um endereço de email, selecione a opção **Endereço de e-mail**, digite o endereço e depois clique em **Adicionar**. Sintaxe: nome@dominio.com.

Para adicionar os endereços de e-mail de um domínio específico, selecione a opção **Nome do domínio**, insira o nome do domínio e, em seguida, clique em **Adicionar**. Sintaxe:

- @domain.com e domain.com - todas as mensagens de e-mail recebidas de domain.com chegarão à sua **Caixa de entrada** independentemente do seu conteúdo;
- dominio - todos os mails provenientes de dominio (independentemente dos sufixos de domínio) serão marcados como INDESEJADOS;
- com - todos os mails tendo o sufixo de domínio com serão marcados como INDESEJADOS;

É recomendado que evite adicionar domínios completos, mas isto poderá ser útil em algumas situações. Por exemplo, pode adicionar o domínio do endereço eletrónico da empresa para a qual trabalha ou de parceiros de confiança.

Para eliminar um item da lista, clique no botão correspondente  ao lado. Para eliminar todas as entradas da lista, clique em **Limpar lista**.

Pode guardar a lista de Amigos num ficheiro para que mais tarde possa utilizá-lo noutro dispositivo ou quando reinstalar o produto. Para guarda a lista de Amigos, clique no botão **Guardar** e guarda no local desejado. O ficheiro terá a extensão .bwl

Para carregar uma lista de Amigos guardada anteriormente, clique em **Carregar** e abra o ficheiro .bwl correspondente. Para restabelecer o conteúdo da lista existente ao carregar uma lista previamente guardada, marque a caixa ao lado de **Sobrescrever lista atual**.

4.4.5. Configurar a lista de Spammers

A **Lista de indesejados** é uma lista de todos os endereços de e-mail, dos quais nunca pretende receber mensagens, independentemente do seu conteúdo. Todo o mail proveniente de um endereço presente na **Lista de**

indesejados, será marcado automaticamente com indesejado, sem mais demora.

Para configurar e gerir a lista de Spammers:

- Se estiver a utilizar o Microsoft Outlook ou Thunderbird, clique no botão **Spammers** na barra de ferramentas antispam do Bitdefender integrada no seu cliente de e-mail.
- Alternativa:
  1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
  2. No painel **ANTISPAM**, clique em **Definições**.
  3. Aceda à janela **Gerir Spammers**.

Para adicionar um endereço de email, selecione a opção **Endereço de e-mail**, digite o endereço e depois clique em **Adicionar**. Sintaxe: nome@dominio.com.

Para adicionar os endereços de e-mail de um domínio específico, selecione a opção **Nome do domínio**, insira o nome do domínio e, em seguida, clique em **Adicionar**. Sintaxe:

- @domain.come domain.com - todas as mensagens de e-mail recebidas de domain.com chegarão à sua **Caixa de entrada** independentemente do seu conteúdo;
- dominio - todos os mails provenientes de dominio (independentemente dos sufixos de domínio) serão marcados como INDESEJADOS;
- com - todos os mails tendo o sufixo de domínio com serão marcados como INDESEJADOS.

É recomendado que evite adicionar domínios completos, mas isto poderá ser útil em algumas situações.

Atenção

Não adicione domínios de serviços web-mail (tais como o Yahoo, Gmail, Hotmail ou outro) à lista de Spammers. Caso contrário, as mensagens de email recebidas de algum utilizador registado nesses serviços será detectado como spam. Se, por exemplo, adicionar yahoo.com à lista de Spammer, todos as mensagens de e-mais recebidas do endereço yahoo.com, serão marcadas como [spam].

Para eliminar um item da lista, clique no botão correspondente ao lado. Para eliminar todas as entradas da lista, clique em **Limpar lista**.

Pode guardar a lista de Spammers num ficheiro para que mais tarde possa utilizá-lo noutro dispositivo ou quando reinstalar o produto. Para guarda a lista de Spam, clique no botão **Guardar** e guarda no local desejado. O ficheiro terá a extensão .bwl

Para carregar uma lista de Spammers previamente guardada, clique em **CARREGAR** e abra o ficheiro .bwl correspondente. Para repor o conteúdo da lista existente ao carregar uma lista guardada anteriormente, selecione **Sobrescrever lista atual**.

4.4.6. A configurar os filtros locais Antispam

Como descrito em "*Compreender o Antispam*" (p. 96), o Bitdefender utiliza um conjunto de diferentes filtros antispam para identificar o spam. Os filtros antispam são pré-configurados para uma proteção eficaz.

Importante

Dependendo se recebe ou não mensagens eletrónicas fiáveis ou não escrita com caracteres asiáticos ou cirílicos, desative ou ative a definição que bloqueia automaticamente estas mensagens. A respetiva definição está desativada nas versões localizadas do programa que utilizam conjuntos de caracteres (por exemplo, na versão russa ou chinesa).

Para configurar os filtros locais antispam:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTISPAM**, clique em **Definições**.
3. Vá para a janela **Definições** e clique nos interruptores ligar/desligar correspondentes.

Se estiver a usar Microsoft Outlook ou Thunderbird, pode configurar os filtros locais antispam diretamente a partir do seu cliente de e-mail. Clique no botão **Definições** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela do cliente de e-mail) e depois no separador **Filtros Antispam**.

4.4.7. Configurar as definições da nuvem

A deteção na nuvem utiliza os Serviços na Nuvem do Bitdefender para lhe proporcionar uma proteção antispam eficaz e sempre atualizada.

As funções de proteção na nuvem enquanto mantiver o AntiSpam do Bitdefender ativado.

As amostras de emails legítimos ou spam podem ser enviados para a Nuvem Bitdefender quando indica erros de detecção ou emails de spam não detectados. Isto ajuda a melhorar a detecção antispam do Bitdefender.

Configurar o envio de amostra por e-mail para a Nuvem Bitdefender através da seleção das opções pretendidas seguindo estes passos:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTISPAM**, clique em **Definições**.
3. Vá para a janela **Definições** e clique nos interruptores ligar/desligar correspondentes.

Se estiver a utilizar Microsoft Outlook ou Thunderbird, pode configurar a deteção na nuvem diretamente a partir do seu cliente de e-mail. Clique no botão ⚙ **Definições** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela do cliente de e-mail) e depois no separador **Definições de Nuvem**.

4.5. Firewall

A Firewall protege o seu dispositivo de tentativas de ligação de saída e entrada não-autorizadas, quer em redes locais quer na Internet. É bastante semelhante a um guarda no seu seu portão - regista as tentativas de ligação e decide quais deve permitir e quais bloquear.

A firewall do Bitdefender usa um conjunto de regras para filtrar dados transmitidos para ou a partir do seu sistema.

Em condições normais, o Bitdefender cria automaticamente uma regra sempre que uma aplicação tenta aceder à Internet. Também pode adicionar ou editar manualmente regras das aplicações.

Como medida de segurança, será notificado sempre que uma aplicação potencialmente maliciosa tiver o acesso à Internet bloqueado.

OBitdefender atribui automaticamente um tipo de rede a cada ligação de rede que deteta. Dependendo do tipo de rede, a proteção firewall é definida para o nível apropriado para cada ligação.

Para saber mais sobre as definições da firewall para cada tipo de rede e como pode editar as definições de rede, por favor consulte "*Gerir definições da ligação*" (p. 108).

Ativar/desativar firewall de proteção

Para ativar ou desativar a proteção por firewall:

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

Atenção

Porque expõe o seu dispositivo a ligações não autorizadas, desligar a firewall deveria ser uma medida temporária. Volte a ligar a firewall assim que possível.

4.5.1. Gerir regras de aplicações

Para visualizar e gerir as regras da firewall de controlo do acesso a aplicações a recursos da rede e à Internet:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel do **FIREWALL**, clique em **Definições**.
3. Vá para a janela **Acesso à aplicação**.

Pode ver os últimos programas (processos) que passaram pela Firewall do Bitdefender e a rede de Internet à qual está ligado. Para ver as regras criadas para uma aplicação específica, basta clicar nela e clicar na hiperligação **Ver regras da aplicação**. A janela **Regras** abre.

Para cada regra é apresentada a seguinte informação:

- **REDE** - o processo e os tipos de adaptador de rede (doméstico/escritório, público ou todos) aos quais a rede se aplica. As regras são automaticamente criadas para filtrar o acesso à rede ou à Internet através de qualquer adaptador. Por defeito, as regras aplicam-se a qualquer rede. Pode criar manualmente as regras ou editar as regras existentes para filtrar o acesso à rede ou à Internet de uma aplicação através de um determinado adaptador (por exemplo, um adaptador de rede wireless).
- **PROTOCOLO** - o protocolo IP ao qual a regra se aplica. Por defeito, as regras aplicam-se a qualquer protocolo.
- **TRÁFEGO** - a regra aplica-se em ambas as direções, entrada e saída.

- **PORTAS** - o protocolo PORTA ao qual a regra se aplica. Por predefinição, as regras aplicam-se a todas as portas.
- **IP** - o protocolo Internet (IP) ao qual a regra se aplica. Por predefinição, as regras aplicam-se a qualquer endereço IP.
- **ACESSO** - se a aplicação permite ou recusa acesso à rede ou Internet em circunstâncias específicas.

Para editar ou eliminar as regras da aplicação selecionada, clique no ícone ⋯.

- **Editar regra** - abre uma janela onde é possível editar a regra atual.
- **Eliminar regra** - é possível optar por remover o conjunto de regras atual para a aplicação selecionada.

A adicionar regras de aplicações

Para adicionar uma regra de aplicação:

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

Aqui pode aplicar as seguintes mudanças:

- **Aplicar esta regra a todas as aplicações.** Ative esta opção para aplicar a regra criada a todas as aplicações.
- **Caminho do Programa.** Clique em **EXPLORAR** para selecionar a aplicação à qual a regra se aplica.
- **Permissão.** Selecione uma das seguintes permissões disponíveis:

Permissão	Descrição
Permitir	À aplicação especificada será permitido o acesso à rede / Internet nas circunstâncias determinadas.
Bloquear	À aplicação especificada será negado o acesso à rede / Internet nas circunstâncias determinadas.

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

Tipo de rede	Descrição
Qualquer Rede	Permite todo o tráfego entre o seu dispositivo e outros dispositivos independentemente do tipo de rede.
Casa/Escritório	Permitir todo o tráfego entre o seu dispositivo e outros diferentes na rede local.
Público	Todo o tráfego é filtrado.

- **Protocolo.** Selecione do menu o protocolo IP ao qual a regra se aplica.
  - Se deseja que a regra se aplique a todos os protocolos, selecione **Todos**.
  - Se deseja que a regra se aplique ao TCP, selecione **TCP**.
  - Se deseja que a regra se aplique ao UDP, selecione **UDP**.
  - Se pretender que a regra se aplique a ICMP, selecione **ICMP**.
  - Se pretender que a regra se aplique a IGMP, selecione **IGMP**.
  - Se deseja que a regra se aplique ao GRE, selecione **GRE**.
  - Se quiser que a regra se aplique num protocolo específico, introduza o número atribuído ao protocolo que quiser filtrar no campo de edição em branco.

> **Nota**
>
> Os números dos protocolos IP são atribuídos pelo Internet Assigned Numbers Authority (IANA). Pode encontrar a lista completa de números IP atribuidos em http://www.iana.org/assignments/protocol-numbers.

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

Direção	Descrição
Saída	A regra aplica-se apenas ao tráfego de saída.
Entrada	A regra aplica-se apenas ao tráfego de entrada.
Ambos	A regra aplica-se em ambos os sentidos.

Clique no botão **Definições avançadas** na parte inferior da janela para personalizar as seguintes definições:

- **Endereço Local Customizado.** Especifique o endereço IP local e a porta aos quais a regra se aplica.
- **Endereço remoto personalizado.** Especifique o endereço IP remoto e a porta aos quais a regra se aplica.

Para remover o conjunto de regras atual e restaurar as predefinições, clique na hiperligação **Repor regras** na janela **Regras**.

4.5.2. Gerir definições da ligação

Independentemente de se ligar à Internet por Wi-Fi ou adaptador Ethernet, pode configurar as definições que devem ser aplicadas para uma navegação segura. As opções disponíveis são:

- **Dinâmica** – o tipo de rede será definido automaticamente com base no perfil da rede ligada, doméstica/escritório ou pública. Quando isto acontece, só serão aplicadas as regras de firewall do tipo de rede específica ou as definidas para se aplicarem a todos so tipos de rede.
- **Doméstica/escritório** – o tipo de rede será sempre doméstica/escritório, independentemente do perfil da rede ligada. Quando isto acontece, só serão aplicadas as regras de firewall para doméstica/escritório ou as definidas para se aplicarem a todos so tipos de rede.
- **Pública** – o tipo de rede será sempre pública, independentemente do perfil da rede ligada. Quando isto acontece, só serão aplicadas as regras de firewall para pública ou as definidas para se aplicarem a todos so tipos de rede.

Para configurar os adaptadores de rede:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel do **FIREWALL**, clique em **Definições**.
3. Selecione a janela **Adaptadores de rede**.
4. Selecione as definições que pretende aplicar ao estabelecer ligação com os seguintes adaptadores:
   - Wi-Fi
   - Ethernet

4.5.3. Configurar definições avançadas

Para definições avançadas da firewall:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel do **FIREWALL**, clique em **Definições**.
3. Selecione a janela **Definições**.

É possível configurar as seguintes funcionalidades:

- **Proteção de verificação de porta** - detecta e bloqueia tentativas de descobrir quais portas estão abertas.

  Os scans de portas são frequentemente utilizados pelos hackers para descobrir que portas se encontram abertas no seu dispositivo. Então eles poderão entrar no seu dispositivo se descobrirem uma porta menos segura ou vulnerável.

- **Modo Paranoico** - são apresentados alertas sempre que uma aplicação tenta estabelecer ligação com a Internet. Selecione **Permitir** ou **Bloquear**. Quando o Modo de Alerta está ativo, a função de Perfis é desligada automaticamente. O Modo Paranoico pode ser utilizado em simultâneo com o **Modo de Bateria**.

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

- **Modo Invisível** - para não ser detetado por outros dispositivos. Clique em **Editar definições sigilosas** para escolher quando o seu dispositivo deve ou não ficar visível para outros dispositivos.

- **Comportamento predefinido da aplicação** - permite que o Bitdefender aplique definições automáticas às aplicações sem regras definidas. Clique em **Editar regras predefinidas** para escolher se as definições automáticas devem ser aplicadas ou não.

  - Automático - o acesso a aplicações será permitido ou recusado com base nas regras automáticas de firewall e utilizadores.
  - Permitir - as aplicações que não têm qualquer regra de firewall definidas serão permitidas automaticamente.
  - Bloquear - as aplicações que não têm qualquer regra de firewall definidas serão bloqueadas automaticamente.

4.6. Vulnerabilidade

Um passo importante na proteção do seu dispositivo contra as ações e aplicações maliciosas é manter atualizado o seu sistema operativo e as aplicações que utiliza regularmente. Além disso, para evitar o acesso físico não autorizado ao seu dispositivo, palavras-passe fortes (palavras-passe que não são facilmente descobertas) devem ser configuradas para cada conta de utilizador do Windows e também para as redes Wi-Fi às quais se liga.

O Bitdefender proporcionar duas formas fáceis de resolver as vulnerabilidades do seu sistema:

- Pode analisar o seu sistema por vulnerabilidades e repará-las passo a passo com a opção **Análise de Vulnerabilidades**.
- Utilizando a monitorização automática de vulnerabilidades, pode verificar e reparar as vulnerabilidades detetadas na janela Notificações.

Deve verificar e resolver as vulnerabilidades do sistema semanal ou quinzenalmente.

4.6.1. Procurar vulnerabilidades no seu sistema

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

Para analisar o seu sistema em busca de vulnerabilidades:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **VULNERABILIDADE**, clique em **Abrir**.
3. No separador **Verificação de vulnerabilidades** clique em **Iniciar análise** e, em seguida, aguarde até que o Bitdefender verifique seu sistema em busca de vulnerabilidades. As vulnerabilidades detetadas são agrupadas nas três categorias:
   - **SISTEMA OPERATIVO**
     - **Segurança de sistemas operativos**

       Definições de sistema alteradas que podem comprometer o seu dispositivo e dados, como não exibir avisos quando ficheiros executados realizam alterações no seu sistema sem a sua permissão ou quando dispositivos MTP como telefones ou câmaras se conectam e executam operações diferentes sem o 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 a Bitdefender finalizar a instalação. As atualizações podem demorar a serem instaladas.

- **Contas do Windows fracas**

  Pode ver a lista dos utilizadores de contas Windows configurados no seu dispositivo e o nível de proteção que as suas palavras-passe garantem. Pode escolher entre pedir ao utilizador para alterar a palavra-passe da próxima vez que iniciar sessão ou o próprio alterar a palavra-passe imediatamente. Para definir uma nova palavra-passe para o seu sistema, selecione **Definir a palavra-passe agora**.

  Para criar uma palavra-passe segura, recomendamos a utilização de uma combinação de maiúsculas e minúsculas, números e caracteres especiais (como #, $ ou @).

- **APLICAÇÕES**
  - **Segurança do Navegador**

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

  - **Atualização de aplicações**

    Para visualizar informação sobre a aplicação que precisa de ser atualizada, clique no nome dela na lista.

    Caso uma aplicação não esteja atualizada, clique na ligação **Transferir nova versão** para transferir a última versão.

- **REDE**
  - **Rede e credenciais**

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

  - **Routers e redes Wi-Fi**

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

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

4.6.2. Usar monitorização de vulnerabilidade automática

O Bitdefender verifica o seu sistema quanto a vulnerabilidades regularmente, em segundo plano, e mantém os registos de problemas detetados na janela Notificações.

Para verificar e reparar os problemas detetados:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Todas**, selecione a notificação referente à verificação de vulnerabilidades.
3. Pode ver a informação detalhada sobre as vulnerabilidades do sistema detetadas. Dependendo da incidencia, para reparar uma vulnerabilidade específica proceda da seguinte forma:
   - Se estiverem disponíveis atualizações para o Windows, clique em **Instalar**.
   - Se as atualizações automáticas do Windows estiverem desativadas, clique em **Ativar**.
   - Se uma aplicação estiver desatualizada, clique em **Atualizar agora** para obter a hiperligação para a página de Internet do fornecedor a partir da qual pode instalar a versão mais recente dessa aplicação.
   - Se uma conta de utilizador do Windows tiver uma palavra-passe fraca, clique em **Alterar palavra-passe** para obrigar o utilizador a mudar a palavra-passe no próximo início de sessão ou alterá-la por si mesmo. Para obter uma palavra-passe forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).
   - Se a funcionalidade de Execução Automática do Windows estiver ativada, clique em **Reparar** para a desativar.

- Se o router que tem configurado tiver uma palavra-passe fraca, clique em **Alterar palavra-passe** para aceder à sua interface a partir da qual é possível definir uma palavra-passe forte.
- Se a rede à qual está ligado apresentar vulnerabilidades que possam expor o seu sistema a riscos, clique em **Alterar definições de WI-FI**.

Para configurar as definições de monitorização de vulnerabilidades:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **VULNERABILIDADE**, clique em **Abrir**.

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

3. Vá para o separador **Definições**.
4. Escolha as vulnerabilidades do sistema que deseja que sejam regularmente verificadas usando os botões correspondentes.

Windows updates
Verifique se o seu sistema operativo Windows possui as mais recentes e importantes atualizações de segurança da Microsoft.

Atualização de aplicações
Verifique se as aplicações instaladas no seu sistema estão atualizadas. As aplicações desatualizadas podem ser exploradas por software malicioso, tornando o PC vulnerável a ataques externos.

Palavras-passe do utilizador
Verifique se as palavras-passe dos routers e contas Windows configuradas no sistema são fáceis de descobrir ou não. A definição de palavras-passe difíceis de descobrir (palavras-passe fortes) torna muito difícil a invasão do seu sistema pelos hackers. Uma palavra-passe forte inclui maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).

Autorreprodução
Verifique o estado do recurso Windows Autorun. Esta característica permite que as aplicações se iniciem automaticamente a partir dos CDs, DVDs, drives USB ou outros dispositivos externos.

Alguns tipos de ameaças utilizam Autorun para se propagar automaticamente dos suportes multimédia removíveis do PC. Por isso, recomenda-se a desactivação desta janela.

Consultor de Segurança Wi-Fi

Verifique se a rede doméstica sem fios à qual está ligado é segura ou não e se tem vulnerabilidades. Além disso, verifique se a palavra-passe do seu router doméstico é suficientemente e se pode torná-la mais segura.

A maioria das redes não protegidas não são seguras, permitindo o fácil acesso de hackers às suas atividades privadas.

Nota

Se desativar a monitorização de uma vulnerabilidade específica, os problemas relacionados não serão mais registados na janela de notificações.

4.6.3. Consultor de Segurança Wi-Fi

Enquanto caminha, trabalha num café ou aguarda no aeroporto, ligar-se a uma rede pública sem fios para realizar pagamentos, verificar e-mails ou aceder às contas de redes sociais pode ser a solução mais rápida. Enquanto isso, pessoas curiosas tentam roubar os seus dados pessoais vendo como as informações fluem ao longo da rede.

Dados pessoais consistem em palavras-passe e nomes de utilizadores que utilizar para aceder às suas contas online, tais como e-mails, contas bancárias, contas de redes sociais, mas também mensagens enviadas por si.

Geralmente, as redes públicas sem fios tendem a ser menos seguras uma vez que não necessitam de qualquer palavra-passe para efetuar a ligação ou, caso seja necessária uma palavra-passe, esta é disponibilizada a qualquer pessoa que pretenda ligar-se. Além disso, podem ser redes maliciosas ou "honeypot", que representam um alvo para criminosos informáticos.

Para protegê-lo contra os perigos dos hotspots de ligação sem fios públicos não seguros ou não encriptados, o Consultor de Segurança do Wi-Fi do Bitdefender analisa a segurança de uma rede sem fios e, quando necessário, recomenda que use o Bitdefender VPN.

O Consultor de Segurança Wi-Fi do Bitdefender fornece informações sobre:

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

Ativar ou desativar as notificações do Consultor de Segurança Wi-Fi

Para ativar ou desativar as notificações do Consultor de Segurança Wi-Fi:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **VULNERABILIDADE**, clique em **Abrir**.
3. Vá para a janela **Definições** e ative ou desative a opção **Consultor de Segurança do Wi-Fi**.

Configurar a rede Wi-Fi doméstica

Para começar a configurar a sua rede doméstica:

1. Clique em **Definições** no menu de navegação na 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. No separador **Rede Wi-Fi doméstica**, clique em **SELECIONAR REDE WI-FI DOMÉSTICA**.

   Uma lista com redes sem fios às quais já esteve ligado é agora exibida.
5. Indique a sua rede doméstica e, em seguida, clique em **SELECIONAR**.

Se uma rede doméstica for considerada insegura ou desprotegida, são exibidas as recomendações de configuração para aumentar a sua segurança.

Para remover a rede sem fios definida como rede doméstica, clique no botão **REMOVER**.

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

Configurar a rede Wi-Fi do trabalho

Para começar a configurar sua rede de escritório:

1. Clique em **Definições** no menu de navegação na 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 escritório**.
4. No separador **Wi-Fi do escritório**, clique em **SELECIONAR WI-FI DO ESCRITÓRIO**.

   Uma lista com redes sem fios às quais já esteve ligado é agora exibida.
5. Aponte para a sua rede de escritório e, em seguida, clique em **SELECIONAR**.

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

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

Para remover a rede sem fios que definiu como rede de escritório, clique no botão **Selecionar nova rede WI-FI do escritório**.

Wi-Fi público

Enquanto está ligado a uma rede sem fios insegura ou desprotegida, o perfil de Wi-Fi pública é ativado. Ao executar neste perfil, o Bitdefender Total Security é definido automaticamente de modo a obter as seguintes definições de programa:

- Advanced Threat Defense ativado
- A Firewall do Bitdefender é ativada e as definições seguintes são aplicadas ao seu adaptador sem fios:
  - Modo Stealth - : LIGADO
  - Tipo de rede - Pública
- As seguintes definições da Prevenção contra ameaças online são ativadas:
  - Encrypted web scan
  - Proteção contra fraudes
  - Proteção contra phishing
- Está disponível um botão que abre o Bitdefender Safepay™. Neste caso, a proteção Hotspot para redes desprotegidas está ativada por predefinição.

Verificar informações sobre redes Wi-Fi

Para verificar as informações sobre as redes sem fios a que é habitual ligar-se:

1. Clique em **Definições** no menu de navegação na 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 precisar, selecione um dos três separadores, **Wi-Fi doméstica**, **Wi-Fi de escritório** ou **Wi-Fi pública**.
5. Clique em **Visualizar detalhes** junto à rede sobre a qual pretende obter mais informações.

Existem três tipos de redes sem fios filtrados por importância, sendo cada tipo indicado com um ícone específico:

Wi-Fi desprotegida - indica que o nível de segurança da rede é reduzido. Isto significa que existe um risco elevado de utilização e não é recomendado realizar pagamentos ou verificar contas bancárias sem uma proteção adicional. Nestas situações, recomendamos a utilização do Bitdefender Safepay™ com a proteção Hotspot para redes desprotegidas ativada.

Wi-Fi desprotegida - indica que o nível de segurança da rede é moderado. Isto significa que podem existir vulnerabilidades e não é recomendado realizar pagamentos ou verificar contas bancárias sem uma proteção adicional. Nestas situações, recomendamos a utilização do Bitdefender Safepay™ com a proteção Hotspot para redes desprotegidas ativada.

Wi-Fi é segura - indica que a rede utilizada é segura. Neste caso, pode utilizados dados confidenciais para realizar operações online.

Ao clicar na ligação **Ver detalhes** na área de cada rede, são apresentados os seguintes detalhes:

- **Segura** - onde pode ver se a rede selecionada está segura ou não. As redes não encriptadas podem deixar os seus dados expostos.
- **Tipo de encriptação** - aqui pode visualizar o tipo de encriptação utilizado pela rede selecionada. Alguns tipos de encriptação podem não ser seguros. Assim, recomendamos vivamente verificar as informações sobre o tipo de encriptação exibido para garantir que está protegido ao navegar na Web.

- **Canal/Frequência** - aqui pode visualizar a frequência do canal utilizada pela rede selecionada.
- **Força da palavra-passe** - aqui pode visualizar a força da palavra-passe. Observe que as redes que têm palavras-passe fracas definidas representam um alvo para os cibernautas criminosos.
- **Tipo de início de sessão** - aqui pode visualizar se a rede selecionada está ou não protegida com uma palavra-passe. É altamente recomendado ligar-se apenas a redes que possuem palavras-passe fortes definidas.
- **Tipo de autenticação** - aqui pode visualizar o tipo de autenticação utilizado pela rede selecionada.

4.7. Proteção de Vídeo e Áudio

Cada vez há mais ameaças desenhadas para aceder a câmaras web e microfones integrados. Para evitar o acesso não autorizado à sua câmara web e para o(a) manter informado(a) sobre que aplicações não confiáveis acederam o seu microfone e quando, o Bitdefender Vídeo & Áudio inclui:

- Proteção da Webcam
- Supervisor do microfone

4.7.1. Proteção da Webcam

O facto de que os hackers podem controlar a sua câmara Web para o espiar já não é uma novidade e as soluções para o proteger, tal como revogar privilégios de aplicações, desativar a câmara integrada do dispositivo ou tapá-la, não são muito práticas. Para evitar futuras tentativas de acesso à sua privacidade, a Proteção da Câmara Web do Bitdefender monitoriza permanentemente as aplicações que tentam aceder à câmara e bloqueiam as que não estão listadas como fidedignas.

Como uma medida de segurança, será notificado sempre que uma aplicação não fiável tentar ganhar acesso à sua câmara.

Ativar ou desativar a Proteção da Câmara Web

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel de **PROTEÇÃO DE VÍDEO E ÁUDIO**, clique em **Definições**.

3. Agora vá para a janela **Definições** e ative ou desative o interruptor correspondente.

Configuração da Proteção da Câmara Web

É possível configurar as regras que devem ser aplicadas quando uma aplicação tentar aceder à sua câmara ao seguir estes passos:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel de **PROTEÇÃO DE VÍDEO E ÁUDIO**, clique em **Definições**.
3. Vá para o separador **Definições**.

Estão disponíveis as seguintes opções:

Regras de bloqueio de aplicações

- **Bloquear todo o acesso à câmara Web** - nenhuma aplicação pode aceder à sua câmara Web.
- **Bloquear o acesso dos browsers à câmara Web** - nenhum browser exceto Internet Explorer e Microsoft Edge podem aceder à câmara Web. As aplicações da Windows Store são executados num único processo. Por isso, o Internet Explorer e o Microsoft Edge não podem ser detectados pelo Bitdefender como navegadores, e, portanto, estão excluídos da lista.
- **Estabelecer permissões da aplicação com base na escolha da comunidade** - se a maioria dos utilizadores de Bitdefender considerar uma aplicação popular como sendo inofensiva, o seu acesso à câmara Web é automaticamente definido como Permitir. Se uma aplicação popular for considerada como perigosa por muitas pessoas, o seu acesso será automaticamente definido como Bloqueado.

  Será informado sempre que uma das suas aplicações instaladas for listada como bloqueada pela maioria dos utilizadores do Bitdefender.

Notificações

- **Notifique quando aplicações permitidas se ligam à webcam** - será notificado sempre que uma aplicação permitida aceder à sua câmara.

Adicionar aplicações à lista de Proteção da Câmara Web

As aplicações que tentam estabelecer ligação à sua câmara Web são detetadas automaticamente e, dependendo do respetivo comportamento e da escolha da comunidade, o acesso é permitido ou recusado. No entanto,

é possível começar a configurar manualmente a ação que deve ter tomada ao seguir estes passos:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel de **PROTEÇÃO DE VÍDEO E ÁUDIO**, clique em **Definições**.
3. Vá para a janela **Proteção da Webcam**.
4. Clique na janela **Adicionar aplicação**.
5. Clique na hiperligação pretendida:
   - **Na Windows Store** - será exibida uma lista com as aplicações do Windows Store detetados. Ative os botões perto das aplicações que pretende adicionar à lista.
   - **Nas suas aplicações** - vá para o ficheiro .exe que deseja adicionar à lista e, em seguida, clique em **OK**.

Para ver o que os utilizadores do Bitdefender optaram por fazer com a aplicação selecionada, clique no ícone .

As aplicações que pedem acesso à câmara, assim como a hora da última atividade são apresentadas nesta janela.

Será notificado sempre que uma das aplicações permitidas for bloqueada pelos utilizadores do Bitdefender.

Para impedir o acesso de uma aplicação adicionada à sua webcam, clique no ícone . O ícone muda para , o que significa que a aplicação selecionada não terá acesso à sua webcam.

4.7.2. Supervisor do microfone

Aplicações nocivas podem aceder ao seu microfone integrado de forma silenciosa ou em segundo plano sem o seu consentimento. Para que fique ciente de potenciais exploits maliciosos, o supervisor do microfone do Bitdefender irá notificá-lo sobre esses eventos. Assim, nenhuma aplicação conseguirá aceder ao seu microfone sem a sua permissão.

Ativar e desativar o Supervisor do microfone

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel de **PROTEÇÃO DE VÍDEO E ÁUDIO**, clique em **Definições**.

3. Selecione a janela **Definições**.
4. Na janela **Definições**, ative ou desative o interruptor **Monitorizador do microfone**.

Configurar notificações para o Supervisor do microfone

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

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel de **PROTEÇÃO DE VÍDEO E ÁUDIO**, clique em **Definições**.
3. Vá para a janela **Definições**.

Notificações

- **Enviar notificação quando uma aplicação tentar aceder ao microfone**
- **Enviar notificação quando navegadores acederem ao microfone**
- **Enviar notificação quando aplicações não fiáveis acederem ao microfone**
- **Mostrar notificações com base na escolha dos utilizadores do Bitdefender**

Adicionar aplicações à lista do Supervisor do microfone

As aplicações que tentarem aceder ao seu microfone serão automaticamente detetadas e adicionadas à Lista de notificação. No entanto, pode configurar manualmente se uma notificação deve ser mostrada ou não, seguindo simplesmente estes passos:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel de **PROTEÇÃO DE VÍDEO E ÁUDIO**, clique em **Definições**.
3. Vá para a janela **Proteção de áudio**.
4. Clique na janela **Adicionar aplicação**.
5. Clique na hiperligação pretendida:
   - **Na Windows Store** - será exibida uma lista com as aplicações do Windows Store detetados. Ative os botões perto das aplicações que pretende adicionar à lista.
   - **Nas suas aplicações** - vá para o ficheiro .exe que deseja adicionar à lista e, em seguida, clique em **OK**.

Para ver o que os utilizadores do Bitdefender optaram por fazer com a aplicação selecionada, clique no ícone .

As aplicações que irão solicitar acesso ao seu microfone e a hora da última atividade aparecerão nesta janela.

Para deixar de receber notificações sobre a atividade de uma aplicação específica, clique no ícone . O ícone muda para , o que significa que nenhuma notificação do Bitdefender será exibida quando a aplicação selecionada tentar aceder ao microfone.

4.8. Remediação de Ransomware

A Remediação de Ransomware da Bitdefender faz uma cópia de segurança dos seus ficheiros, 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, poderá recuperar o conteúdo total de seus ficheiros sem pagar qualquer resgate exigido.

Ativar ou desativar a Remediação de Ransomware

Para ativar ou desativar a Remediação de Ransomware:

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

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

A ativar ou desativar a restauração automática

A Restauração Automática assegura que seus ficheiros sejam restaurados automaticamente em caso de encriptação por ransomware.

Para ativar ou desativar a restauração automática:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **REMEDIAÇÃO DE RANSOMWARE**, clique em **Gerir**.

3. Na janela Definições, ative ou desative o interruptor **Restauração automática**.

Ver ficheiros restaurados automaticamente

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

Para ver ficheiros restaurados automaticamente:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. Na tabela **Todas**, selecione a notificação referente ao último comportamento de ransomware remediado e, em seguida, clique em **Ficheiros Restaurados**.

   Será exibida a lista dos ficheiros restaurados. Neste local também pode ver o local onde seus ficheiros foram restaurados.

Restauração manual de ficheiros encriptados

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

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador**Todas**, selecione a notificação referente ao último comportamento de ransomware detectado e, em seguida, clique em **Ficheiros Encriptados**.
3. Será exibida a lista dos ficheiros encriptados.

   Clique em **Recuperar Ficheiros** para continuar.
4. Caso o processo de recuperação falhe inteira ou parcialmente, deve escolher o local em que os ficheiros encriptados devem ser guardados. Clique em **Restaurar localização** e, em seguida, escolha uma localização no seu PC.
5. Aparece uma janela de confirmação.

   Clique em **Finalizar** para terminar o processo de restauração.

Ficheiros com as seguintes extensões podem ser restaurados caso sejam encriptados:

.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;

Adicionar aplicações às exceções

Pode configurar regras de excepção para aplicações de confiança para que a função de Remediação de Ameaças não bloqueie caso executem ações típicas de ransomware.

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

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **REMEDIAÇÃO DE RANSOMWARE**, clique em **Gerir**.
3. Vá para a janela **Exceções** e clique em **+Adicionar uma Exceção**.

4.9. Proteção do Gestor de palavras-passe para as 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 aplicações de mensagens instantâneas.

Mas como todos sabemos, nem sempre é fácil memorizar a palavra-passe!

E se não formos cuidadosos ao navegar online, as nossas informações privadas, tais como endereço de e-mail, ID de mensagens instantâneas ou os dados do cartão de crédito, podem ficar comprometidas.

Guardar as suas palavras-passe ou os seus dados pessoais numa folha ou no computador pode ser perigoso, pois podem ser acedidos e utilizados por pessoas que pretendam roubar e utilizar essas informações. E memorizar todas as palavras-passe definidas para as suas contas online ou para os seus sites Web favoritos não é uma tarefa fácil.

Portanto, há alguma forma de garantir que encontramos as nossas palavras-passe quando necessitamos das mesmas? E podemos ter a certeza de que as nossas palavras-passe secretas estão sempre seguras?

O Gestor de palavras-passe ajuda-o a controlar as suas palavras-passe, protege a sua privacidade e proporciona uma experiência de navegação segura.

Utilizando uma única palavra-passe principal para aceder às suas credenciais, o Gestor de palavras-passe simplifica a proteção das suas palavras-passe numa Carteira.

Para oferecer a melhor proteção para as suas atividades online, o Gestor de palavras-passe está integrado com o Bitdefender Safepay™ e fornece uma solução única para as várias maneiras com que os seus dados pessoais podem ficar comprometidos.

O Gestor de palavras-passe protege as seguintes informações privadas:

- Informações pessoais, tais como endereço de e-mail e número de telefone
- Credenciais de início de sessão dos sites Web
- Informações de contas bancárias ou o número do cartão de crédito
- Dados de acesso às contas de e-mail
- Palavras-passe para as aplicações
- Palavras-passe das redes Wi-Fi

Criar uma nova base de dados Carteira

A Carteira do Bitdefender é onde pode armazenar os seus dados pessoais. Para uma experiência no navegador, deve criar uma base de dados Carteira conforme o seguinte:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **GESTOR DE PALAVRAS-PASSE**, clique em **Definições**.
3. Na janela **As Minhas Carteiras**, clique em **Adicionar carteira**.
4. Clique em **Criar nova**.
5. Digite as informações solicitadas nos campos correspondentes.
   - Nome da Carteira - introduza um nome personalizado para a sua base de dados da Carteira.
   - Palavra-passe Principal - escreva uma palavra-passe para a sua Carteira.
   - Sugestão - escreva uma sugestão para lembrar-se da palavra-passe.

6. Clique em **Continuar**.
7. Nesta etapa pode escolher armazenar as suas informações na nuvem, ao ativar o interruptor ao lado de **Sincronizar em todos os meus dispositivos**. Escolha a opção pretendida, em seguida, clique em **Continuar**.
8. Selecione o navegador da Internet de onde deseja importar as credenciais.
9. Clique em **Terminar**.

Importar uma base de dados existente

Para importar a base de dados da carteira armazenada localmente:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **GESTOR DE PALAVRAS-PASSE**, clique em **Definições**.
3. Na janela **As Minhas Carteiras**, clique em **Adicionar carteira**.
4. Clique em **Importar uma base de dados existente**.
5. Vá até ao local no seu dispositivo onde deseja guardar a base de dados da Carteira e selecione-a.
6. Clique em **Abrir**.
7. Dê um nome à sua Carteira e introduza a palavra-passe atribuída quando foi criada pela primeira vez.
8. Clique em **Importar**.
9. Selecione os programas cujas credenciais pretende que a Carteira importe e, de seguida, o botão **Terminar**.

Exportar a base de dados da Carteira

Para exportar a sua base de dados do portfólio:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **GESTOR DE PALAVRAS-PASSE**, clique em **Definições**.
3. Vá para a janela **As Minhas Carteiras**.
4. Clique no ícone • • • na carteira pretendida e, em seguida, selecione **Exportar**.

5. Aceda ao local do seu dispositivo onde deseja guardar a base de dados da carteira e escolha um nome para ele.
6. Clique em **Guardar**.

Nota
A Carteira precisa de ser aberta para que a opção **Exportar** esteja disponível. Se a carteira que precisar de exportar estiver bloqueada, clique em **Ativar carteira** e, em seguida, introduza a palavra-passe designada quando for criada.

Sincronize as suas carteiras na nuvem

Para ativar ou desativar a sincronização das carteiras na nuvem:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **GESTOR DE PALAVRAS-PASSE**, clique em **Definições**.
3. Vá para a janela **As Minhas Carteiras**.
4. Clique no ícone ••• na carteira pretendida e, em seguida, selecione **Definições**.
5. Escolha a opção pretendida na janela que aparecer, em seguida, clique em **Guardar**.

Nota
A Carteira precisa de ser aberta para que a opção **Exportar** esteja disponível. Se a carteira que precisa sincronizar estiver bloqueada, clique em **ATIVAR CARTEIRA** e, em seguida, introduza a palavra-passe designada quando ela for criada.

Gerir as suas credenciais da Carteira

Para gerir as suas palavras-passe:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **GESTOR DE PALAVRAS-PASSE**, clique em **Definições**.
3. Vá para a janela **As Minhas Carteiras**.
4. Selecione a base de dados da carteira desejada e, em seguida, clique em **Ativar Carteira**.
5. Introduza a palavra-passe principal e, de seguida, clique em **OK**.

Aparece uma nova janela. Selecione a categoria pretendida na parte superior da janela:

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

Adicionar/editar as credenciais

- Para adicionar uma nova palavra-passe, escolha a categoria pretendida acima, clique em **+ Adicionar item**, insira as informações nos campos correspondentes e clique no botão Guardar.
- Para editar uma entrada na tabela, selecione-a e clique no botão **Editar** no lado direito.
- Para eliminar uma entrada, selecione-a e clique no botão **Eliminar**.

Ativar ou desativar a proteção do Gestor de palavras-passe

Para ativar ou desativar a proteção do Gestor de Palavras-passe:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **GESTOR DE PALAVRAS-PASSE**, ative ou desative o botão.

Gerir as definições do Gestor de Palavras-passe

Para configurar a palavra-passe principal de forma detalhada:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **GESTOR DE PALAVRAS-PASSE**, clique em **Definições**.
3. Vá para a janela **Definições**.

Na seção **Definições de segurança**, as seguintes opções estão disponíveis:

- **Solicitar a minha palavra-passe principal sempre que eu aceder ao meu dispositivo** - ser-lhe-á solicitado a introduzir a palavra-passe principal ao aceder ao computador.

- **Solicitar palavra-passe principal quando abro browsers e aplicações** - ser-lhe-á solicitada a introdução da palavra-passe principal quando acede a um browser ou aplicação.
- **Não solicitar a minha palavra-passe principal** — não necessita de introduzir a sua palavra-passe principal ao aceder ao seu dispositivo, um browser ou uma aplicação.
- **Bloquear automaticamente a Carteira quando deixo o meu dispositivo sem supervisão** - ser-lhe-á solicitada a introdução da palavra-passe principal quando regressar ao seu computador após 15 minutos.

Importante
Não se esqueça da sua palavra-passe principal e registe-a num local seguro. Se esquecer a palavra-passe, terá de reinstalar o programa ou contactar o apoio do Bitdefender.

Melhore a sua experiência

Para selecionar os navegadores ou aplicações onde deseja integrar o Gestor de Palavras-passe:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **GESTOR DE PALAVRAS-PASSE**, clique em **Definições**.
3. Selecione a janela **Definições**.

   Ligue o interruptor ao lado de uma aplicação para utilizar o Administrador de Palavras-passe e melhore a sua experiência:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Safepay

Configurar o Preenchimento automático

A funcionalidade Preenchimento automático simplifica a ligação aos seus sites Web favoritos ou o início de sessão nas suas contas online. A primeira vez que introduzir as suas credenciais de início de sessão e informações pessoais no navegador da Internet, estes estarão automaticamente protegidos na Carteira.

Para configurar as definições de **Preenchimento automático**:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **GESTOR DE PALAVRAS-PASSE**, clique em **Definições**.
3. Na janela **Definições**, vá para o separador **Definições de preenchimento automático**.
4. Configure as seguintes opções:
   - **Configure como o Gestor de Palavras-passe protege as suas credenciais**:
     - **Guardar credenciais automaticamente na Carteira** - as credenciais de início de sessão e outras informações pessoais como os detalhes do seu cartão de crédito e detalhes pessoais são guardados e atualizados automaticamente na sua Carteira.
     - **Perguntar-me sempre** - ser-lhe-á sempre perguntado se pretende adicionar as suas credenciais à Carteira.
     - **Não guardar, atualizarei as informações manualmente** - as credenciais só podem ser atualizadas na Carteira manualmente.
   - **Preencher automaticamente as credenciais de início de sessão**:
     - **Preencher automaticamente e sempre as credenciais de início de sessão** - ao credenciais são inseridas automaticamente no browser.
   - **Formulários de preenchimento automático**:
     - **Mostrar as minhas opções de preenchimento quando eu visitar uma página com formulários** - um pop-up com as opções de preenchimento irá aparecer sempre que o Bitdefender detetar que deseja realizar um pagamento online ou iniciar a sessão.

Gerir as informações do Gestor de Palavras-passe a partir do seu navegador

Pode gerir facilmente os detalhes do Gestor de Palavra-passe diretamente do seu navegador para ter todos os dados importantes à mão. O add-on da Carteira do Bitdefender é suportado pelos seguintes navegadores: Google Chrome, Internet Explorer e Mozilla Firefox, e também é integrado com o Safepay.

Para aceder à extensão da Carteira do Bitdefender, abra seu navegador, permita que o add-on seja instalado e clique no ícone na barra de ferramentas.

A extensão da Carteira do Bitdefender contém as seguintes opções:

- Abrir Carteira - abre a Carteira.
- Bloquear Carteira - bloqueia a Carteira.
- Páginas da web - abre um submenu com todos os inícios de sessão em sites Web armazenados na Carteira. Clique em **Adicionar Páginas da web** para adicionar novos sites Web à lista.
- Preencher formulários - abre o submenu que contém as informações que adicionou para uma categoria específica. Aqui pode adicionar novos dados à sua Carteira.
- Gerador de Palavras-passe - permite-lhe gerar palavras-passe aleatórias que pode utilizar para contas novas ou existentes. Clique em **Mostrar definições avançadas** para personalizar a complexidade da palavra-passe.
- Definições - abre a janela de definições do Gestor de Palavras-passe.
- Relatar problema - relata qualquer problema encontrado com o Gestor de Palavras-passe do Bitdefender.

4.10. Antitracker

Uma grande parte dos sites que utiliza monitorizadores para recolher informação sobre o seu comportamento para compartilhar com empresas ou para mostrar publicidade direcionada para si. Devido a isso, os donos dos sites ganham dinheiro por proporcionar conteúdo de graça ou para continuarem a funcionar. Além de recolher informação, os monitorizadores podem desacelerar a sua navegação ou desperdiçar a sua banda larga.

Ao ativar a extensão Antitracker da Bitdefender no seu navegador, evita ser rastreado para que os seus dados permaneçam privados enquanto 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 monitorizadores que detectamos estão divididos nas seguintes categorias:

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

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 visitar um site, vai aparecer um contador no ícone referente aos monitorizadores detectados e bloqueados. Para visualizar mais detalhes sobre os monitorizadores bloqueados, clique no ícone para abrir a interface. Além do número de monitorizadores bloqueados, pode visualizar o tempo que a página precisa para carregar e as categorias às quais os monitorizadores pertencem. Para ver a lista de sites que estão a monitorizar, clique na categoria desejada.

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

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

Desligar o Antitracker da Bitdefender

Para desligar o Antitracker da Bitdefender:

- Do seu navegador Web:

1. Abra o seu navegador web.
2. Clique no ícone ao lado da barra de endereços no seu navegador.
3. Clique no ícone no canto superior direito.
4. Utilize o interruptor correspondente para o desativar.

   O ícone da Bitdefender fica cinzento.

- A partir da interface do Bitdefender:
  1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
  2. No painel **ANTITRACKER**, clique em **Definições**.
  3. Desligue o interruptor correspondente do lado do navegador web no qual deseja desativar a extensão.

Permitir a monitorização de um site

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

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

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

4.11. VPN

A aplicação do VPN pode ser instalada a partir do seu produto Bitdefender e utilizada sempre que desejar adicionar uma camada de proteção extra à sua ligação. A VPN funciona como um túnel entre o seu dispositivo e a rede à qual se liga, protegendo a sua ligação, encriptando os seus dados utilizando uma encriptação de nível bancário e escondendo o seu endereço IP onde quer que esteja. O seu tráfego é redirecionado por meio de um servidor separado, tornando o seu dispositivo quase impossível de ser identificado

entre os incontáveis dispositivos que usam os nossos serviços. Além disso, enquanto estiver ligado à Internet com o Bitdefender VPN, pode aceder a conteúdos que normalmente são restritos em áreas específicas.

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

A abrir a VPN

Para aceder à interface principal do Bitdefender VPN, use um dos seguintes métodos:

- Do tabuleiro 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 **Definições** no menu de navegação na interface do Bitdefender.
  2. No painel do **VPN**, clique em **Abrir VPN**.

Interface da VPN

A interface do VPN exibe o estado da aplicação, conectado ou desconectado. Aqui tem a possibilidade de alterar a localização do servidor ao qual está ligado.

Para conectar ou desconectar, basta clicar no estado exibido no topo do ecrã ou clique com o botão direito na bandeja do sistema. O ícone da bandeja do sistema exibe um símbolo verde quando a VPN está ligada e vermelho quando a VPN está desligada.

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

Para visualizar a área completa do **Menu**, clique no ícone no lado superior esquerdo. Tem as seguintes opções:

- **A minha conta** - detalhes sobre a sua conta Bitdefender e a subscrição 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.

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

  - **Geral**
    - Notificações
    - Arranque - escolha se executar o Bitdefender VPN ao iniciar ou não
    - Relatórios do produto - envie relatórios de produtos anónimos para nos ajudar a melhorar a sua experiência
    - Modo escuro
    - Idioma
  - **Avançadas**
    - Internet Kill-Switch - esta funcionalidade suspende temporariamente todo o tráfego da internet se a ligação VPN cair acidentalmente. Assim que estiver online novamente, a ligação VPN é restabelecida.
    - Autoconnect - Ligue o Bitdefender VPN automaticamente quando aceder a uma rede Wi-Fi pública/insegura ou quando uma aplicação de partilha de ficheiros par-a-par for iniciada

- **Suporte** - pode aceder à plataforma do Centro de Suporte onde pode ler um artigo útil sobre como utilizar o VPN Bitdefender ou nos enviar um feedback.

- **Sobre** - são apresentadas informações sobre a versão instalada.

4.12. Segurança Safepay para transações online

O computador está a tornar-se na principal ferramenta para a realização de compras e operações bancárias. Pagar contas, transferir dinheiro, comprar praticamente qualquer coisa que possa imaginar nunca foi tão fácil e rápido.

Isto engloba enviar informação pessoal, de conta e de cartão de crédito, palavras-passe e outros tipos de informação privada pela Internet, por outras

palavras exatamente o tipo de fluxo de informação que os cibercriminosos estão muito interessados em deitar a mão. Os hackers são incansáveis nos seus esforços para roubar esta informação, assim que nunca poderá ser demasiado cuidadoso em manter seguras as suas transações online.

O Bitdefender Safepay™ é, acima de tudo, um navegador protegido, um ambiente desenhado para manter a sua atividade bancária, as suas compras online e qualquer outra transação online privada e segura.

Para a melhor proteção da privacidade, o Gestor de palavras-passe do Bitdefender foi integrada ao Bitdefender Safepay™ para proteger as suas credenciais quando quiser aceder a locais online privados. Para mais informação, dirija-se a "*Proteção do Gestor de palavras-passe para as suas credenciais*" (p. 124).

O Bitdefender Safepay™ oferece as seguintes funcionalidades:

- Bloqueia o acesso ao seu ambiente de trabalho e de qualquer tentativa de tirar fotografias do seu ecran.
- Protege as suas palavras-passe secretas enquanto navega online com o Gestor de palavras-passe.
- Vem com 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 hotspot embutida para ser utilizada quando o seu dispositivo se liga a redes Wi-fi não-seguras.
- Suporta bookmarks e permite-lhe navegar entre os seus sites favoritos de bancos/compras.
- Não está só limitado ao banking e às compras online. Qualquer página Web pode ser aberta no Bitdefender Safepay™.

A utilizar o Bitdefender Safepay™

Por defeito, o Bitdefender deteta quando entra numa página de um banco ou de compras em qualquer navegador do seu dispositivo e pergunta se gostaria de utilizar o Bitdefender Safepay™.

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

- A partir da interface do Bitdefender:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel do **SAFEPAY**, clique em **Definições**.
3. Na janela do **Safepay**, clique em **Iniciar Safepay**.

- Do Windows:
  - No **Windows 7**:
    1. Clique em **Iniciar** e vá para **Todos os Programas**.
    2. Clique em **Bitdefender**.
    3. Clique em o **Bitdefender Safepay™**.
  - No **Windows 8 e Windows 8.1**:

    Encontre o Bitdefender Safepay™ no Ecrã inicial do Windows (por exemplo, pode introduzir "Bitdefender Safepay™" diretamente no Ecrã Inicial) e, em seguida, clique no ícone.
  - No **Windows 10**:

    Introduza "Bitdefender Safepay™" na caixa de pesquisa da barra de tarefas e, em seguida, clique no ícone correspondente.

Se estiver habituado a navegadores da Internet, não terá nenhum problema em utilizar o Bitdefender Safepay™ - ele parece e comporta-se como um navegador normal:

- insira URLs que deseja ir na barra de endereços.
- adicione separadores para visitar múltiplas páginas na janela do Bitdefender Safepay™ clicando em  .
- navegue para a frente e para trás e atualize as páginas usando   respetivamente.
- aceda às definições do Bitdefender Safepay™ clicando em e escolhendo **Definições**.

- proteja as suas palavras-passe com o Gestor de palavras-passe clicando em  .
- pode gerir os seus bookmarks clicando em  ao lado da barra de endereço.
- pode abrir o teclado virtual clicando em  .
- aumente ou diminua o tamanho do navegador pressionando as teclas **Ctrl** e **+/-** simultaneamente no teclado numérico.
- veja informações sobre o seu Bitdefender clicando em e escolhendo **Sobre**.
- imprima a informação importante clicando em e selecionando **Imprimir**.

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

Configurar definições

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

Aplicar as regras do Bitdefender Safepay aos domínios acedidos
Os sites que adicionou aos Favoritos com a opção **Abrir automaticamente no Safepay** ativa aparecerão aqui. Se quiser que um site da lista pare de abrir automaticamente com o Bitdefender Safepay™, clique em × do lado da entrada desejada na coluna **Remover**.

Bloqueio pop-ups
Pode escolher para bloquear pop-ups clicando no botão correspondente.

Também pode criar uma lista de páginas que possa permitir pop-ups. A lista deve conter apenas os sites web em que confia plenamente.

Para adicionar uma página à lista, introduza o seu endereço no campo correspondente e clique em **Adicionar domínio**.

Para remover uma página da web da lista, selecione o X correspondente à entrada pretendida.

Gerir Plugins
Pode escolher se pretende ativar ou desativar os plug-ins específicos no Bitdefender Safepay™.

Gerir certificados
Pode importar certificados do seu sistema para uma loja de certificados.

Clique em **IMPORTAR** e siga o assistente para utilizar os certificados no Bitdefender Safepay™.

Utilizar teclado virtual
O teclado virtual irá aparecer automaticamente quando o campo de palavra-passe for selecionado.

Utilize o botão correspondente para ativar ou desativar a função.

Confirmação de impressão
Ative esta opção se pretender dar a sua confirmação antes de iniciar o processo de impressão.

Gerir bookmarks

Se desativou a detecção automática de alguma ou de todas as páginas, ou o Bitdefendersimplesmente não detectar algumas páginas, pode adicionar bookmarks ao Bitdefender Safepay™ para que possa abrir facilmente as suas páginas favoritas no futuro.

Siga estes passos para adicionar um URL aos bookmarks do Bitdefender Safepay™

1. Clique em ••• e escolha **Marcadores** para abrir a página de Marcadores.

   Nota
   A página de Bookmarks abre por defeito quando executa o Bitdefender Safepay™.

2. Clique no botão **+** para adicionar um novo bookmark.

3. Introduza o URL e o título do favorito, e depois clique em **CRIAR**. Marque a opção **Abrir automaticamente no Safepay** se quiser que a página marcada abra com o Bitdefender Safepay™ todas as vezes que acedê-la. O URL é também adicionado à lista de Domínios na página de definições.

Desligar as notificações do Safepay

Quando um site bancário 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 **Definições** no menu de navegação na interface do Bitdefender.
2. No painel do **SAFEPAY**, clique em **Definições**.
3. Na janela **Definições**, desative o botão ao lado de **Notificações do Safepay**.

Utilizar VPN com o Safepay

Para realizar pagamentos online num ambiente seguro enquanto estiver ligado a redes inseguras, o produto Bitdefender está configurado para executar automaticamente a aplicação do VPN ao mesmo tempo com o Safepay.

Para começar a utilizar o VPN juntamente com o Safepay:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel do **SAFEPAY**, clique em **Definições**.
3. Na janela **Definições**, ligue o interruptor ao lado de **Utilizar VPN com Safepay**.

4.13. Controlo Parental

O Controlo Parental Premium da Bitdefender permite proteger as atividades online da sua criança. Uma vez configurado o Controlo Parental Premium da Bitdefender, pode facilmente descobrir o que as suas crianças estão a fazer nos dispositivos que utilizam e onde estiveram nas últimas 24 horas. Além disso, para saber melhor o que as suas crianças estão a fazer, esta caraterística mostra estatísticas sobre suas atividades e interesses.

As seguintes características estão incluídas na sua subscrição da Bitdefender:

- Em dispositivos Windows, macOS ou Android:

- Bloquear páginas web inapropriadas.
- Bloquear aplicações como jogos, conversas, programas de partilha de ficheiros ou outros.
- Bloquear a utilização do dispositivo monitorizado.
- Bloqueie o acesso à internet por períodos de tempo específicos (como a hora dos trabalhos de casa).
- Estabeleça restrições de tempo de utilização dos dispositivos.
- Veja o tempo médio gasto pelas suas crianças num dispositivo.
- Receba um relatório das aplicações utilizadas no dispositivo monitorizado nos últimos 30 dias.
- Definir áreas restritas.
- Encontre os dispositivos Android das suas crianças.

- Em dispositivos iOS:
  - Bloqueie a entrada de chamadas da lista de contactos.
  - Definir áreas restritas.
  - Localize os dispositivos iOS das suas crianças.

Para verificar as atividades online das suas crianças, faça a gestão dos dispositivos que eles utilizam ou mude as definições de Controlo Parental, precisa de aceder à sua conta da Bitdefender.

Existem duas formas de aceder à sua conta da Bitdefender, ao utilizar um navegador, indo para https://central.bitdefender.com, ou através da aplicação da Bitdefender Central, que pode ser instalada em dispositivos iOS e Android.

Para instalar a aplicação da Bitdefender Central nos seus dispositivos:

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

Nota
Neste material, recebe as opções e instruções disponíveis na plataforma web.

4.13.1. A aceder ao Controlo Parental - Os Meus Filhos

Quando aceder a secção do Controlo Parental, a janela **Os Meus filhos** estará disponível. Aqui pode começar a criar perfis para as suas crianças, e posteriormente, pode vê-los e editá-los. Uma vez criados, os perfis são mostrados como cartões de perfil, permitindo-lhe geri-los de forma rápida e mudar o seu estado em segundos.

Assim que criar um perfil, poderá personalizar as configurações mais detalhadas para monitorizar e controlar o acesso à Internet e às aplicações específicas para os seus filhos.

Pode aceder às definições do Controlo Parental a partir da sua Bitdefender Central em qualquer PC ou dispositivo móvel ligado à Internet.

Aceda à sua conta Bitdefender:

- Em qualquer dispositivo com acesso à Internet:
  1. Aceda Bitdefender Central.
  2. Inicie sessão na sua conta Bitdefender utilizando o seu endereço de e-mail e palavra-passe.
  3. Selecione o painel **Controlo Parental**.
  4. Na janela que aparecer, pode controlar e configurar os perfis do Controlo Parental para cada dispositivo.
- A partir do interface do Bitdefender :
  1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
  2. No painel **CONTROLO PARENTAL**, clique em **Configurar**.

     Será redirecionado para a página Web da conta Bitdefender. Certifique-se de que tem sessão iniciada com as suas credênciais
  3. Selecione a ferramenta **Controlo Parental**.
  4. Na janela que aparecer, pode controlar e configurar os perfis do Controlo Parental para cada dispositivo.

> **Nota**
> Certifique-se que tem a sessão iniciada no dispositivo com uma conta de administrador. Apenas os utilizadores com direitos de administrador no sistema podem aceder e configurar o Controlo Parental.

4.13.2. Crie perfis para as suas crianças

Para começar a monitorizar as atividades das suas crianças, precisa de configurar os seus perfis e instalar a aplicação de Controlo Parental da Bitdefender nos dispositivos que elas utilizam.

Para criar um perfil infantil:

1. Aceda Bitdefender Central.
2. Selecione o painel Controlo Parental.
3. Clique em **ADICIONAR UM PERFIL INFANTIL** na janela **Os Meus filhos**.
4. Estabelecer informações específicas como nome, data de nascimento ou sexo. Para adicionar uma foto ao perfil da sua criança, clique no ícone no canto inferior direito da opção **Foto de perfil**. Clique em **GUARDAR** para continuar.

   Com base no desenvolvimento infantil, definir a idade da criança carrega automaticamente as definições para pesquisar na Web consideradas apropriadas para a sua faixa etária.
5. Clique em **VAMOS ADICIONAR UM DISPOSITIVO**.
6. Se o dispositivo da sua criança já tiver a Bitdefender instalado, selecione o seu dispositivo na lista disponível e, em seguida, selecione a conta que deseja monitorizar. Clique em **ATRIBUIR**.

   Se a sua criança não tem o produto Bitdefender instalado no dispositivo que utiliza, clique em **Instalar em novo dispositivo** e, em seguida, clique em **ENVIAR LINK DE TRANSFERÊNCIA**. Escreva um endereço de e-mail no campo correspondente e clique em **Enviar e-mail**. Observe que a hiperligação de download gerada será válida apenas durante as próximas 24 horas. Se a hiperligação expirar, precisará de gerar uma nova seguindo os mesmos passos.

   No dispositivo em que deseja instalar a Bitdefender, verifique a conta de e-mail que escreveu e clique no botão de transferência correspondente.

Importante

Em dispositivos do Windows ou macOS sem o produto Bitdefender instalado, o monitorizador de verificação do Controlo Parental da Bitdefender será instalado para monitorizar as atividades online das suas crianças.
Em dispositivos Android e iOS, será feita a transferência e instalada a aplicação de Controlo Parental da Bitdefender.

Para vincular outros dispositivos, clique em **ADICIONAR DISPOSITIVO** ao lado do perfil infantil. Siga as instruções do passo 6 deste capítulo.

Instalar a aplicação do Controlo Parental da Bitdefender em dispositivos Android e iOS

Para monitorizar as atividades online das suas crianças em dispositivos Android ou iOS, deve instalar a aplicação do Controle Parental e, em seguida, vincular os seus dispositivos à sua conta da Bitdefender. Dependendo do dispositivo da sua criança, siga estes passos:

- Em **Android**:

  1. Vá para a Google Play Store, procure Controlo Parental da Bitdefender e clique em instalar.
  2. Clique em **ACEITAR** as permissões quando lhe for solicitado. Bitdefender necessita de permissões para o manter informado sobre a atividade do seu filho e, se não forem aceites, a aplicação não será instalada.
  3. Abra a aplicação do Controlo Parental.
  4. Um assistente introdutório com detalhes sobre as funções do produto é apresentado na primeira vez que abre a aplicação. Selecione **PRÓXIMO** para continuar a ser guiado, ou **SALTAR** para fechar o assistente.
  5. Para continuar a instalação, a Bitdefender precisa da sua aprovação para recolher informações pessoais da sua criança, que serão utilizadas apenas para o informar sobre as atividades da sua criança. Para mais detalhes, toque em **Política de privacidade**. Ao tocar em **CONTINUAR**, aceita que sejam recolhidos dados pessoais do dispositivo.
  6. Inicie sessão na sua conta Bitdefender existente. Se não tiver uma conta Bitdefender, pode optar por criar uma nova conta utilizando a opção correspondente. Alternativamente, pode entrar com uma conta do Facebook, Google ou Microsoft.
  7. Toque em **ATIVAR** para ser redirecionado para o ecrã de onde pode ativar a opção de acessibilidade da aplicação. Siga as instruções no ecrã para configurar corretamente a aplicação.
  8. Toque em **PERMITIR** para ser redirecionado para o ecrã de onde pode ativar a opção Ativar Acesso de Utilização da aplicação. Siga as instruções no ecrã para configurar corretamente a aplicação.

9. Toque em **ATIVAR** para ser redirecionado para o ecrã de onde pode ativar a opção Ativar Direitos de Administrador de Dispositivo da aplicação. Siga as instruções no ecrã para configurar corretamente a aplicação.

   Isto evitará que o seu filho desinstale a aplicação do Controlo Parental.

10. Clique em **PERMITIR** e, em seguida, conceda todas as permissões solicitadas.

11. Atribua o dispositivo ao perfil da criança.

- Em **iOS**:

1. Vá para App Store, pesquise Controlo Parental da Bitdefender e toque na opção de instalar.

2. Para continuar a instalação, a Bitdefender precisa da sua aprovação para recolher informações pessoais da sua criança, que serão utilizadas apenas para o informar sobre as atividades da sua criança. Para mais detalhes, toque em **Política de privacidade**. Ao tocar em **Continuar**, aceita que sejam recolhidos dados pessoais do dispositivo.

3. Inicie sessão na sua conta Bitdefender existente. Se não tiver uma conta Bitdefender, pode optar por criar uma nova conta utilizando a opção correspondente. Alternativamente, pode entrar com uma conta do Facebook, Google ou Microsoft.

4. Solicita-se que dê acesso a todas as permissões solicitadas, que são necessárias para a aplicação. Toque em **Permitir**.

5. Permita o acesso à localização do dispositivo para que o Bitdefender o possa localizar.

6. Permita que a aplicação envie notificações. Para gerir as notificações do Bitdefender, vá a Definições > Notificações > Parental.

7. Para monitorizar os contactos da sua criança, precisa de ativar o **Bloqueio e identificação de ligações**. Siga os passos necessários para poder utilizar o Controlo Parental da Bitdefender para restringir a entrada de chamadas.

8. Atribua o dispositivo ao perfil da criança.

Monitorizar as atividades online da sua criança

O Controlo Parental da Bitdefender irá ajudá-lo a estar informado sobre as atividades online das suas crianças. Assim, saberá sempre as atividades exatas nas quais estão envolvidas durante o tempo que passam em cada dispositivo.

Dependendo das definições, o Bitdefender fornece relatórios que podem conter informações para cada evento, tais como:

- O estado do evento.
- A gravidade da notificação.
- O nome do dispositivo.
- A data e a hora em que ocorreu o evento.

Para monitorizar o tráfego na internet, as aplicações acedidas ou a atividade online das suas crianças:

1. Aceda Bitdefender Central.
2. Selecione o painel Controlo Parental.
3. Selecione um perfil infantil.

   Na janela principal de **Atividades**, pode ver as informações que lhe interessam.

Configurar as Definições de relatórios

Como definição padrão, o Controlo Parental está ativo, e as atividades online das suas crianças são registadas.

Para receber notificações sobre as atividades online das suas crianças:

1. Aceda Bitdefender Central.
2. Selecione o painel Controlo Parental.
3. Clique em **DEFINIÇÕES DO RELATÓRIO**.
4. Ative o interruptor correspondente para receber relatórios de atividades.
5. Digite o endereço eletrónico para onde serão enviadas das notificações por correio eletrónico.
6. Ajuste a frequência selecionando: diário, semanal ou mensal, e clique em **GUARDAR**.

Também pode escolher receber notificações na sua conta da Bitdefender nas seguintes situações:

- Cada vez que as suas crianças tentem aceder a aplicações bloqueadas (Windows, macOS e Android).
- Cada vez que as suas crianças recebam chamadas de números bloqueados/desconhecidos (iOS).
- Cada vez que as suas crianças saiam das áreas seguras ou entrem em áreas restritas.
- Cada vez que as suas crianças cheguem em segurança.

Editar um perfil

Para editar um perfil existente:

1. Aceda Bitdefender Central.
2. Selecione o painel **Controlo Parental**.
3. Clique em **OPÇÕES** no cartão de perfil desejado e, em seguida, selecione **Editar perfil**.
4. Após personalizar as definições pretendidas, selecione **GUARDAR**.

Remover um perfil

Para remover um perfil existente:

1. Aceda Bitdefender Central.
2. Selecione o painel **Controlo Parental**.
3. Selecione o perfil infantil.
4. Clique no botão **OPÇÕES** e, em seguida, selecione **Eliminar perfil**.
5. Confirme a sua escolha.

4.13.3. Configurar perfis do Consultor Parental

Para começar a monitorizar as suas crianças, um perfil precisa de ser vinculado ao dispositivo que tem instalado a funcionalidade ou aplicação do Controlo Parental da Bitdefender.

Depois de criar o perfil, pode personalizar as definições mais detalhadas para monitorizar e controlar o acesso à internet e a aplicações específicas.

Para começar a configurar um perfil, selecione o cartão do perfil desejado e clique em **OPÇÕES**.

Clique num separador para configurar as funcionalidades do Consultor Parental correspondentes ao dispositivo:

- Tempo de ecrã - permite bloquear o acesso a dispositivos especificados por si no perfil das suas crianças. O acesso pode ser restrito tanto para um determinado intervalo de tempo quanto para limites diários acumulativos.
- Aplicações - permite bloquear o acesso a certas aplicações, como jogos, programas de mensagens, filmes, etc.
- Websites - permite filtrar a navegação na internet.
- Localização da sua criança - aqui pode determinar locais seguros ou inseguros para as suas crianças.
- Contactos do telefone - aqui poderá ver os contactos no telefone do seu filho.
- Visualizar dispositivos - aqui pode visualizar o estado dos dispositivos monitorizados, vincular um novo dispositivo ao perfil do seu filho ou remover um dispositivo vinculado.

Actividade

A janela principal oferece-lhe informações detalhadas sobre as atividades online dos seus filhos nas últimas 24 horas ou nos últimos 7 dias, segundo a sua escolha, dentro e fora da casa. Para ver as atividades dos sete dias anteriores clique em **Últimos 7 dias**.

Dependendo da atividade, esta janela pode incluir informações sobre:

- **Localização da sua criança** - aqui pode saber onde as suas crianças estiveram durante o dia.
- **Atividade do website** - aqui pode ver informação sobre as categorias de sites que os seus filhos visitaram. Clique na ligação **ALTERAR DEFINIÇÕES** para permitir ou negar acesso a interesses específicos.
- **Contactos telefónicos recentemente adicionados** - aqui pode ver se foram adicionados novos contactos nos dispositivos do seu filho. Clique na hiperligação **VER TODOS OS CONTACTOS DO TELEFONE** para selecionar os contactos com os quais as suas crianças podem comunicar ou não.

- **Aplicações** - aqui pode ver as aplicações utilizadas pelas suas crianças. Clique na hiperligação **VER TODAS AS APLICAÇÕES** para bloquear ou permitir o acesso a aplicações específicas.
- **Tempo de ecrã** - aqui pode ver o tempo gasto online em todos os dispositivos vinculados às suas crianças e o local onde eles estiveram ativos. Clique em **VER TEMPO DE ECRÃ** para aceder à janela de **Tempo de ecrã**.

Aplicações

A janela de Aplicações permite bloquear a execução de aplicações em dispositivos Windows, macOS e Android. Jogos, software de multimédia e de mensagens, assim como outras categorias de software podem ser bloqueadas desta forma.

Aqui pode ver as aplicações mais utilizadas nos últimos 30 dias, bem como o tempo gasto nelas pelas suas crianças. As informações sobre o tempo gasto em aplicações só podem ser recolhidas em dispositivos Windows, macOS e Android.

Para configurar o controlo de aplicações para uma conta de utilizador específica:

1. Será exibida uma lista com os dispositivos atribuídos.

   Selecione o cartão com o dispositivo cujo acesso a aplicações deseja limitar.

2. Clique em **Gerir aplicações utilizadas por...**.

   Será exibida uma lista das aplicações instaladas.

3. Selecione **Bloqueado** próximo às aplicações que deseja que o seu filho pare de utilizar.

4. Clique em **GUARDAR** para aplicar as novas definições.

Pode parar de monitorizar as aplicações instaladas ao desligar a opção **Monitorizar aplicações utilizadas** no canto superior direito da janela.

Websites

A janela Websites permite bloquear sites com conteúdo inadequado em dispositivos Windows, macOS e Android. Os sites que possuem vídeos, jogos, software multimédia e de mensagens instantâneas, assim como outras categorias de conteúdo negativo, podem ser bloqueados desta forma.

A funcionalidade pode ser ativada ou desativada utilizando o botão correspondente.

Segundo a idade definida para as suas crianças, a Lista de interesses apresenta uma seleção de categorias ativas como predefinição. Para permitir ou negar o acesso a uma categoria específica, clique na mesma.

O ícone  indica que a sua criança não poderá aceder a conteúdo relacionado com uma categoria específica.

Permitir ou bloquear um site Web

Para permitir ou negar o acesso a certas páginas Web, tem de adicioná-las à lista de Exclusões, conforme se segue:

1. Clique no botão **GERIR**.
2. Escreva o endereço da página que deseja permitir ou bloquear no campo correspondente.
3. Selecione **Permitir** ou **Bloquear**.
4. Clique no ícone **+** para guardar as alterações.

Nota
As restrições de acesso a sites Web só podem ser definidas para dispositivos Windows, Android e macOS adicionados ao perfil do seu filho.

Contactos telefónicos

A janela Contactos telefónicos oferece a possibilidade de ver os contactos no telefone do seu filho.

A funcionalidade está disponível em dispositivos iOS e Android.

Localização do seu filho

Visualizar a localização atual do dispositivo no Google Maps. A localização é atualizada a cada 5 segundos para que possa controlá-lo se estiver em movimento.

A precisão da localização depende do quanto o Bitdefender é capaz de o determinar:

- Caso o GPS esteja ativado no dispositivo, a sua localização pode ser determinada no alcance de dois metros, desde que esteja ao alcance dos satélites GPS (ou seja, fora de um edifício).
- Se o dispositivo estiver dentro de um edifício, a sua localização pode ser determinada no alcance de 10 metros caso o Wi-Fi esteja ativado e existam rede sem fios disponíveis no seu alcance.
- Caso contrário, a localização será determinada utilizando apenas as informações da rede móvel, que pode oferecer uma precisão não melhor que várias centenas de metros.

Configurar localização e check-in seguro

Para certificar-se de que o seu filho vai a certos locais, pode criar uma lista de locais seguros e não seguros. Sempre que entrar sozinho numa área predefinida, será apresentada uma notificação na aplicação Controlo Parental a pedir para confirmar que está seguro. Ao tocar em **CHEGUEI BEM** é informado através de uma notificação na sua conta Bitdefender de que o destino final foi alcançado.

No caso de o seu filho não confirmar, continua a poder ver o histórico da sua localização ao longo do dia ao consultar o seu perfil na sua conta Bitdefender.

Para configurar um local:

1. Na interface do Controlo Parental, aceda o perfil do seu filho, clique em **OPÇÕES** e selecione a janela **Localização do seu filho**.
2. Clique em **Dispositivos**.
3. Clique no dispositivo que deseja configurar.
4. Na janela **Áreas**, clique no botão **ADICIONAR ÁREA**.
5. Escolha o tipo de local, **SEGURO** ou **RESTRITO**.
6. Digite um nome válido para a área onde o seu filho tem autorização para entrar.
7. Defina a distância que deverá ser utilizada para monitorização na barra **Raio**.
8. Clique em **ADICIONAR ÁREA** para guardar as suas definições. É-lhe perguntado se o seu filho vai viajar sozinho ou acompanhado. Confirme com Sim ou Não.

Nota
O controlador de localização pode ser utilizado para monitorizar dispositivos Android e iOS que têm a aplicação Controlo Parental do Bitdefender instalada.

Tempo no ecrã

Na janela Tempo de Ecrã, é informado sobre o tempo gasto nos dispositivos designados no dia atual, quanto tempo resta do limite diário que definiu, e o estado do perfil selecionado, ativo ou em pausa. Nesta janela, também pode definir limites de horário para diferentes horas do dia, como a hora de ir para cama, fazer os trabalhos de casa ou lições particulares.

Limites de Tempo

Para começar a configurar os limites de tempo:

1. Clique em **OPÇÕES** e selecione **Tempo de ecrã**.
2. Na área de **Agendamentos**, clique em **ADICIONAR AGENDAMENTO**.
3. Dê um nome para o agendamento que deseja definir (por exemplo, hora de ir para a cama, trabalhos de casa, aulas de ténis, etc.).
4. Defina um período de tempo no qual as restrições devem ser aplicadas e, em seguida, clique em **ADICIONAR AGENDAMENTO** para guardar as definições.

Para editar uma restrição que definiu, vá para a secção Agendamentos, indique a restrição que deseja editar e, em seguida, clique no botão **EDITAR**.

Para eliminar uma restrição, vá para a janela de Tempo da Ecrã, indique a restrição que deseja editar, clique em **EDITAR** e depois selecione **ELIMINAR AGENDAMENTO**.

Limite diário

O limite de utilização diário pode ser aplicado a dispositivos Windows, macOS e Android. Se ajustou o perfil para entrar em pausa quando o limite for alcançado, então essa configuração aplicar-se-á a todos os dispositivos atribuídos, não importa se forem Windows, macOS, Android ou iOS.

Para determinar um limite de utilização diária:

1. Clique em **OPÇÕES** e selecione **LIMITES DE TEMPO DIÁRIO**.
2. Defina a hora e o dia nos quais as restrições devem ser aplicadas e, em seguida, clique em **GUARDAR ALTERAÇÕES** para guardar as definições.

4.14. Dispositivo Anti-Roubo

O roubo de portáteis é um assunto importante que afeta igualmente indivíduos e empresas. Mais do que perder o hardware em si, é a perda de informação que pode causar danos significativos, quer financeiramente quer emocionalmente.

No entanto são poucas as pessoas que tomam as devidas precauções para proteger a sua importante informação pessoal, financeira e de negócio em caso de perda ou roubo.

O Anti-roubo do Bitdefender ajuda-o a estar mais bem preparado para tal situação ao permitir-lhe localizar ou bloquear remotamente o seu computador portátil e até mesmo destruir toda a informação dele, se alguma vez se separar do seu computador portátil contra a sua vontade.

Para usar as funcionalidades do Anti-Roubo, os seguintes pré-requisitos devem ser preenchidos:

- Os comandos só podem ser enviados da conta Bitdefender.
- O computador portátil deve estar ligado à Internet para receber os comandos.

As funcionalidades Anti-roubo funcionam da seguinte forma:

Localizar

Mostra a localização do seu dispositivo no Google Maps.

A precisão da localização depende do quanto o Bitdefender é capaz de o determinar. A localização é determinada em dezenas de metros se a ligação Wi-fi está ativada no seu computador portátil e existam redes wireless ao seu alcance.

Se o computador portátil estiver ligado a uma rede LAn por cabo sem uma localização por Wi-fi disponível, a localização será determinada baseada no endereço IP, que é consideravelmente menos precisa.

Alerta

Envie um alerta remoto no dispositivo.

Esta funcionalidade só está disponível em dispositivos móveis.

Fechar

Bloqueie o seu computador portátil e defina um PIN de 4 dígitos para o desbloquear. Quando envia o comando de **Bloqueio**, o sistema reinicia e o login no Windows só é possível após inserir o PIN que definiu.

Se pretender que o Bitdefender tire fotos da pessoa que tentar aceder ao seu computador portátil, marque a caixa de verificação correspondente. As fotos são tiradas utilizando a câmara frontal e exibidas com a data e hora no painel da função Anti-furto. Apenas serão guardadas as duas fotos mais recentes.

Esta ação está disponível apenas para computadores portáteis que têm uma câmara frontal.

Limpar
Remover todos os dados do seu sistema. Quando envia o comando de **Limpeza**, o computador portátil reinicia e toda a informação nas partições do disco rígido é apagada.

Mostrar IP
Exibe o último endereço de IP para o dispositivo selecionado. Clique em **MOSTRAR IP** para torná-lo visível.

O Anti-roubo é ativado após a instalação e só pode ser acedido exclusivamente através da sua conta Bitdefender a partir de qualquer dispositivo ligado à Internet, em qualquer lado.

Utilizar funcionalidades Anti-Roubo

Para aceder às funcionalidades Anti-furto, utilize uma das seguintes possibilidades:

- A partir da interface principal do Bitdefender:
  1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
  2. Clique em **IR PARA A CENTRAL**.

     Será redirecionado para a página da Bitdefender Central. Certifique-se de que tem sessão iniciada com as suas credênciais
  3. Na janela da Bitdefender Central que abrir, clique no cartão do dispositivo pretendido e, em seguida, selecione **Anti-furto**.
- Em qualquer dispositivo com acesso à Internet:
  1. Abra um navegador Web e vá para: https://central.bitdefender.com.
  2. Inicie sessão na sua conta Bitdefender utilizando o seu endereço de e-mail e palavra-passe.
  3. Selecione o painel **Os Meus Dispositivos**.

4. Clique no cartão do dispositivo pretendido e, em seguida, selecione **Anti-furto**.
5. Selecione a funcionalidade que deseja usar:

   Mostrar IP - exibe o último endereço de IP do seu dispositivo.
   Localizar - exibe a localização do seu dispositivo no Google Maps.

    **Alerta** - emite um alerta no dispositivo.

    **Bloquear** - bloqueie o seu computador portátil e defina um PIN para desbloqueá-lo.

    **Limpar** - eliminar todos os dados do seu computador portátil.

   
   Importante
   Após apagar toda a informação de um dispositivo, todas as funcionalidades Anti-Roubo deixam de funcionar.

4.15. Bitdefender USB Immunizer

A funcionalidade Autorun embutida ao sistema operacional Windows é uma ferramenta bastante útil que permite aos dispositivos executarem automaticamente um ficheiro de um dispositivo de media ligado a ele. Por exemplo, as instalações de software podem iniciar automaticamente quando o CD é inserido na drive de CDs.

Infelizmente, esta funcionalidade também pode ser utilizada pelas ameaças para iniciar automaticamente e infiltrar no seu dispositivo a partir de dispositivos multimédia graváveis, tais como unidades USB flash e cartões de memória ligados através de leitores de cartões. Numerosos ataques Autorun foram criados nestes últimos anos.

Com o Imunizador USB pode evitar que qualquer unidade flash formatada em NTFS, FAT32 ou FAT jamais possa automaticamente executar ameaças. Uma vez que um dispositivo USB esteja imunizado, as ameaças já não o podem configurar para executar determinada aplicação quando o dispositivo esteja ligado a um dispositivo em Windows.

Para imunizar um dispositivo USB:

1. Ligue a drive flash ao seu dispositivo.

2. Explore o seu dispositivo para localizar o dispositivo de armazenagem amovível e clique com o botão direito do rato sobre ele.
3. No menu contextual, aponte para o **Bitdefender** e selecione **Imunizar esta drive**.

> **Nota**
> Se a unidade já tiver sido imunizada, a mensagem **O dispositivo USB está protegido contra ameaças no autorun** aparecerá em vez da opção Imunizar.

Para prevenir que o seu dispositivo execute ameaças de dispositivos USB não imunizados, desative a funcionalidade de media autorun. Para mais informação, dirija-se a "*Usar monitorização de vulnerabilidade automática*" (p. 112).

5. UTILITÁRIOS

5.1. Perfis

Atividades de trabalho diárias, ver filmes ou jogar podem provocar lentidão no sistema, especialmente se estes estiverem a ser executados simultaneamente com os processos de atualização do Windows e as tarefas de manutenção. Com o Bitdefender, pode agora escolher e aplicar o seu perfil preferido; o que irá ajustar o sistema a melhorar o desempenho de aplicações específicas.

O Bitdefender fornece os seguintes perfis:

- Perfil Trabalho
- Perfil de Filme
- Perfil de Jogo
- Perfil Wi-Fi Público
- Perfil do Modo de Bateria

Caso decida não utilizar os **Perfis**, um perfil predefinido chamado **Padrão** será ativado e não fará qualquer otimização no seu sistema.

De acordo com a sua atividade, as seguintes definições do produto serão aplicadas quando os perfis Trabalho, Filme ou Jogo são ativados:

- Todos os alertas e pop-ups do Bitdefender são desativados.
- A Atualização Automática é adiada.
- As análises agendadas são adiadas.
- O módulo Antispam está ativado.
- O Consultor de Pesquisa é desativado.
- As notificações de ofertas especiais estão desativadas.

De acordo com sua atividade, as seguintes definições do sistema são aplicadas quando os perfis Trabalho, Filme ou Jogo são ativados:

- As Atualizações Automáticas do Windows são adiadas.
- Os alertas e pop-ups do Windows são desativados.
- Os programas desnecessários em segundo plano são suspensos.

- Os efeitos visuais são ajustados para o melhor desempenho.
- As tarefas de manutenção são adiadas.
- As definições do plano de energia são ajustadas.

Ao executar neste perfil Wi-Fi público, o Bitdefender Total Security é definido automaticamente de modo a obter as seguintes definições de programa:

- Advanced Threat Defense ativado
- A Firewall do Bitdefender é ativada e as definições seguintes são aplicadas ao seu adaptador sem fios:
  - Modo Stealth - : LIGADO
  - Tipo de rede - Pública
- As seguintes definições da Prevenção contra ameaças online são ativadas:
  - Encrypted web scan
  - Proteção contra fraudes
  - Proteção contra phishing

5.1.1. Perfil Trabalho

A execução de várias tarefas no trabalho, tais como o envio de e-mails, ter uma videoconferência com os seus colegas distantes ou trabalhar com aplicações de design pode afetar o desempenho do sistema. O Perfil de Trabalho foi desenhado para ajudá-lo a melhorar a sua eficiência no trabalho, desativando alguns dos serviços e tarefas de manutenção em segundo plano.

A configurar o Perfil de Trabalho

Para configurar as ações a executar enquanto está no Perfil de Trabalho:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Perfis**, clique em **Definições**.
3. Clique no botão **CONFIGURAR** na área do Perfil de Trabalho.
4. Escolha os ajustes do sistema que quer que sejam aplicados selecionando as seguintes opções:
   - Aumente o desempenho das aplicações de trabalho

- Otimize as definições do produto para o perfil Trabalho
- Adie programas em segundo plano e tarefas de manutenção
- Adiar as Atualizações Automáticas do Windows

5. Clique em **GUARDAR** para guardar as alterações e fechar a janela.

A adicionar aplicações manualmente à lista do Perfil de Trabalho

Se o Bitdefender não entrar automaticamente no Perfil de Trabalho quando abre uma determinada aplicação de trabalho, pode adicionar a aplicação manualmente à **Lista de aplicações de trabalho**.

Para adicionar aplicações manualmente à Lista de aplicações de trabalho do Perfil de Trabalho:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Perfis**, clique em **Definições**.
3. Clique no botão **CONFIGURAR** na área do Perfil de Trabalho.
4. Na janela **Definições do perfil de trabalho**, clique em **Lista de aplicações**.
5. Clique em **ADICIONAR**.

   Aparece uma nova janela. Vá até ao ficheiro executável da aplicação, selecione-o e clique em **OK** para o adicionar à lista.

5.1.2. 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 definições do sistema e do produto para que possa desfrutar de uma experiência cinematográfica agradável e sem interrupções.

A configurar o Perfil de Filme

Para configurar as ações a serem tomadas no Perfil de Filme:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Perfis**, clique em **Definições**.
3. Clique no botão **CONFIGURAR** na área do Perfil de Filme.
4. Escolha os ajustes do sistema que quer que sejam aplicados selecionando as seguintes opções:

- Aumente o desempenho dos leitores de vídeo
- Otimize as definições do produto para o perfil Filme
- Adie programas em segundo plano e tarefas de manutenção
- Adiar as Atualizações Automáticas do Windows
- Ajustar as definições do esquema de energia para filmes

5. Clique em **GUARDAR** para guardar as alterações e fechar a janela.

A adicionar manualmente leitores de vídeo à lista do Perfil de Filme

Se o Bitdefender não entrar automaticamente no Perfil de Cinema quando abrir uma certa aplicação de reprodução de vídeo, pode adicioná-lo manualmente à **Lista de aplicações de filme**.

Para adicionar manualmente leitores de vídeo à Lista de aplicações de filme no Perfil de Filme:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Perfis**, clique em **Definições**.
3. Clique no botão **CONFIGURAR** na área do Perfil de Filme.
4. Na janela **Definições do perfil de trabalho**, clique em **Lista de aplicações**.
5. Clique em **ADICIONAR**.

   Aparece uma nova janela. Vá até ao ficheiro executável da aplicação, selecione-o e clique em **OK** para o adicionar à lista.

5.1.3. Perfil de Jogo

Para desfrutar de uma experiência de jogo sem interrupções, é importante reduzir a carga do sistema e diminuir a lentidão. Ao utilizar 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 possa aproveitar a sua pausa de jogo.

A configurar o Perfil de Jogo

Para configurar as ações a serem tomadas no Perfil de Jogos:

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

2. No separador **Perfis**, clique em **Definições**.
3. Clique no botão **Configurar** na área do Perfil de Jogos.
4. Escolha os ajustes do sistema que quer que sejam aplicados selecionando as seguintes opções:
   - Aumente o desempenho dos jogos
   - Otimize as definições do produto para o perfil Jogo
   - Adie programas em segundo plano e tarefas de manutenção
   - Adiar as Atualizações Automáticas do Windows
   - Ajustar as definições do esquema de energia para jogos
5. Clique em **GUARDAR** para guardar as alterações e fechar a janela.

Adicionar os jogos manualmente à lista de Jogos

Se o Bitdefender não entrar automaticamente no Perfil de Jogo quando abre um certo jogo ou aplicação, pode adicioná-lo manualmente à **Lista de aplicações de jogos**.

Para adicionar jogos manualmente à lista de aplicações de jogos no Perfil de Jogo:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Perfis**, clique em **Definições**.
3. Clique no botão **CONFIGURAR** na área do Perfil de Jogos.
4. Na janela **Definições do perfil de trabalho**, clique em **Lista de aplicações**.
5. Clique em **ADICIONAR**.

   Aparece uma nova janela. Navegue até o ficheiro executável do jogo, selecione-o e clique em **OK** para adicioná-lo à lista.

5.1.4. Perfil Wi-Fi Público

Enviar e-mails, digitar credenciais sensíveis ou fazer compras online enquanto ligado a uma rede sem fios insegura pode colocar os seus dados pessoais em risco. O perfil Wi-Fi Público ajusta as definições do produto para lhe dar a possibilidade de fazer pagamentos online e utilizar informações sensíveis num ambiente protegido.

A configurar o perfil Wi-Fi Público

Para configurar o Bitdefender para aplicar as definições do produto enquanto ligado a uma rede sem fios insegura:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Perfis**, clique em **Definições**.
3. Clique no botão **CONFIGURAR** na área do Perfil Wi-Fi Público.
4. Deixe a caixa de verificação **Ajusta as definições do produto para aumentar a proteção quando ligado a uma rede Wi-Fi pública insegura** marcada.
5. Clique em **Guardar**.

5.1.5. Perfil do Modo de Bateria

O perfil Modo de Bateria foi concebido especialmente para utilizadores de portáteis e tablets. O seu objetivo é minimizar o impacto do sistema e do Bitdefender no consumo de energia quando o nível de bateria estiver abaixo do nível predefinido que selecionou.

Configurando o perfil Modo de Bateria

Para configurar o perfil Modo de Bateria:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Perfis**, clique em **Definições**.
3. Clique no botão **Configurar** na área do Perfil do Modo de Bateria.
4. Escolha os ajustes do sistema que serão aplicados selecionando as seguintes opções:
   - Otimize as definições do produto para o modo Bateria.
   - Adie programas em segundo plano e tarefas de manutenção.
   - Adiar as Atualizações Automáticas do Windows.
   - Ajuste as definições do plano de energia para o modo Bateria.
   - Desative os dispositivos externos e as portas de rede.
5. Clique em **GUARDAR** para guardar as alterações e fechar a janela.

Digite um valor válido na caixa de rotação ou selecione um valor utilizando os botões de setas para cima e para baixo para especificar quando o sistema

deve começar a operar no Modo de Bateria. Por defeito, o modo é ativado quando o nível da bateria cai abaixo dos 30%.

As definições do produto seguinte são aplicadas quando o Bitdefender opera em Modo de Bateria:

- A Atualização Automática do Bitdefender é adiada.
- As análises agendadas são adiadas.

O Bitdefender detecta quando o seu portátil está a funcionar na bateria e dependendo do nível de carga, entra automaticamente em Modo de Bateria. Da mesma forma, o Bitdefender sai automaticamente do Modo de Bateria ao detectar que o portátil já não está a funcionar pela bateria.

5.1.6. Otimização em tempo real

A Otimização em Tempo Real do Bitdefender é um plugin que melhora o desempenho do seu sistema de forma silenciosa, em segundo plano, garantindo que não seja interrompido enquanto está num modo de perfil. Dependendo da carga do CPU, o plug-in monitoriza todos os processos, focando naqueles que utilizam uma carga maior, para ajustá-los às suas necessidades.

Para ativar ou desativar a Otimização em Tempo Real:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No separador **Perfis**, clique em **Definições**.
3. Desloque-se para baixo até ver a opção de otimização em tempo real e utilize o botão correspondente para a ativar ou desativar.

5.2. Otimizador de Um Clique

Problemas como falhas no disco rígido, ficheiros de registo excedentes e histórico do navegador podem atrasar o seu trabalho, o que se pode tornar num desconforto para si. Tudo isto pode ser corrigido com um único clique de um botão.

O Otimizador de Um Clique permite-lhe identificar e remover ficheiros inúteis ao executar uma série de tarefas de limpeza ao mesmo tempo.

Para iniciar o processo do OneClick Optimizer:

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

2. Clique no botão **Otimizar**.

   a. **A analisar**

      Aguarde que o Bitdefender termine de procurar por problemas no sistema.

      - Limpeza de Disco — identifica os ficheiros e pastas desnecessários.
      - Limpeza do Registo - identifica referências inválidas ou obsoletas no Registo do Windows.
      - Limpeza de Privacidade - identifica ficheiros temporários da Internet, cookies, cache e histórico do navegador.

      O número de problemas encontrados foi exibido. Clique na hiperligação **Ver detalhes** para revê-los antes de prosseguir com o processo de limpeza. Clique em **Otimizar** para continuar.

   b. **A otimizar**

      Aguarde que o Bitdefender conclua a otimização do seu sistema.

   c. **Questões**

      Aqui pode ver o resultado da operação.

      Se desejar informações detalhadas sobre o processo de otimização, clique no botão **Visualizar relatório detalhado**.

5.3. Proteção de dados

Apagar ficheiros permanentemente

Quando apaga um ficheiro, o mesmo já não fica acessível por meios normais. No entanto o ficheiro continua armazenado no disco duro até que seja sobrescrito quando copiar para lá novos ficheiros.

O Destruidor de Ficheiros do Bitdefender ajuda a eliminar permanentemente dados removendo-os fisicamente do seu disco rígido.

Pode rapidamente destruir ficheiros ou pastas do seu dispositivo utilizando o menu contextual Windows seguindo os seguintes passos:

1. Clique botão direito sobre o ficheiro ou pasta que deseja apagar permanentemente.

2. Selecione **Bitdefender** > **Destruidor Ficheiros** no menu contextual que aparece.
3. Clique em **Eliminar permanentemente** e, em seguida, confirme que deseja continuar com o processo.

   Aguarde que o Bitdefender termine a destruição dos ficheiros.
4. Os resultados são apresentados. Clique em **Terminar** para sair do assistente.

Alternativamente pode destruir os ficheiros a partir da interface do Bitdefender, conforme o seguinte:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **Proteção de dados**, clique em **Destruidor de Ficheiros**.
3. Siga o assistente do Destruidor de Ficheiros:
   a. Clique no botão **Adicionar pastas** para adicionar os ficheiros ou pastas que deseja remover permanentemente.

      Alternativamente, arraste estes ficheiros ou pastas para esta janela.
   b. Clique em **Eliminar permanentemente** e, em seguida, confirme que deseja continuar com o processo.

      Aguarde que o Bitdefender termine a destruição dos ficheiros.
   c. **Resumo do Resultado**

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

6. SOLUÇÃO DE PROBLEMAS

6.1. Resolver 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 correta das definições do produto.

- "*O meu sistema parece estar lento*" (p. 166)
- "*A análise não inicia*" (p. 168)
- "*Já não posso utilizar uma aplicação*" (p. 170)
- "*O que fazer quando a Bitdefender bloqueia um site, domínio, endereço de IP ou aplicação online segura*" (p. 171)
- "*Como atualizar o Bitdefender numa ligação à Internet lenta*" (p. 175)
- "*Os serviços Bitdefender não estão a responder*" (p. 176)
- "*O filtro Antispam não está a funcionar corretamente*" (p. 177)
- "*A funcionalidade Preenchimento automático na minha Carteira não funciona*" (p. 181)
- "*Remoção de Bitdefender falhou*" (p. 182)
- "*O meu sistema não reinicia após a instalação de Bitdefender*" (p. 183)

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 "*Pedir Ajuda*" (p. 302).

6.1.1. O meu sistema parece estar lento

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

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

- **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 informação, dirija-se a "*Como posso remover outras soluções de segurança?*" (p. 68).

- **Não estão cumpridos os requisitos do sistema para executar o Bitdefender.**

  Se o seu dispositivo não cumprir os Requisitos do Sistema, ficará lento, especialmente se estiver a executar várias aplicações ao mesmo tempo. Para mais informação, dirija-se a "*Requisitos do sistema*" (p. 2).

- **Instalou aplicações que não utiliza**.

  Qualquer dispositivo tem programas ou aplicações que não utiliza. E quaisquer programas indesejados são executados em segundo plano, ocupando espaço no disco rígido e na memória. Caso não utilize um programa, desinstale-o. Também se aplica a qualquer outro software pré-instalado ou aplicação de teste que se esqueceu de remover.

  > **Importante**
  > Caso suspeite que um programa ou aplicação seja parte essencial de seu sistema operativo, não remova o mesmo e entre em contacto com a Assistência ao Cliente do Bitdefender para obter assistência.

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

  A velocidade do seu sistema e o seu comportamento geral também podem ser afetados pelas ameaças. Spyware, malware, Trojans e adware prejudicam o desempenho do seu dispositivo. Certifique-se de que analisa o seu sistema periodicamente, pelo menos uma vez por semana. Recomendamos a utilização da Análise do Sistema do Bitdefender pois a mesma analisa todos os tipos de ameaças que prejudicam a segurança do seu sistema.

  Para iniciar a Verificação do Sistema:

  1. a
     Clique em **Definições** no menu de navegação na interface do Bitdefender.
  2. No painel **ANTIVÍRUS**, clique em **Abrir**.
  3. Na janela **Análises**, clique em **Executar Análise** ao lado de **Análise do Sistema**.
  4. Siga os passos do assistente.

6.1.2. A análise não inicia

Este tipo de problema pode ter duas causas principais:

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

  Neste caso, reinstale o Bitdefender:

  - No **Windows 7**:

    1. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
    2. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
    3. Clique em **REINSTALAR** na janela que aparece.
    4. Aguarde pela conclusão do processo de reinstalação e reinicie o sistema.

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

    1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
    2. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
    3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
    4. Clique em **REINSTALAR** na janela que aparece.
    5. Aguarde pela conclusão do processo de reinstalação e reinicie o sistema.

  - No **Windows 10**:

    1. Clique em **Iniciar**, em seguida, clique em Definições.
    2. Clique no ícone **Sistema** na área das Definições, em seguida, selecione **Aplicações instaladas**.
    3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
    4. Clique em **Desinstalar** novamente para confirmar a sua escolha.
    5. Clique em **REINSTALAR** na janela que aparece.
    6. Aguarde pela conclusão do processo de reinstalação e reinicie o sistema.

Nota
Ao seguir este procedimento de reinstalação, as definições personalizadas são guardadas e estão disponíveis no novo produto instalado. As outras definições podem ser alteradas novamente para a configuração predefinida.

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

  Neste caso:

  1. Remover a outra solução de segurança. Para mais informação, dirija-se a "*Como posso remover outras soluções de segurança?*" (p. 68).
  2. Reinstalar Bitdefender:
     - No **Windows 7**:
       a. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
       b. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
       c. Clique em **REINSTALAR** na janela que aparece.
       d. Aguarde pela conclusão do processo de reinstalação e reinicie o sistema.
     - No **Windows 8 e Windows 8.1**:
       a. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
       b. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
       c. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
       d. Clique em **REINSTALAR** na janela que aparece.
       e. Aguarde pela conclusão do processo de reinstalação e reinicie o sistema.
     - No **Windows 10**:
       a. Clique em **Iniciar**, em seguida, clique em Definições.
       b. Clique no ícone **Sistema** na área das Definições, em seguida, selecione **Aplicações instaladas**.

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

d. Clique em **Desinstalar** novamente para confirmar a sua escolha.

e. Clique em **REINSTALAR** na janela que aparece.

f. Aguarde pela conclusão do processo de reinstalação e reinicie o sistema.

Nota
Ao seguir este procedimento de reinstalação, as definições personalizadas são guardadas e estão disponíveis no novo produto instalado. As outras definições podem ser alteradas novamente para a configuração predefinida.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 302).

6.1.3. Já não posso utilizar uma aplicação

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

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

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

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

Advanced Threat Defense é uma funcionalidade do Bitdefender que monitoriza constantemente as aplicações executadas no seu sistema e comunica o comportamento potencialmente malicioso. Como esta funcionalidade se baseia num sistema heurístico, pode haver casos em que as aplicações legítimas são comunicadas pelo Advanced Threat Defense.

Quando isso acontecer, poderá excluir a respectiva aplicação para que não seja monitorizada pela Defesa Avançada Contra Ameaças.

Para adicionar o programa à lista de exceções:

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

2. No painel **ADVANCED THREAT DEFENSE**, clique em **Abrir**.
3. Na janela **Definições**, clique em **Gerir exceções**.
4. Clique em **+Adicionar uma Exceção**.
5. Introduza o caminho do executável que deseja adicionar à lista de exceção da verificação no campo correspondente.

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

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 302).

6.1.4. O que fazer quando a Bitdefender bloqueia um site, domínio, endereço de IP ou aplicação online segura

O Bitdefender oferece uma experiência de navegação Web segura filtrando todo o tráfego da rede e bloqueando os conteúdos maliciosos. No entanto, é possível que o Bitdefender considere um site, domínio, endereço de IP ou aplicação online seguros como inseguros, o que fará com que a análise de tráfego HTTP da Bitdefender os bloqueie incorretamente.

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

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

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **PREVENÇÃO CONTRA AMEAÇAS ONLINE**, clique em **Definições**.
3. Clique em **Gerir exceções**.
4. Clique em **+Adicionar uma Exceção**.
5. No campo correspondente, escreva o nome do site, do domínio ou do endereço IP que deseja adicionar às excepções.
6. Clique no botão ao lado de **Prevenção de Ameaças Online**.
7. Clique em **Guardar** para guardar as alterações e fechar a janela.

Apenas sites, domínios, endereços de IP e aplicações nos quais confia plenamente devem ser adicionados à lista. Estes serão excluídos da análise pelos seguintes mecanismos: ameaças, phishing e fraude.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 302).

6.1.5. Não consigo ligar-me à Internet

Poderá verificar que um programa ou navegador da web já não consegue ligar à Internet ou aceder aos serviços em rede após a instalação do Bitdefender.

Neste caso, a melhor solução é configurar o Bitdefender para permitir automaticamente as ligações de e para a respetiva aplicação de software:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel do **FIREWALL**, clique em **Definições**.
3. Na janela **Regras**, clique em **Adicionar regra**.
4. Uma nova janela aparece onde possa adicionar os detalhes. Certifique-se de que seleciona todos os tipos de rede disponíveis e na seção **Permissão** seleciona **Permitir**.

Feche o Bitdefender, abra a aplicação de software e tente de novo ligar-se à Internet.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 302).

6.1.6. Não consigo aceder a um dispositivo na minha rede

Dependendo da rede a que está ligado, a firewall do Bitdefender poderá bloquear a ligação entre o seu sistema e outro dispositivo (como outro PC ou uma impressora). Como resultado, já não poderá partilhar ou imprimir ficheiros.

Neste caso, a melhor solução é configurar o Bitdefender para permitir automaticamente as ligações de e para o respetivo dispositivo como se segue:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel do **FIREWALL**, clique em **Definições**.

3. Na janela **Regras**, clique em **Adicionar regra**.
4. Ative a opção **Aplicar esta regra a todas as aplicações**.
5. Clique no botão **Configuração Avançada** .
6. Na caixa **Endereço remoto personalizado**, digite o endereço de IP do PC ou da impressora aos quais deseja ter acesso ilimitado.

Se ainda não conegue ligar-se ao dispositivo, a incidência poderá não ser causada pelo Bitdefender.

Procure por outras potenciais causas, tais como as seguintes:

- O Firewall do outro dispositivo pode bloquear a partilha de ficheiros e impressoras com o seu PC.
  - Se a Firewall do Windows estiver a utilizada, pode ser configurada para permitir a partilha de ficheiros e impressora da seguinte forma:
    - No **Windows 7**:
      1. Clique em **Iniciar**, aceda ao **Painel de Controlo** e selecione **Sistema e Segurança**.
      2. Aceda a **Firewall do Windows** e, em seguida, clique em **Permitir um programa através da Firewall do Windows**.
      3. Selecione a caixa de verificação **Partilha de ficheiros e impressoras**.
    - No **Windows 8 e Windows 8.1**:
      1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
      2. Clique em **Sistema e Segurança**, aceda a **Firewall do Windows** e selecione **Deixar uma aplicação passar pela Firewall do Windows**.
      3. Selecione a caixa de verificação **Partilha de ficheiros e impressoras** e, em seguida, clique em **OK**.
    - No **Windows 10**:
      1. Introduza "Permitir uma aplicação através do Firewall do Windows" na caixa de pesquisa da barra de tarefas e clique no ícone correspondente.
      2. Clique em **Alterar definições**.

3. Na lista **Aplicações e recursos permitidos**, selecione a caixa de verificação **Partilha de Ficheiros e Impressoras** e, em seguida, clique em **OK**.

- Se outro programa de firewall estiver a ser utilizado, por favor consulte a documentação e ficheiro de ajuda.

- Condições gerais que podem impedir a utilização ou conexão com a impressora compartilhada:
  - Poderá precisar de se ligar com uma conta de administrador do Windows para aceder à impressora compartilhada.
  - As permissões são definidas para a impressora partilhada para permitir acesso a um dispositivo específico e apenas utilizadores. Se está a partilhar a sua impressora, verifique as permissões definidas para a impressora para saber se o utilizador do outro dispositivo está autorizado a aceder à impressora. Se está a tentar ligar-se a uma impressora partilhada, verifique com o utilizador do outro dispositivo se tem permissão para se ligar com a impressora.
  - A impressora ligada ao seu dispositivo ou ao outro não é partilhada.
  - A impressora partilhada não está adicionada ao dispositivo.

  Nota
  Para aprender como gerir o compartilhamento de impressoras (compartilhar uma impressora, definir ou remover permissões para a impressora, conecta-se a uma rede de impressora ou a uma impressora partilhada), vá à Ajuda e Suporte do Windows (no menu Iniciar, clique em **Ajuda e Suporte**).

- O acesso a uma impressora em rede pode ser restringido a dispositivo ou apenas a utilizadores. Deverá verificar com o administrador da rede se tem ou não permissão para aceder à impressora.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 302).

6.1.7. A minha Internet está lenta

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

Para resolver esta situação:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel da **FIREWALL**, clique no botão desligar para desativar a função.
3. Verifique se a sua ligação à Internet melhorou com a firewall do Bitdefender desativada.
   - Se ainda tem uma ligação à Internet lenta, a incidência poderá não ser causada pelo Bitdefender. Deve contactar o seu Fornecedor de Serviço de Internet para confirmar se a ligação está operacional.

     Se receber a confirmação do seu Fornecedor de Serviços de Internet que a ligação está operacional e o problema persistir, contacte a Bitdefender como indicado na secção "*Pedir Ajuda*" (p. 302).
   - Se a ligação à Internet melhorou depois de desativar a firewall do Bitdefender:
     a. Clique em **Definições** no menu de navegação na interface do Bitdefender.
     b. No painel do **FIREWALL**, clique em **Definições**.
     c. Vá para o separador **Adaptadores de Rede** e configure sua ligação com a internet como **Doméstica/Escritório**.
     d. Na janela **Configurações**, desative a **Proteção de análise de porta**.

        Na área **Modo Sigiloso**, clique em **Editar definições sigilosas**. Ative o modo furtivo para o adaptador de rede ao qual está ligado.
     e. Feche o Bitdefender, reinicie o sistema e verifique a velocidade de ligação à Internet.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 302).

6.1.8. Como atualizar o Bitdefender numa ligação à Internet lenta

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

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

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

2. Selecione o separador **Atualizar**.
3. Desligar o botão **Atualização silenciosa**.
4. A próxima vez que uma atualização estiver disponível, ser-lhe-á pedido para selecionar a atualização que deseja descarregar. Selecionar apenas **Atualização de assinaturas**.
5. O Bitdefender transfere e instala apenas a base de dados de informações de ameaças.

6.1.9. Os serviços Bitdefender não estão a responder

Este artigo ajuda-o a troubleshoot os erros de**Os Serviços Bitdefender não estão a responder**. Pode encontrar esse erro da seguinte forma:

- O ícone Bitdefender na Barra de Notificação está a cinzento e é informado que os serviços do Bitdefender não estão a responder.
- A janela do Bitdefender indica que os serviços do Bitdefender não estão a responder.

O erro pode ter ocorrido devido a um dos seguintes fatores:

- problemas temporários de comunicação entre os serviços da Bitdefender.
- alguns dos serviços da Bitdefender estão parados.
- outras soluções de segurança em execução no seu dispositivo, ao mesmo tempo que o Bitdefender.

Para solucionar este erro, tente estas soluções:

1. Espere uns momentos e verifique se existe alguma alteração. Este erro pode ser temporário.
2. Reinicie o dispositivo e aguarde alguns momentos até o Bitdefender iniciar. Abra o Bitdefender e veja se o erro se mantém. Reiniciar o dispositivo normalmente resolve o problema.
3. Verifique se tem qualquer outra solução de segurança instalada na medida em que possam interferir no funcionamento normal do Bitdefender. Se for este o caso, recomendamos que remova todas as outras soluções de segurança e reinstale Bitdefender.

   Para mais informação, dirija-se a "*Como posso remover outras soluções de segurança?*" (p. 68).

Se o erro persistir, por favor contacte os nossos representantes do suporte conforme descrito na secção "*Pedir Ajuda*" (p. 302).

6.1.10. O filtro Antispam não está a funcionar corretamente

Este artigo ajuda a solucionar os seguintes problemas relacionados com a operação de filtragem do Antispam do Bitdefender:

- Um número de mensagens de e-mail legítimas são marcadas como [spam].
- Muitas mensagens spam não estão marcadas de acordo com o filtro antispam.
- O filtro antispam não deteta qualquer mensagem de spam.

Mensagens legítimas são marcadas como [spam]

Mensagens legítimas são marcadas como [spam] simplesmente porque elas parecem spam para o filtro antispam do Bitdefender. Pode normalmente resolver este problema ao configurar adequadamente o filtro Antispam.

O Bitdefender adiciona automaticamente os remetentes das suas mensagens de e-mail à Lista de Amigos. As mensagens de e-mail recebidas dos contactos na lista de Amigos são consideradas legítimas. Elas não são verificadas pelo filtro antispam e, deste modo, elas nunca são marcadas como [spam].

A configuração automática da lista de Amigos não impede a deteção de erros que podem ocorrer nestas situações:

- Recebeu muitos e-mails publicitários solicitados como resultado de se inscrever em vários sites. Neste caso, a solução é adicionar à Lista de Amigos o endereço de e-mail do qual recebeu esses e-mails.
- Uma parte significativa dos seus mails legítimos são de pessoas com quem nunca trocou e-mails antes, tais como clientes, potenciais parceiros empresariais e outros. Outras soluções são requeridas neste caso.

  Se estiver a utilizar um cliente de email com o qual o Bitdefender é compatível, indique erros de deteção.

> **Nota**
> O BiDefender integra uma barra antispam de facil utilização, nos clientes de email mais comuns. Para ver a lista completa de clientes de e-mail suportados, por favor consulte o "*Clientes de email e protocolos suportados*" (p. 97).

Adicionar contactos à Lista de Amigos

Se está a utilizar um cliente de mail suportado, pode facilmente adicionar os remetentes das mensagens legítimas à lista de Amigos. Siga os seguintes passos:

1. No seu cliente de mail, selecione a mensagem de e-mail do remetente que quer adicionar à lista de Amigos.
2. Clique no botão **Adicionar Amigos** da barra de tarefas antispam do Bitdefender.
3. Poderá ser convidado a reconhecer os endereços adicionados à lista de Amigos. Selecione **Não mostrar esta mensagem outra vez** e clique **OK**.

Irá sempre receber mensagens de e-mail destes endereços, independentemente do conteúdo da mensagem.

Se está a utilizar um cliente de mail diferente, poderá adicionar os contactos à lista Amigos a partir do interface do Bitdefender. Siga os seguintes passos:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTISPAM**, clique em **Gerir amigos**.

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

Indique os erros de deteção

Se estiver a usar um cliente de e-mail suportado, pode facilmente corrigir o filtro antispam (indicando mensagens de correio eletrónico que não deveriam ter sido marcadas como[spam]). Se o fizer, ajuda a melhorar a eficiência do filtro antispam. Siga os seguintes passos:

1. Abra o mail de cliente.
2. Vá à pasta de lixo eletrónico, para onde são movidas as mensagens.
3. Selecione a mensagem legítima incorretamente marcada como [spam] pelo Bitdefender.
4. Clique no botão **Adicionar Amigos** da barra de tarefas antispam do Bitdefender para adicionar o remetente à lista de Amigos. Pode necessitar

de clicar em **OK** para confirmar. Irá sempre receber mensagens de e-mail destes endereços, independentemente do conteúdo da mensagem.

5. Clique no botão **Não Spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de mail do cliente). A mensagem de email será movida para a pasta de Entrada.

Muitas mensagens de spam não são detetadas

Se está a receber muitas mensagens spam que não estão marcadas como [spam], tem de configurar o filtro antispam Bitdefender de modo a melhorar a sua eficiência.

Tente as seguintes soluções:

1. Se estiver a utilizar um cliente de email com o qual o Bitdefender é compatível, indique mensagens de spam não detetadas.

   Nota

   O BiDefender integra uma barra antispam de facil utilização, nos clientes de email mais comuns. Para ver a lista completa de clientes de e-mail suportados, por favor consulte o *"Clientes de email e protocolos suportados" (p. 97)*.

2. Adicione spammers à lista de Spammers. As mensagens de e-mail recebidas dos endereços na lista de Spammers são automaticamente marcadas como [spam].

Indica mensagens de spam não detetadas

Se estiver a utilizar um cliente de e-mail suportado, pode facilmente indicar quais as mensagens de e-mail que devem ser detectadas como spam. Se o fizer, ajuda a melhorar a eficiência do filtro antispam. Siga os seguintes passos:

1. Abra o mail de cliente.
2. Vá à pasta Caixa de Entrada.
3. Selecione as mensagens spam não detetadas
4. Clique no botão **É Spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de email do cliente). São imediatamente marcadas como [spam] e movidas para a pasta de lixo electrónico.

Adicionar spammers à lista de Spammers

Se está a utilizar um cliente de mail suportado, pode facilmente adicionar os remetentes das mensagens spam à lista Spammers. Siga os seguintes passos:

1. Abra o mail de cliente.
2. Vá à pasta de lixo eletrónico, para onde são movidas as mensagens.
3. Selecione a mensagem marcada como [spam] pelo Bitdefender.
4. Clique no botão **Adicionar Spammer** da barra de tarefas antispam do Bitdefender.
5. Poderá ser convidado a reconhecer os endereços como Spammers. Selecione **Não mostrar esta mensagem outra vez** e clique **OK**.

Se está a utilizar um cliente de mail diferente, poderá adicionar manualmente os spammers à lista de Spammers a partir do interface do Bitdefender. É conveniente que o faça apenas quando receber várias mensagens spam do mesmo endereço e-mail. Siga os seguintes passos:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. No painel **ANTISPAM**, clique em **Definições**.
3. Vá para a janela **Gerir Spammers**.
4. Digite o endereço de email do spammer e depois clique em **Adicionar**. Pode adicionar quantos endereços de email desejar.
5. Clique em **OK** para guardar as alterações e fechar a janela.

O Filtro Antispam não deteta nenhuma mensagem spam

Se nenhuma mensagem spam for marcada como [spam], poderá haver algum problema como o filtro Antispam do Bitdefender. Antes de resolver este problema, certifique-se de que não é causado por nenhuma das seguintes condições:

- A proteção antispam poderá estar desligada. Para verificar o estado da proteção antispam, clique em **Proteção** no menu de navegação da interface do Bitdefender. Verifique o painel **Antispam** para comprovar se a função está ativa

  Se o Antispam estava desligado, era isso que estava a causar o problema. Clique no botão correspondente para ativar a sua proteção antispam.

- A proteção de Antispam do Bitdefender está disponível apenas para clientes de correio eletrónico configurado para receber mensagens de e-mail via protocolo POP3. Isto significa o seguinte:
  - As mensagens de Email obtidas através de Webmail (Yahoo, Gmail, Hotmail ou outros) não são filtradas como spam pelo Bitdefender.
  - Se o seu cliente de e-mail está configurado para receber mensagens de e-mail usando outro protocolo que não o POP3 (por exemplo, IMAP4), o filtro Antispam do Bitdefender não as analisará à procura de spam.

  Nota

  POP3 é um dos protocolos mais utilizados para fazer o download de mensagens de e-mail a partir de um servidor de correio. Se você não sabe o protocolo que o seu cliente de e-mail utiliza para importar mensagens de e-mail, solicite à pessoa que o configurou.

- O Bitdefender Total Security não analisa o tráfego POP3 do Lotus Notes.

Uma solução possivel é reparar ou reinstalar o produto. Contudo, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 302).

6.1.11. A funcionalidade Preenchimento automático na minha Carteira não funciona

Guardou as suas credenciais online no seu Gestor de Palavras-passe do Bitdefender e constatou que o preenchimento automático não está a funcionar. Normalmente, este problema surge quando a extensão da Carteira do Bitdefender não está instalada no seu browser.

Para resolver esta situação, siga estes passos:

- No **Internet Explorer:**
  1. Abra o Internet Explorer.
  2. Clique em Ferramentas.
  3. Clique em Gerir suplementos.
  4. Clique em Ferramentas e Extensões.
  5. Consulte **Portfólio do Bitdefender** e clique em **Ativar**.
- No **Mozilla Firefox:**

1. Abra o Mozilla Firefox.
2. Clique no botão **Abrir menu** no canto superior direito do ecrã.
3. Clique em Suplementos.
4. Clique em Extensões.
5. Vá à **Carteira do Bitdefender** e clique no interruptor ao lado dela.

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

Nota
O suplemento será ativado após reiniciar o browser.

Agora verifique se a funcionalidade de preenchimento automático na Carteira está a funcionar para as suas contas online.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 302).

6.1.12. Remoção de Bitdefender falhou

Caso pretenda remover o seu produto Bitdefender e constate que o processo demora ou o sistema bloqueia, clique em **Cancelar** para interromper a ação. Se isso não funcionar, reinicie o sistema.

Se a remoção falhar, algumas chaves de registo e ficheiros do Bitdefender poderão permanecer no seu sistema. Esses resquícios podem impedir uma nova instalação do Bitdefender. Podem também afectar o desempenho e a estabilidade do sistema.

Para remover o Bitdefender completamente do seu sistema:

- No **Windows 7**:
  1. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
  2. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.

3. Clique em **REMOVER** na janela que aparece.
4. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

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

1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
2. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
4. Clique em **REMOVER** na janela que aparece.
5. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

- No **Windows 10**:

1. Clique em **Iniciar**, em seguida, clique em Definições.
2. Clique no ícone **Sistema** na área das Definições, em seguida, selecione **Aplicações instaladas**.
3. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
4. Clique em **Desinstalar** novamente para confirmar a sua escolha.
5. Clique em **REMOVER** na janela que aparece.
6. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

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

Se instalou o Bitdefender e não consegue reiniciar o seu sistema no modo normal, podem existir vários motivos para este problema.

Isto é muito provavelmente causado por uma instalação anterior de Bitdefender que não foi removida adequadamente ou por outra solução de segurança que ainda se encontra no sistema.

Eis como pode resolver cada situação:

- **Você tinha o Bitdefender anteriormente e não o removeu corretamente.**

Para resolver isto:

1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como o fazer, consulte "*Como posso reiniciar no Modo de Segurança?*" (p. 69).
2. Remove Bitdefender do seu sistema:
   - No **Windows 7**:
     a. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
     b. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
     c. Clique em **REMOVER** na janela que aparece.
     d. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.
     e. Reinicie o sistema no modo normal.
   - No **Windows 8 e Windows 8.1**:
     a. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
     b. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
     c. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
     d. Clique em **REMOVER** na janela que aparece.
     e. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.
     f. Reinicie o sistema no modo normal.
   - No **Windows 10**:
     a. Clique em **Iniciar**, em seguida, clique em Definições.
     b. Clique no ícone **Sistema** na área das Definições, em seguida, selecione **Aplicações instaladas**.
     c. Encontre o **Bitdefender Total Security** e selecione **Desinstalar**.
     d. Clique em **Desinstalar** novamente para confirmar a sua escolha.
     e. Clique em **REMOVER** na janela que aparece.

f. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

g. Reinicie o sistema no modo normal.

3. Reinstale o seu produto Bitdefender

- **Você tinha uma solução de segurança diferente anteriormente e não a eliminou corretamente.**

  Para resolver isto:

  1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como o fazer, consulte "*Como posso reiniciar no Modo de Segurança?*" (p. 69).
  2. Remova as outras soluções de segurança do seu sistema:
     - No **Windows 7**:
       a. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
       b. Encontre o nome do programa que pretende remover e selecione **Remover**.
       c. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.
     - No **Windows 8 e Windows 8.1**:
       a. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
       b. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
       c. Encontre o nome do programa que pretende remover e selecione **Remover**.
       d. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.
     - No **Windows 10**:
       a. Clique em **Iniciar**, em seguida, clique em Definições.
       b. Clique no ícone **Sistema** na área das Definições, em seguida, selecione **Aplicações instaladas**.

c. Encontre o nome do programa que pretende remover e selecione **Desinstalar**.

d. Aguarde pela conclusão do processo de desinstalação e reinicie o sistema.

Para desinstalar corretamente outro software, aceda ao site Web do fornecedor e execute a ferramenta de desinstalação ou contacte-o para diretamente, para que lhe indiquem os procedimentos de desinstalação.

3. Reinicie o seu sistema no modo normal e reinstale o Bitdefender.

Já seguiu os passos acima e o problema não está resolvido.

Para resolver isto:

1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como o fazer, consulte "*Como posso reiniciar no Modo de Segurança?*" (p. 69).
2. Utilizar a opção de Restauração do Sistema do Windows para restaurar o dispositivo para uma data anterior antes de instalar o produto Bitdefender.
3. Reinicie o sistema no modo normal e contacte os nossos representantes do suporte conforme descrito na secção "*Pedir Ajuda*" (p. 302).

6.2. Remover ameaças do seu sistema

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

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

- "*Ambiente de Resgate*" (p. 187)
- "*O que fazer quando o Bitdefender encontra ameaças no seu dispositivo?*" (p. 188)
- "*Como posso limpar uma ameaça num ficheiro?*" (p. 189)
- "*Como posso limpar uma ameaça num ficheiro de e-mail?*" (p. 190)
- "*O que fazer se suspeitar que um ficheiro é perigoso?*" (p. 191)

- "*O que são os ficheiros protegidos por palavra-passe no relatório de análise?*" (p. 192)
- "*O que são os itens ignorados no relatório de análise?*" (p. 192)
- "*O que são os ficheiros muito comprimidos no relatório de análise?*" (p. 192)
- "*Por que é que Bitdefender eliminou automaticamente um ficheiro infectado?*" (p. 193)

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 "*Pedir Ajuda*" (p. 302).

6.2.1. Ambiente de Resgate

O **Modo de Recuperação** é uma funcionalidade do Bitdefender que permite analisar e desinfetar todas as partições existentes do disco rígido dentro e fora do sistema operativo.

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

Arranque do sistema no Ambiente de Recuperação

Só pode aceder ao Ambiente de Recuperação a partir do produto Bitdefender como se segue:

1. Clique em **Definições** no menu de navegação na 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 Recuperação do Bitdefender é carregado dentro de momentos.

Analisar o seu sistema no Ambiente de Recuperação

Para analisar o seu sistema no Ambiente de Recuperação:

1. Aceda ao Ambiente de Recuperação como descrito em "Arranque do sistema no Ambiente de Recuperação" (p. 187).
2. O processo de análise do Bitdefender começa automaticamente assim que o sistema é carregado no Ambiente de Recuperação.

3. Aguarde que a análise termine. Se for detetada qualquer ameaça, siga as instruções para a remover.
4. Para sair do Ambiente de Recuperação, clique no botão **Fechar** na janela com os resultados da análise.

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

Pode descobrir que há uma ameaça no seu dispositivo numa dessas formas:

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

Nessas situações, atualize o Bitdefender para se certificar de que possui a base de dados mais recente de informações sobre a ameaça e realize uma Análise de Sistema.

Assim que a análise do sistema terminar, selecione a ação pretendida para os itens infetados (Desinfetar, Eliminar, Mover para a Quarentena).

Atenção
Se suspeitar que o ficheiro faz parte do sistema operativo do Windows ou que não é um ficheiro infectado, não siga estes passos e contacte e Apoio ao Cliente do Bitdefender assim que possível.

Se não for possível efetuar a ação selecionada e o relatório da análise indicar uma infecção que não foi possível eliminar, tem de remover o(s) ficheiro(s) manualmente:

O primeiro método pode ser utilizado no modo normal:

1. Desative a proteção antivírus em tempo real do Bitdefender:
   a. Clique em **Definições** no menu de navegação na 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 como o fazer, consulte "*Como posso mostrar objetos ocultos no Windows?*" (p. 67).

3. Procure a localização do ficheiro infectado (veja no relatório da análise) e elimine-o.
4. Ligue a proteção antivírus em tempo real do Bitdefender.

Caso o primeiro método para remover a infeção falhe:

1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como o fazer, consulte "*Como posso reiniciar no Modo de Segurança?*" (p. 69).
2. Mostrar objetos ocultos no Windows. Para saber como o fazer, consulte "*Como posso mostrar objetos ocultos no Windows?*" (p. 67).
3. Procure a localização do ficheiro infectado (veja no relatório da análise) e elimine-o.
4. Reinicie o seu sistema e inicie sessão no modo normal.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 302).

6.2.3. Como posso limpar uma ameaça num ficheiro?

Um arquivo é um ficheiro ou um conjunto de ficheiros comprimidos num formato especial para reduzir o espaço no disco necessário para armazenar os ficheiros.

Alguns destes formatos são formatos livres, possibilitando ao Bitdefender a opção de analisar o conteúdo e aplicar as ações adequadas para os remover.

Outros formatos de arquivo estão parcial ou totalmente fechados, mas o Bitdefender só pode detetar a presença de ameaças no interior, mas não pode aplicar outras ações.

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

Eis como pode limpar uma ameaça armazenada num arquivo:

1. Identifique o arquivo que inclui a ameaça ao executar uma Análise do Sistema.
2. Desative a proteção antivírus em tempo real do Bitdefender:

a. Clique em **Definições** no menu de navegação na 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 ficheiro infectado.
5. Elimine o arquivo original de modo a garantir que a infecção é totalmente removida.
6. Comprima novamente os ficheiros num novo arquivo com uma aplicação de arquivo, como o WinZip.
7. Ative a proteção antivírus em tempo real do Bitdefender e execute uma análise ao sistema para se certificar que não há outras infeções no sistema.

Nota
É importante observar que uma ameaça armazenada num arquivo não é uma ameaça imediata para o seu sistema pois a ameaça tem de ser descomprimida e executada para infetar o seu sistema.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 302).

6.2.4. Como posso limpar uma ameaça num ficheiro de e-mail?

O Bitdefender também pode identificar ameaças em bases de dados de correio eletrónico e arquivos de correio eletrónico armazenados no disco.

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

Eis como pode limpar uma ameaça armazenada num arquivo de e-mail:

1. Analisar a base de dados do correio eletrónico com o Bitdefender.
2. Desative a proteção antivírus em tempo real do Bitdefender:

a. Clique em **Definições** no menu de navegação na 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 eletrónico.
4. Elimine as mensagens infectadas. A maioria dos clientes de correio eletrónico move a mensagem eliminada para uma pasta de recuperação, a partir da qual pode ser recuperada. Deve certificar-se que a mensagem também é eliminada desta pasta de recuperação.
5. Compactar a pasta com a mensagem infectada.
   - No Microsoft Outlook 2007: No menu Ficheiro, clique em Gestão de Ficheiros de Dados. Selecione os ficheiros das pastas (.pst) que pretende compactar e clique em Definições. Clique em Compactar Agora.
   - No Microsoft Outlook 2010/2013/2016: No menu Ficheiro, clique em Informações e, em seguida, em definições de Conta (Adicionar e remover contas ou alterar as definições de ligação existentes). Clique em Ficheiro de Dados, selecione os ficheiros das pastas (.pst) que pretende compactar e clique em Definições. Clique em Compactar Agora.
6. Ligue a proteção antivírus em tempo real do Bitdefender.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 302).

6.2.5. O que fazer se suspeitar que um ficheiro é perigoso?

Pode suspeitar que um ficheiro do seu sistema é perigoso, embora o seu produto Bitdefender não o tenha detetado.

Para garantir que o seu sistema está protegido:

1. Execute uma **Análise de Sistema** com o Bitdefender. Para saber como o fazer, consulte "*Como posso analisar o seu sistema?*" (p. 46).
2. Se no resultado da análise parece estar limpo, mas você ainda tem dúvidas e quer verificar o ficheiro, contacte os representantes do suporte para que o possamos ajudar.

   Para saber como o fazer, consulte "*Pedir Ajuda*" (p. 302).

6.2.6. O que são os ficheiros protegidos por palavra-passe no relatório de análise?

Isto é apenas uma notificação que indica que o Bitdefender detetou que estes ficheiros estão protegidos por palavra-passe ou por outra forma de encriptação.

Normalmente, os itens protegidos por palavra-passe são:

- Ficheiros que pertencem a outras solução de segurança.
- Ficheiros que pertencem ao sistema operativo.

Para analisar verdadeiramente os conteúdos, estes ficheiros têm de ser extraídos ou descodificados.

Se esses conteúdos pudessem ser extraídos, o analisador em tempo real do Bitdefender analisaria-os automaticamente para manter o seu dispositivo protegido. Se pretende analisar esses ficheiros com o Bitdefender, terá de contactar o fabricante do produto para receber mais informações sobre esses ficheiros.

Recomendamos que ignore estes ficheiros pois não constituem uma ameaça ao seu sistema.

6.2.7. O que são os itens ignorados no relatório de análise?

Todos os ficheiros que aparecem como Ignorados no relatório de análise estão limpos.

Para um melhor desempenho, o Bitdefender não analisa ficheiros que não tenham sido alterados desde a última análise.

6.2.8. O que são os ficheiros muito comprimidos no relatório de análise?

Os itens sobre-comprimidos são elementos que não puderam ser extraídos pelo motor de análise ou elementos para os quais a desencriptação levaria demasiado tempo, tornando o sistema instável.

Sobre-comprimido significa que o Bitdefender não realizou a análise a esse arquivo pois a descompactação iria consumir demasiados recursos do sistema. O conteúdo será analisado aquando o acesso em tempo real, se necessário.

6.2.9. Por que é que Bitdefender eliminou automaticamente um ficheiro infectado?

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

Para determinados tipos de ameaças, a desinfeção não é possível por o ficheiro detetado ser totalmente malicioso. Nestes casos, o ficheiro infectado é eliminado do disco.

Este é, normalmente, o caso de ficheiros de instalação que são transferidos de sites Internet suspeitos. Se se deparar numa situação assim, transfira o ficheiro de instalação do site Internet do fabricante ou de outro site fidedigno.

ANTIVIRUS PARA MAC

7. INSTALAÇÃO E REMOÇÃO

Este capítulo inclui os seguintes tópicos:

7.1. Requisitos de Sistema

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

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

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

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

Como obter a versão do seu macOS e informações de hardware do seu Mac

Clique no ícone Apple no canto superior esquerdo do ecrã e escolha **Sobre este Mac**. Na janela apresentada, pode ver a versão do seu sistema operativo e outras informações úteis. Clique em **Relatório de Sistema** para obter informações detalhadas sobre o hardware.

7.2. A instalar Bitdefender Antivirus for Mac

A aplicação Bitdefender Antivirus for Mac pode ser instalada a partir da sua conta Bitdefender, conforme se segue:

1. Inicie sessão como administrador.
2. Vá para: https://central.bitdefender.com.
3. Inicie sessão na sua conta Bitdefender utilizando o seu endereço de e-mail e palavra-passe.
4. Selecione o painel **Os meus dispositivos**, e clique em **INSTALAR PROTEÇÃO**.

5. Escolha uma das duas opções disponíveis:
   - **Proteger este dispositivo**
     a. Selecione esta opção e, em seguida, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique no botão correspondente.
     b. Guarde o ficheiro de instalação.
   - **Proteger outros dispositivos**
     a. Selecione esta opção e, em seguida, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique no botão correspondente.
     b. Clique em **ENVIAR HIPERLIGAÇÃO DE DOWNLOAD**.
     c. Escreva um endereço de email no campo correspondente e clique em **ENVIAR EMAIL**.

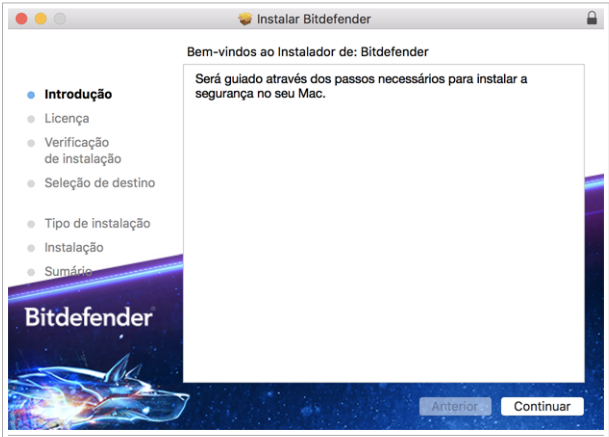
        Observe que a hiperligação de download gerada será válida apenas durante as próximas 24 horas. Se a hiperligação expirar, precisará de gerar uma nova seguindo os mesmos passos.
     d. No dispositivo em que deseja instalar o seu produto Bitdefender, verifique a conta de e-mail que escreveu e clique no botão de download correspondente.
6. Execute o Bitdefender que transferiu.
7. Conclua os passos de instalação.

7.2.1. Processo de instalação

Para instalar o Bitdefender Antivirus for Mac:

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

Passo 1 - Janela de Boas-vindas



Janela de boas-vindas

Clique em **Continuar**.

Passo 2 - Ler o Acordo da Subscrição

Ler o Acordo da Subscrição

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

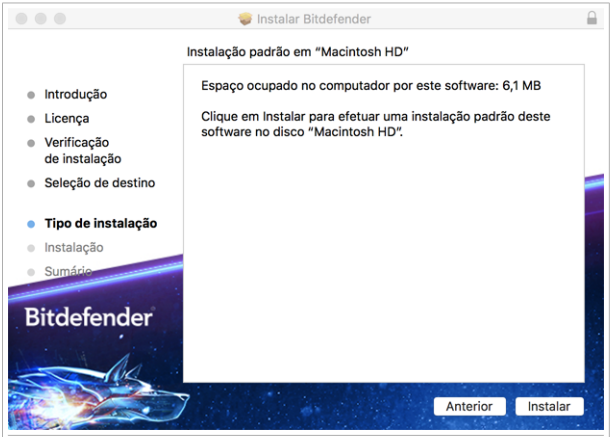
Nesta janela pode também selecionar o idioma em que quer instalar o produto.

Clique em **Continuar** e em **Concordar**.

Importante

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

Passo 3 - Iniciar instalação

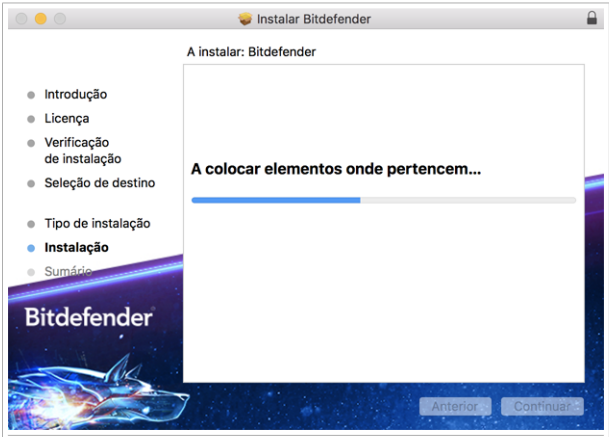


Iniciar instalação

O Bitdefender Antivirus for Mac será instalado em Macintosh HD/Biblioteca/Bitdefender. O caminho da instalação não pode ser modificado.

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

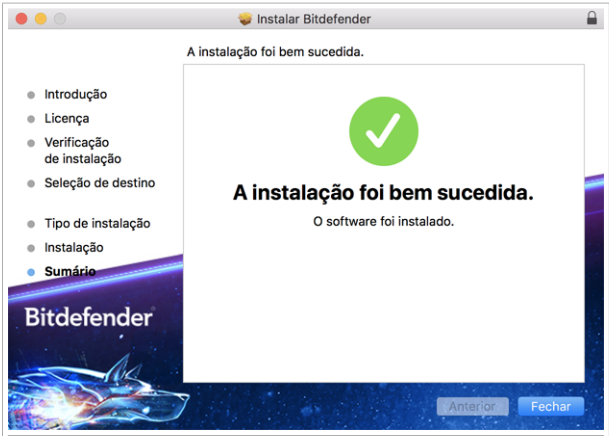
Passo 4 - Instalar o Bitdefender Antivirus for Mac



A instalar Bitdefender Antivirus for Mac

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

Passo 5 - Terminar



Terminar

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

O processo de instalação agora está concluído.

Importante

- Se você está instalando o Bitdefender Antivirus for Mac no macOS versão High Sierra 10.13.0 ou superior, a notificação **System Extension Blocked** é exibida. A notificação informa que as extensões assinadas por Bitdefender foram bloqueadas e devem ser habilitadas manualmente. Clique em **OK** para continuar. Na janela Bitdefender Antivirus for Mac que é exibida, clique no link **Security & Privacy**. Clique em **Permitir** na parte inferior da janela ou selecione o SRL do Bitdefender na lista e, de seguida, cloque em **OK**.
- Se estiver a instalar o Bitdefender Antivirus for Mac no macOS Mojave 10.14 ou numa versão mais recente, será exibida uma nova janela a informar que deve **Conceder acesso total ao disco à Bitdefender** e **Permitir que a Bitdefender carregue**. Siga as instruções no ecrã para configurar corretamente o produto.

7.3. Remover o Bitdefender Antivirus for Mac

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

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

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

Importante

Se ocorrer um erro, pode entrar em contacto com o Atendimento ao Consumidor da Bitdefender, como descrito em “Contacte-nos” (p. 301).

8. INTRODUÇÃO

Este capítulo inclui os seguintes tópicos:

8.1. Sobre o Bitdefender Antivirus for Mac

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

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

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

8.2. A abrir o Bitdefender Antivirus for Mac

Pode abrir o Bitdefender Antivirus for Mac de várias formas.

- Clique no ícone do Bitdefender Antivirus for Mac no Launchpad.
- Clique no ícone na barra de menus e escolha **Abrir Janela Principal**.
- Abra uma janela do Finder, aceda a Aplicações e clique duas vezes no ícone Bitdefender Antivirus for Mac.

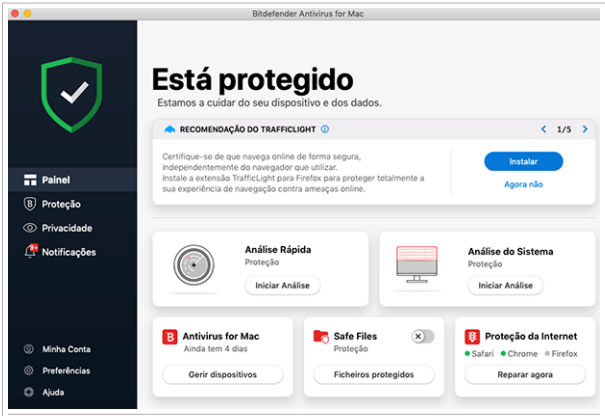
Importante

Przy pierwszym uruchomieniu Bitdefender Antivirus for Mac na macOS Mojave 10.14 lub nowszej wersji pojawia się zalecenie dotyczące ochrony. Esta recomendação aparece porque precisamos de permissões para fazer uma análise completa do seu sistema em busca de ameaças. Para dar permissões, precisa de ter iniciado sessão como administrador e seguir estes passos:

1. Clique na hiperligação **Preferências do Sistema**.
2. Clique no ícone e digite as credenciais de administrador.
3. Uma nova janela aparece. Przeciągnij plik **BDLDaemon** na listę dozwolonych aplikacji.

8.3. Janela principal da aplicação

O Bitdefender Antivirus for Mac vai de encontro às necessidades quer dos principiantes quer dos utilizadores mais técnicos. Assim, o interface gráfico do utilizador foi desenhado para servir quer uns quer outros.



Janela principal da aplicação

Vá à interface do Bitdefender, encontra-se exibido no canto superior esquerdo um assistente de introdução que contém detalhes sobre como interagir com o produto e como o configurar. Selecione o ícone do ângulo direito para continuar a ser guiado ou **Ignorar** para fechar o assistente.

A barra de estado na parte superior da janela informa-o sobre o estado de segurança do sistema utilizando mensagens explícitas e cores sugestivas. Se o Bitdefender Antivirus for Mac não tiver alertas, a barra de estado é

verde. Quando um problema de segurança é detectado, a cor da barra de estado muda para vermelho. Para informações detalhadas sobre problemas e como os reparar, consulte "*Reparar Incidência*" (p. 218).

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 realizar, seja trabalhar ou fazer pagamentos online, o Bitdefender Autopilot fornecerá recomendações contextuais com base na utilização e necessidades do seu dispositivo. Isto irá ajudá-lo a descobrir e beneficiar das vantagens trazidas pelas funcionalidades incluídas na aplicação Bitdefender Antivirus for Mac.

No menu de navegação, à esquerda, pode aceder às secções da Bitdefender para obter a configuração detalhada e tarefas administrativas avançadas (separadores **Proteção** e **Privacidade**), notificações, à sua conta Bitdefender e à área Preferências. Pode também entrar em contacto connosco (separador **Ajuda**) para obter assistência, caso tenha dúvidas ou surja algo inesperado.

8.4. Ícone Dock da aplicação

O ícone do Bitdefender Antivirus for Mac pode ser visto na Dock assim que abrir a aplicação. O ícone na Dock proporciona uma forma fácil de procurar ameaças em ficheiros e pastas. Basta arrastar e largar o ficheiro ou pasta no ícone da Dock e a análise iniciará imediatamente.

Ícone na Dock

8.5. Menu de navegação

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

- **Painel**. A partir daqui, pode resolver rapidamente problemas de segurança, ver recomendações de acordo com os requisitos do seu sistema

e padrões de utilização, realizar ações rápidas, e aceder à sua conta da Bitdefender para gerir os dispositivos que adicionou à sua subscrição da Bitdefender.

- **Proteção**. A partir daqui, pode executar análises de antivírus , adicione ficheiros à lista de exceções, proteger ficheiros e aplicações contra ataques de ransomware, proteger as suas cópias de segurança do Time Machine e configurar a proteção enquanto navega na Internet.
- **Privacidade**. Aqui, pode abrir a aplicação Bitdefender VPN e instale a extensão Anti-tracker no seu browser.
- **Notificações**. A partir daqui, pode ver os detalhes das ações tomadas nos ficheiros analisados.
- **A minha conta**. Daqui, pode aceder à sua conta Bitdefender para verificar as suas subscrições e realizar tarefas de segurança nos dispositivos que controla. Detalhes sobre a conta Bitdefender e subscrição em utilização também estão disponíveis.
- **Privacidade**. A partir daqui, pode configurar as definições da Bitdefender.
- **Ajuda**. Aqui, pode entrar em contacto com o departamento de Assistência Técnica sempre que precisar de ajuda com o seu produto Bitdefender. Pode também enviar feedback para melhorar o produto.

8.6. Modo Escuro

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


Bitdefender Antivirus for Mac
Está protegido
Estamos a cuidar do seu dispositivo e dos dados.
RECOMENDAÇÃO DE ANÁLISE DO SISTEMA
1/4
Vamos realizar uma verificação única do seu dispositivo completo para nos certificarmos de que ele está livre de ameaças. Todas as montagens ligadas também serão verificadas.
Análise
Agora não
Painel
Proteção
Privacidade
Notificações
Análise Rápida
Proteção
Iniciar Análise
Análise do Sistema
Proteção
Iniciar Análise
Minha Conta
Preferências
Ajuda
Family Pack
Ainda tem 594 dias
Gerir dispositivos
Safe Files
Proteção
Ficheiros protegidos
Proteção da Internet
Safari
Reparar agora

Modo Escuro

9. PROTEGER CONTRA SOFTWARE MALICIOSO

Este capítulo inclui os seguintes tópicos:

9.1. Dicas de Utilização

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

- Mantenha o **Bitdefender Escudo** ligado para permitir que os ficheiros do sistema sejam verificados automaticamente pelo Bitdefender Antivirus for Mac.
- Mantenha o seu Bitdefender Antivirus for Mac atualizado com as informações sobre as ameaças e atualizações de produto mais recentes.
- Verifique e repare os problemas relatados pelo Bitdefender Antivirus for Mac regularmente. Para informação detalhada dirija-se a "*Reparar Incidência*" (p. 218).
- Verifique o registo detalhado de eventos referentes à atividade do Bitdefender Antivirus for Mac no seu computador. Sempre que algo relevante para a segurança do seu sistema ou dados acontecer, é

adicionada uma nova mensagem à área de notificações de Bitdefender. Para mais detalhes, aceda a "*Notificações*" (p. 220).

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

  A forma mais fácil de analisar um ficheiro, pasta ou volume é arrastar&largar na janela ou ícone do Bitdefender Antivirus for Mac na Dock.

Nenhuma outra configuração ou ação é necessária. No entanto, se pretender, é possível ajustar as definições e preferências da aplicação para melhor satisfazer as suas necessidades. Para mais informação, dirija-se a "*Configurar preferências*" (p. 223).

9.2. Analisar o seu Mac

Além da funcionalidade **Escudo da Bitdefender**, que monitoriza regularmente as aplicações instaladas à procura de ações típicas de ameaças e previne que novas ameaças de malware entrem no seu sistema, pode analisar o seu Mac ou ficheiros específicos sempre que quiser.

A forma mais fácil de analisar um ficheiro, pasta ou volume é arrastar&largar na janela ou ícone do Bitdefender Antivirus for Mac na Dock. O assistente de análise aparece e orienta-o pelo processo de análise.

Também pode iniciar uma análise como se segue:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. Selecione o separador **Antivirus**.
3. Clique num dos três botões para iniciar a análise desejada.
   - **Análise Rápida** - procura por ameaças nos locais mais vulneráveis no seu sistema (por exemplo, as pastas que contêm os documentos, transferências, transferências de e-mail e ficheiros temporários de cada utilizador).
   - **Análise de Sistema** - realiza uma busca completa por ameaças em todo o sistema. Todas as montagens ligadas também serão analisadas.

Nota

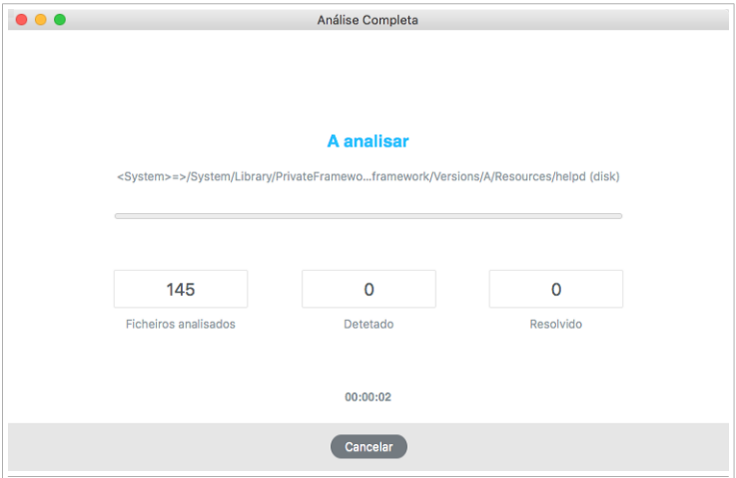
Dependendo do tamanho do seu disco rígido, analisar todo o sistema pode demorar (até uma hora ou mais). Para um desempenho melhor, é recomendável não executar esta tarefa ao executar outras tarefas intensivas (como edição de vídeo).
Se preferir, pode optar por não analisar volumes montados específicos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

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

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

9.3. Assistente de Análise

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



Análise em progresso

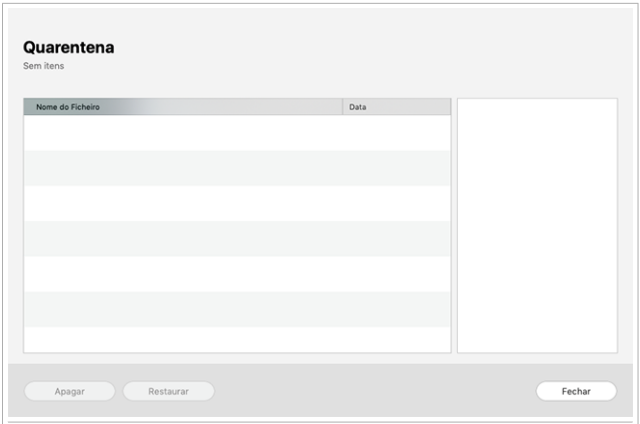
Informações em tempo real sobre as ameaças detetadas e resolvidas são apresentadas durante cada análise.

Espere que o Bitdefender Antivirus for Mac termine a análise.

Nota
O processo de análise pode demorar algum tempo, dependendo da complexidade da mesma.

9.4. Quarentena

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



Ficheiros em quarentena

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

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

Para visualizar a lista de itens adicionados à quarentena:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. É aberta a janela **Antivírus**.

   Clique em **Abrir** no painel de **Quarentena**.

9.5. Escudo da Bitdefender (proteção em tempo real)

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

Para desativar a proteção em tempo real:

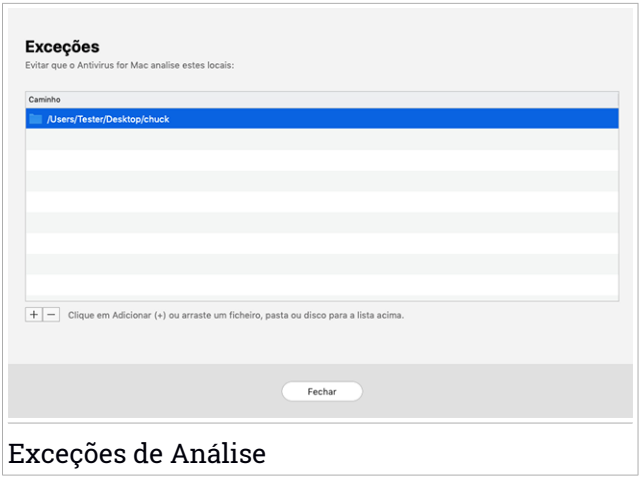
1. Clique em **Preferências** no menu de navegação da interface da Bitdefender.
2. Desative o **Bitdefender Shield** na janela de **Proteção**.

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

9.6. Exceções de Análise

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

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



Exceções de Análise

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

Para aceder à lista de exceções:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. É aberta a janela **Antivírus**.

   Clique em **Abrir** no painel de **Exceções**.

Há duas formas de configurar uma exceção de análise:

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

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

9.7. Proteção da Internet

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

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

Ativar extensões do TrafficLight

Para ativar as extensões do TrafficLight:

1. Clique em **Resolver agora** no cartão de **Proteção web** no Painel de Controlo.
2. É aberta a janela **Proteção na Web**.

   O navegador detetado que tem instalado no seu sistema aparecerá. Para instalar a extensão do TrafficLight no seu browser, clique em **Obter Extensão**.
3. Vai ser redirecionado para:

   https://bitdefender.com/solutions/trafficlight.html
4. Selecione **Transferência gratuita**.
5. Siga os passos para instalar a extensão do TrafficLight correspondente ao seu browser.

Gerir definições da extensões

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

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

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

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

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

Classificação de página e alertas

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

Esta página é segura. Pode continuar com o seu trabalho.
Esta página web pode conter conteúdo perigoso. Tenha cuidado se decidir visitá-la.
Deve sair da página imediatamente, pois contém malware ou outras ameaças.

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

9.8. Antitracker

Uma grande parte dos sites que utiliza monitorizadores para recolher informação sobre o seu comportamento para compartilhar com empresas ou para mostrar publicidade direcionada para si. Devido a isso, os donos dos sites ganham dinheiro por proporcionar conteúdo de graça ou para continuarem a funcionar. Além de recolher informação, os monitorizadores podem desacelerar a sua navegação ou desperdiçar a sua banda larga.

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

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

- Google Chrome
- Mozilla Firefox
- Safari

Os monitorizadores que detectamos estão divididos nas seguintes categorias:

- **Publicidade** - utilizada para analisar o tráfego do site, o comportamento do utilizador ou os padrões de tráfego dos visitantes.
- **Interação com o cliente** - utilizados para medir a interação com o utilizador através de diferentes formas de entrada, como chat ou suporte.
- **Essenciais** - utilizados para monitorizar funcionalidades críticas do site.

- **Analíticas do site** - utilizadas para recolher dados sobre a utilização do site.
- **Redes Sociais** - utilizados para monitorizar o público em redes sociais, as suas atividades e o envolvimento dos utilizadores nas diferentes plataformas de redes sociais.

Activar o Bitdefender Anti-tracker

Para activar a extensão Bitdefender Anti-tracker no seu browser:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. Selecione o separador **Anti-tracker**.
3. Clique **Permitir extensão** no browser em que pretende activar a extensão.

9.8.1. Interface do Antitracker

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

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

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

9.8.2. Desligar o Antitracker da Bitdefender

Para desligar o Bitdefender Anti-tracker no seu browser:

1. Abra o seu navegador web.
2. Clique no ícone ao lado da barra de endereços no seu navegador.

3. Clique no ícone no canto superior direito.
4. Utilize o interruptor correspondente para o desativar.

   O ícone da Bitdefender fica cinzento.

9.8.3. Permitir a monitorização de um site

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

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

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

9.9. Safe Files

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

Utilizando a tecnologia mais recente, a Bitdefender assegura a integridade do sistema ao proteger as áreas críticas do sistema contra ataques de ransomware sem ter impacto no sistema. Contudo, também pode querer proteger os seus ficheiros pessoais, tais como documentos, fotografias ou filmes, contra o acesso de aplicações não fiáveis. Com o Safe Files Bitdefender, pode colocar os ficheiros pessoais num local seguro e definir as aplicações que têm ou não permissão para realizar alterações nos ficheiros protegidos.

Para adicionar ficheiros ao ambiente protegido posteriormente:

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. Selecione o separador **Antiransomware**.

3. Clique em **Ficheiros protegidos** na área de ficheiros seguros.
4. Clique no botão com o sinal mais (+), localizado sob a lista de ficheiros protegidos. Em seguida, escolha o ficheiro, pasta ou volume a proteger no caso de ataques de ransomware que tentam aceder aos mesmos.

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

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

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

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

9.9.1. Acesso de aplicações

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

1. Clique em **Definições** no menu de navegação na interface do Bitdefender.
2. Selecione o separador **Antiransomware**.
3. Clique em **Acesso à aplicação** na área de ficheiros seguros.
4. Altere o estado para Permitir, ao lado da aplicação bloqueada.

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

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

Safe Files

9.10. Time Machine Protection

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

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

Ativar ou desativar a Proteção da Máquina do Tempo

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

1. Clique em **Definições** no menu de navegação na interface do **Bitdefender**.
2. Selecione o separador **Antiransomware**.
3. Ative ou desative o botão de **Proteção Time Machine**.

9.11. Reparar Incidência

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

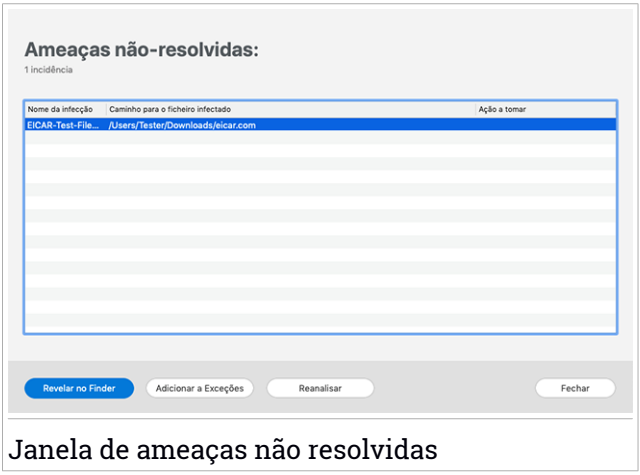
Reparar os problemas indicados pelo Bitdefender Antivirus for Mac é uma forma rápida e fácil de garantir a melhor proteção do seu sistema e dados.

Os problemas detetados incluem:

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

Para verificar e reparar os problemas detetados:

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



Janela de ameaças não resolvidas

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

Pode escolher as seguintes ações para ameaças não resolvidas:

- Apagar manualmente. Escolha essa ação para remover as infeções manualmente.
- Adicionar a Exceções. Essa ação não está disponível para ameaças encontradas dentro de ficheiros.

9.12. Notificações

O Bitdefender mantém um registo detalhado dos eventos relacionados com a sua atividade no seu computador. Sempre que ocorrer algo relevante para a segurança do seu sistema ou dados, será adicionada uma nova mensagem às Notificações do Bitdefender, de forma semelhante a um novo e-mail surgir na sua caixa de entrada.

As notificações são uma ferramenta importante na monitorização e gestão da proteção do seu Bitdefender. Por exemplo, pode verificar com facilidade se a atualização foi realizada com sucesso, se foram encontradas ameaças ou vulnerabilidades no seu computador, etc. Adicionalmente, pode realizar outras ações, se necessário, ou alterar ações tomadas pelo Bitdefender.

Para aceder ao registo de notificações, clique em **Notificações** no menu de navegação da interface do Bitdefender. Sempre que acontecer este evento crítico, pode ser observado um contador no ícone 2.

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

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

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

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

9.13. Atualizações

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

As atualizações de informações sobre as ameaças são executadas na hora, ou seja, os ficheiros que precisam de ser atualizados são substituídos progressivamente. Dessa forma, a atualização não afetará a operação do produto e, ao mesmo tempo, qualquer vulnerabilidade será eliminada.

- Se o Bitdefender Antivirus for Mac estiver atualizado, pode detetar as ameaças mais recentes descobertas e limpar os ficheiros infetados.
- Se o Bitdefender Antivirus for Mac não estiver atualizado, não poderá detetar e remover as ameaças mais recententemente descobertas pelos laboratórios da Bitdefender.

9.13.1. Solicitar uma Actualização

Pode solicitar uma atualização manualmente sempre que quiser.

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

Para solicitar uma atualização manualmente:

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

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

Pode ver o progresso de atualização e ficheiros transferidos.

9.13.2. A obter atualizações através de um servidor proxy

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

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

9.13.3. Atualizar para uma nova versão

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

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

9.13.4. Encontrar informações sobre o Bitdefender Antivirus for Mac

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

Para aceder à janela Sobre:

1. Abrir o Bitdefender Antivirus for Mac.
2. Clique em Bitdefender Antivirus for Mac na barra de menus e escolha **Sobre o antivírus para Mac**.

10. CONFIGURAR PREFERÊNCIAS

Este capítulo inclui os seguintes tópicos:

10.1. Aceder às preferências

Para abrir a janela de preferências do Bitdefender Antivirus for Mac:

1. Faça uma das coisas seguintes:
   - Clique em **Preferências** no menu de navegação da interface da Bitdefender.
   - Clique em Bitdefender Antivirus for Mac na barra de menus e escolha **Preferências**.

10.2. Preferências de proteção

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

- **Escudo Bitdefender.** O Escudo da Bitdefender proporciona uma proteção contínua e em tempo real contra uma ampla variedade de ameaças ao verificar todos os ficheiros instalados, as suas versões atualizadas e ficheiros novos e modificados. Não recomendamos que desligue o Escudo da Bitdefender, mas se for necessário, faça-o durante o tempo mais curto possível. Se o Escudo da Bitdefender estiver desligado, não estará protegido contra ameaças.
- **Analisar só ficheiros alterados.** Selecione esta caixa para configurar o Bitdefender Antivirus for Mac para analisar apenas ficheiros que não foram analisados anteriormente ou que foram modificados desde a última análise.

  Pode optar por não aplicar esta definição para personalização e arrastar&interrompa a análise ao apagar a caixa de verificação correspondente.

- **Não verificar o conteúdo nas cópias.** Selecione esta caixa para eliminar os ficheiros de cópia de segurança da análise. Se os ficheiros infetados forem restaurados posteriormente, o Bitdefender Antivirus for Mac os detetará automaticamente e tomará a ação necessária.

10.3. Preferências avançadas

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

Ação para os itens infectados

Tente desinfetar ou mover para quarentena - Se forem detetados ficheiros infetados, a Bitdefender tentará desinfetá-los (eliminar o código malicioso) ou colocá-los em quarentena.

Não fazer nada - Nada será realizada qualquer ação em relação aos ficheiros detetados.

Ação para os itens suspeitos

Mover os ficheiros para quarentena - Se forem detetados ficheiros suspeitos, a Bitdefender irá colocá-los em quarentena.

Não fazer nada - Nada será realizada qualquer ação em relação aos ficheiros detetados.

10.4. Ofertas Especiais

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

Para ativar ou desativar notificações de ofertas especiais:

1. Clique em **Preferências** no menu de navegação da interface da Bitdefender.
2. Selecione o separador **Outros**.
3. Ative ou desative o botão **As minhas ofertas** .

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

11. VPN

Este capítulo inclui os seguintes tópicos:

11.1. Sobre a VPN

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

A VPN funciona como um túnel entre o seu dispositivo e a rede à qual se liga, protegendo a sua ligação, encriptando os seus dados utilizando uma encriptação de nível bancário e escondendo o seu endereço IP onde quer que esteja. O seu tráfego é redirecionado por meio de um servidor separado, tornando o seu dispositivo quase impossível de ser identificado entre os incontáveis dispositivos que usam os nossos serviços. Além disso, enquanto estiver ligado à Internet com o Bitdefender VPN, pode aceder a conteúdos que normalmente são restritos em áreas específicas.

Nota

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

11.2. A abrir a VPN

Existem três formas de abrir a aplicação de VPN da Bitdefender:

- Clique em **Definições** no menu de navegação na interface do **Bitdefender**.

  Clique em **Abrir** no cartão da VPN Bitdefender.

- Clique no ícone na barra do menu.

- Aceda à pasta Aplicações, abra a pasta Bitdefender e clique duas vezes no ícone VPN Bitdefender.

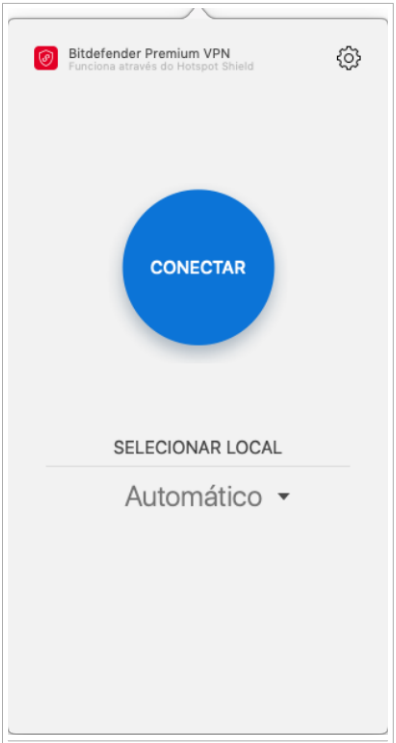
Na primeira vez que abrir a aplicação, ser-lhe-á solicitada permissão para que a Bitdefender possa adicionar configurações. Ao permitir que a Bitdefender adicione configurações, está a concordar que a atividade da rede do seu dispositivo poderá ser filtrada ou monitorizada ao utilizar a aplicação de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

Nota
Aplikacja Bitdefender VPN może być zainstalowana tylko na macOS Sierra (10.12.6), macOS High Sierra (10.13.6) lub macOS Mojave (10.14 lub nowszy).

11.3. Interface

A interface do VPN exibe o estado da aplicação, conectado ou desconectado. Aqui tem a possibilidade de alterar a localização do servidor ao qual está ligado.

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



Interface do VPN

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

- **A minha conta** - detalhes sobre a sua conta Bitdefender e a subscrição do VPN são exibidos. Clique em **Trocar conta** se deseja entrar com outra conta.
- **Definições** - dependendo das suas necessidades, pode personalizar o comportamento do seu produto:
  - Notificações
  - Configure a VPN para que seja executada no arranque do sistema
  - Relatórios do produto

- Autoconnect - localizada no separador **Avançado**, esta funcionalidade permite que se ligue ao VPN da Bitdefender de forma automática sempre que aceder a uma Wi-Fi pública ou não segura, ou ao iniciar uma aplicação de partilha de ficheiros peer-to-peer.

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

12. BITDEFENDER CENTRAL

Este capítulo inclui os seguintes tópicos:

12.1. Sobre Bitdefender Central

Bitdefender Central é a plataforma onde tem acesso às funções e serviços online do produto, e pode realizar remotamente tarefas importantes nos dispositivos em que o Bitdefender estiver instalado. Pode aceder à sua conta Bitdefender desde qualquer computador ou dispositivo móvel ligado à internet, indo para https://central.bitdefender.com, ou diretamente pela aplicação da Bitdefender Central em dispositivos Android e iOS.

Para instalar a aplicação da Bitdefender Central nos seus dispositivos:

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

Assim que iniciar sessão, pode começar a fazer o seguinte:

- Transfira e instale o Bitdefender nos sistemas operativos Windows, macOS, iOS e Android. Os produtos disponíveis para download são:
  - Bitdefender Antivirus for Mac
  - A linha de produtos Windows da Bitdefender
  - Bitdefender Mobile Security para Android
  - Bitdefender Mobile Security for iOS
- Gerir e renovar as suas subscrições do Bitdefender.
- Adicionar novos dispositivos à sua rede e gerir as suas funcionalidades onde quer que esteja.

12.2. A aceder Bitdefender Central

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

- A partir da interface principal do Bitdefender Antivirus for Mac:
  1. Clique na hiperligação **Ir para a sua conta** na parte inferior direita do ecrã.
- Do seu navegador Web:
  1. Abrir um navegador em qualquer dispositivo com acesso à internet.
  2. Vá para: https://central.bitdefender.com.
  3. Inicie sessão na sua conta com o seu endereço de e-mail e palavra-passe.
- No seu dispositivo Android ou iOS:

  Abra a aplicação da Bitdefender Central que instalou.

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

12.3. Autenticação de dois fatores

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

Ativar autenticação de dois fatores

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

Para ativar a autenticação de dois fatores:

1. Aceda Bitdefender Central.
2. Clique no ícone no canto superior direito do ecrã.

3. Clique em **Conta da Bitdefender** no menu deslizante.
4. Selecione o separador **Palavra-passe e segurança**.
5. Clique em **COMEÇAR**.

   Selecione uma das seguintes opções:

   - **Aplicação de autenticação** - utilize uma apliação de autenticação para gerar um código sempre que quiser aceder à sua conta Bitdefender.

     Caso queira utilizar a aplicação de autenticação, mas não tem a certeza de qual escolher, aparecerá uma lista com as aplicações de autenticação recomendadas.

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

     b. Para uniciar sessão num dispositivo Android ou iOS, utilize o seu dispositivo para digitalizar o código QR.

        Para iniciar sessão utilizando um portátil ou um computador, pode adicionar manualmente o código apresentado.

        Clique em **CONTINUAR**.

     c. Insira o código fornecido pela aplicação ou o apresentado no passo anterior e, em seguida, clique em **ATIVAR**.

   - **E-mail** - sempre que iniciar sessão na sua conta Bitdefender, o código de verificação será enviado para a sua caixa de e-mail. Verifique o seu email e utilize o código que lhe foi enviado.

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

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

     c. Clique em **ATIVAR**.

Caso queira deixar de utilizar a autenticação de dois fatores:

1. Clique em **DESATIVAR A AUTENTICAÇÃO EM DOIS FATORES**.
2. Verifique a sua aplicação ou conta de e-mail e introduza o código que recebeu.
3. Confirme a sua escolha.

12.4. Adicionar dispositivos fiáveis

Para garantir que apenas pode aceder à sua conta Bitdefender, poderemos solicitar o código de segurança primeiro. Caso pretenda ignorar este passo sempre que se ligar com o mesmo dispositivo, recomendamos identificá-lo como um dispositivo fiável.

Para adicionar dispositivos como dispositivos fiáveis:

1. Aceda Bitdefender Central.
2. Clique no ícone no canto superior direito do ecrã.
3. Clique em **Conta da Bitdefender** no menu deslizante.
4. Selecione o separador **Palavra-passe e segurança**.
5. Clique em **Dispositivos fiáveis**.
6. Será mostrada a lista com os dispositivos Bitdefender instalados. Clique no dispositivo desejado.

Pode adicionar os dispositivos que pretender, desde que tenham o Bitdefender instalado e a sua subscrição seja válida.

12.5. Actividade

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

Ao aceder a janela **Atividade**, os seguintes cartões são disponibilizados:

- **Meus dispositivos**. Aqui pode visualizar o número de dispositivos ligados e o seu estado de proteção. Para resolver problemas remotamente nos dispositivos detectados, clique em **Resolver problemas** e, em seguida, clique em **ANALISAR E RESOLVER PROBLEMAS**.

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

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

- **Ameaças bloqueadas**. Aqui pode visualizar um gráfico que mostra uma estatística geral que inclui informação sobre as ameaças bloqueadas nas últimas 24 horas e nos últimos sete dias. A informação exibida vai depender do comportamento malicioso detectado e os ficheiros, aplicações e URLs acedidos.

- **Utilizadores principais com ameaças bloqueadas**. Aqui pode visualizar uma lista que mostra onde o maior número ameaças para os utilizadores foram identificadas.
- **Dispositivos principais com ameaças bloqueadas**. Aqui pode visualizar uma lista mostrando onde foram encontrados os dispositivos com o maior número de ameaças.

12.6. As minhas subscrições

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

12.6.1. Ativar subscrição

Uma subscrição pode ser ativada durante o processo de instalação utilizando a sua conta Bitdefender. Juntamente com o processo de ativação, a validade da subscrição inicia a sua contagem decrescente.

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

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

1. Aceda Bitdefender Central.
2. Clique no ícone ☰ localizado no canto superior esquerdo da janela e selecione o painel **As minhas subscrições**.
3. Clique no botão **CÓDIGO DE ATIVAÇÃO** e, em seguida, escreva o código no campo correspondente.
4. Clique em **ATIVAR** para continuar.

A subscrição está ativada agora.

Para começar a instalar o produto nos seus dispositivos, consulte "*A instalar Bitdefender Antivirus for Mac*" (p. 195).

12.7. Meus dispositivos

A seção **Meus dispositivos** na sua conta Bitdefender permite-lhe instalar, gerir e realizar ações remotas no seu Bitdefender em qualquer dispositivo, desde que esteja ativado e ligado à Internet. Os cartões de dispositivos

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

12.7.1. Personalize o seu dispositivo

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

1. Aceda Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.
3. Clique no cartão de dispositivo pretendido e, em seguida, o ícone ⋮ no canto superior direito do ecrã.
4. Selecione **Definições**.
5. Digite um novo nome no campo **Nome do dispositivo** e clique **GUARDAR**.

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

1. Aceda Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.
3. Clique no cartão de dispositivo pretendido e, em seguida, o ícone ⋮ no canto superior direito do ecrã.
4. Selecione **Perfil**.
5. Clique em **Add owner** e, em seguida, preencha os respetivos campos. Personalize o perfil adicionando uma fotografia e selecionando a data de nascimento, além de um e-mail e número de telefone.
6. Clique em **ADICIONAR** para guardar o perfil.
7. Selecione o proprietário pretendido na lista **Proprietário do dispositivo** e, em seguida, clique em **ATRIBUIR**.

12.7.2. Ações remotas

Para atualizar o Bitdefender remotamente no dispositivo:

1. Aceda Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.

3. Clique no cartão de dispositivo pretendido e, em seguida, o ícone ⋮ no canto superior direito do ecrã.
4. Selecione **Atualizar**.

Quando clicar no cartão de dispositivo, ficam disponíveis os seguintes separadores:

- **Painel**. Nesta janela, pode visualizar os detalhes sobre o dispositivo selecionado, verificar o seu estado de proteção e quantas ameaças foram bloqueadas nos últimos sete dias. O estado de proteção pode estar verde, quando não houver problemas a afetar o seu dispositivo, amarelo, quando o dispositivo exigir a sua atenção, ou vermelho, quando o dispositivo estiver em risco. Quando houver problemas a afetar o seu dispositivo, clique no seta pendente na área de estado acima para saber mais detalhes. A partir daqui poderá resolver manualmente os problemas que afetam a segurança dos seus dispositivos.
- **Proteção**. A partir desta janela, pode realizar remotamente uma Análise Rápida ou Completa nos seus dispositivos. Clique no botão **VERIFICAR** para iniciar o processo. Também pode conferir quando é que a última verificação foi realizada no dispositivo e aceder a um relatório da última verificação, contendo as informações mais importantes. Para mais informações sobre esses dois processos de análise, consulte "*Analisar o seu Mac*" (p. 208).

13. PERGUNTAS FREQUENTES

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

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

1. Criar uma conta Bitdefender seguindo os seguintes passos:
   a. Vá para: https://central.bitdefender.com.
   b. Digite as informações solicitadas nos campos correspondentes. Os dados que nos fornecer serão mantidos confidenciais.
   c. Antes de continuar, deve concordar com os Termos de utilização. Aceda aos Termos de Utilização e leia-os com atenção, pois eles contêm os termos e condições segundo os quais pode utilizar o Bitdefender.

      Além disso, pode aceder e ler a Política de Privacidade.
   d. Clique em **CRIAR CONTA**.
2. Transfira o Bitdefender Antivirus for Mac como se segue:
   a. Selecione o painel **Os meus dispositivos**, e clique em **INSTALAR PROTEÇÃO**.
   b. Escolha uma das duas opções disponíveis:
      - **Proteger este dispositivo**
        i. Selecione esta opção e, em seguida, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique no botão correspondente.
        ii. Guarde o ficheiro de instalação.
      - **Proteger outros dispositivos**
        i. Selecione esta opção e, em seguida, selecione o(a) dono(a) do dispositivo. Se o dispositivo for de outra pessoa, clique no botão correspondente.
        ii. Clique em **ENVIAR HIPERLIGAÇÃO DE DOWNLOAD**.

iii. Escreva um endereço de email no campo correspondente e clique em **ENVIAR EMAIL**.

Observe que a hiperligação de download gerada será válida apenas durante as próximas 24 horas. Se a hiperligação expirar, precisará de gerar uma nova seguindo os mesmos passos.

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

c. Execute o Bitdefender que transferiu.

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

Os itens não resolvidos no registo de análise podem ser:

- ficheiros de acesso restrito (xar, rar, etc.)

  Solução: utilize a opção **Revelar no Finder** para encontrar o ficheiro e eliminá-lo manualmente. Não se esqueça de esvaziar a Reciclagem.

- caixas de correio de acesso restrito (Thunderbird, etc.)

  Solução: utilize a aplicação para remover a entrada que contém o ficheiro infetado.

- O conteúdo nas cópias

  Solução: Ative a opção **Não verificar o conteúdo nas cópias de segurança** nas Preferências de Proteção ou selecione **Adicionar às Exceções** para os ficheiros detectados.

  Se os ficheiros infetados forem restaurados posteriormente, o Bitdefender Antivirus for Mac os detetará automaticamente e tomará a ação necessária.

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

Onde posso ver detalhes sobre a atividade do produto?

O Bitdefender mantém um registo de todas as ações importantes, mudanças de estado e outras mensagens críticas relacionadas com a

sua atividade. Para aceder a essas informações, clique em **Notificações** no menu de navegação na interface da Bitdefender.

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

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

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

Como posso remover o Bitdefender Antivirus for Mac?

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

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

> **Importante**
> Se ocorrer um erro, pode entrar em contacto com o Atendimento ao Consumidor da Bitdefender, como descrito em "Contacte-nos" (p. 301).

Como removo as extensões do TrafficLight do meu browser?

- Para remover as extensões do TrafficLight do Mozilla Firefox, siga estes passos:
  1. Aceda a **Ferramentas** e selecione **Suplementos**.
  2. Selecione **Extensões** na coluna da esquerda.
  3. Selecione a extensão e clique em **Remover**.
  4. Reinicie o browser para concluir o processo de remoção.
- Para remover as extensões do TrafficLight do Google Chrome, siga estes passos:
  1. Na parte superior direita, clique em **Mais** ⋮.
  2. Aceda a **Mais Ferramentas** e selecione **Extensões**.

3. Clique no ícone **Remover...**  ao lado da extensão que deseja remover.
4. Clique em **Desinstalar** para confirmar o processo de remoção.

- Para remover o Bitdefender TrafficLight do Safari, siga estes passos:
  1. Ir a **Preferências** ou pressionar **Command-Vírgula(,)**.
  2. Seleccione **Extensões**.

     Será exibida a lista das extensões instaladas.
  3. Seleccione a extensão Bitdefender TrafficLight, e clique em **Desinstalar**.
  4. Clique outra vez em **Desinstalar** para confirmar a desinstalação.

Quando devo usar o Bitdefender VPN?

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

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

O Bitdefender VPN vai ter um impacto negativo na bateria do meu dispositivo?

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

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

O Bitdefender VPN foi concebido para suavizar a sua experiência enquanto navega na Internet. No entanto, a lentidão pode ser causada pela sua conectividade com a internet ou pela distância do servidor ao

qual está ligado. Nesse caso, se não for uma necessidade ligar a um servidor distante com respeito à sua localização (por exemplo, dos EUA ou China), recomendamos que permita ao Bitdefender VPN ligá-lo automaticamente ao servidor mais próximo, ou encontrar um servidor próximo da sua localização atual.

MOBILE SECURITY PARA IOS

14. EM QUE CONSISTE O BITDEFENDER MOBILE SECURITY FOR IOS

Atividades online, como pagar contas, fazer reservas para as férias ou comprar bens e serviços são convenientes e práticas. Mas, como muitas atividades realizadas na Internet, fazem-se acompanhar de elevados riscos e, se os detalhes de segurança forem ignorados, os dados pessoais podem ser hackeados. E o que é mais importante do que proteger os dados armazenados em contas online e no seu smartphone?

O Bitdefender Mobile Security for iOS permite:

- Proteja os seus dados ao ligar-se a redes sem fios não seguras.
- Tenha cuidado com websites e domínios maliciosos enquanto estiver online.
- Verificar se houve fugas nas contas online que utiliza diariamente.

O Bitdefender Mobile Security for iOS é entregue gratuitamente e requer a ativação com uma conta Bitdefender.

15. INTRODUÇÃO

Requisitos do Aparelho

O Bitdefender Mobile Security for iOS funciona em qualquer dispositivo com iOS 11.2 ou superior e necessita de uma ligação à Internet para ser ativado e detetar quaisquer fugas de dados nas suas contas online.

A instalar Bitdefender Mobile Security for iOS

- **Da Bitdefender Central**
  - Em iOS
    1. Aceda Bitdefender Central.
    2. Toque no ícone no canto superior esquerdo do ecrã e, em seguida, selecione **Os meus dispositivos**.
    3. Toque em **INSTALAR A PROTEÇÃO** e, em seguida, toque em **Proteger este dispositivo**.
    4. Selecione o dono do dispositivo. Se o dispositivo pertencer a outra pessoa, pressione o respetivo botão.
    5. Vai ser redirecionado para a aplicação da **App Store**. No ecrã da App Store, toque na opção de instalação.
  - No Windows, macOS e Android
    1. Aceda Bitdefender Central.
    2. Pressione o ícone no canto superior esquerdo do ecrã e, em seguida, selecione **Os meus dispositivos**.
    3. Pressione **INSTALAR A PROTEÇÃO** e, em seguida, pressione **Proteger outros dispositivos**.
    4. Selecione o dono do dispositivo. Se o dispositivo pertencer a outra pessoa, pressione o respetivo botão.
    5. Pressione **Enviar Hiperligação de Download**.
    6. Escreva um endereço de e-mail no campo correspondente e pressione **ENVIAR E-MAIL**. Observe que a hiperligação de download gerada será válida apenas durante as próximas 24 horas. Se a hiperligação expirar, precisará de gerar uma nova seguindo os mesmos passos.

7. No dispositivo em que deseja instalar o Bitdefender verifique a conta de e-mail que escreveu e pressione o botão de download correspondente.

- **Na App Store**

  Pesquise por Bitdefender Mobile Security for iOS para localizar e instalar a aplicação.

É exibida uma janela introdutória com detalhes sobre as funções do produto na primeira vez que abrir a aplicação. Pressione **Começar** para avançar para o próximo passo.

Antes de passar pelos passos de validação, deve concordar com o Acordo de Subscrição. Leia o Contrato de Subscrição com calma pois contém os termos e condições que regem a utilização do Bitdefender Mobile Security for iOS.

Toque em **Continuar** para avançar para a janela seguinte.

Iniciar sessão na sua conta Bitdefender

Para utilizar o Bitdefender Mobile Security for iOS, deve associar o seu dispositivo a uma conta Bitdefender do Facebook, Google, Apple ou Microsoft iniciando sessão na conta a partir da aplicação. A primeira vez que abrir a aplicação, será pedido que inicie sessão numa conta.

Para associar o seu dispositivo a uma conta Bitdefender:

1. Introduza o seu endereço de e-mail da sua conta da Bitdefender no respetivo campo e clique em **PRÓXIMO**. Se não tem uma conta da Bitdefender e pretende criar uma, selecione a respetiva hiperligação e depois siga as instruções no ecrã até a conta ser ativada.

   Para entrar usando uma conta do Facebook, Google, Apple ou Microsoft, pressione o serviço que deseja usar na área **OU ENTRAR COM**. Será redirecionado para a página de login do serviço selecionado. Siga as instruções para vincular a sua conta ao Bitdefender Mobile Security for iOS.

   Nota
   O Bitdefender não obtém acesso a qualquer informação confidencial como a palavra-passe da conta que usa para iniciar sessão ou a informação particular dos seus amigos ou contactos.

2. Introduza a sua palavra-passe e depois toque em **ENTRAR**.

   Aqui também pode aceder à Política de Privacidade do Bitdefender.

Painel

Toque no ícone do Bitdefender Mobile Security for iOS na secção de aplicações do seu dispositivo para abrir a interface da aplicação.

Na primeira vez que abrir a aplicação, será solicitado a permitir ao Bitdefender o envio de notificações. Prima **Permitir** para permanecer informado sempre que o Bitdefender tiver de comunicar algo relevante para a sua aplicação. Para gerir as notificações do Bitdefender, aceda a Definições > Notificações > Segurança móvel.

Para aceder às informações necessárias, toque no ícone correspondente na parte inferior do ecrã.

VPN

Mantenha a sua privacidade independentemente da rede à qual estiver ligado(a) para manter a sua comunicação pela Internet encriptada. Para mais informação, dirija-se a "*VPN*" (p. 247).

Proteção da Internet

Fique seguro(a) enquanto navega na Internet e quando aplicações menos seguras tentarem aceder a domínios não fiáveis. Para mais informação, dirija-se a "*Proteção da Internet*" (p. 249).

Privacidade de conta

Saiba se as suas contas de e-mail foram invadidas ou não. Para mais informação, dirija-se a "*Privacidade de conta*" (p. 252).

Para ver mais opções, toque no ícone ••• no dispositivo enquanto estiver no ecrã inicial da aplicação. São apresentadas as seguintes opções:

- **Restaurar compras** - aqui pode restaurar as antigas subscrições que comprou através da conta do iTunes.
- **Definições** - aqui tem acesso a:
  - **Definições da VPN**
    - **Contrato** - pode ler os termos de utilização do serviço VPN de Bitdefender. Caso selecione **Já não concordo**, não poderá utiliza a VPN de Bitdefender até carregar em **Concordo**.

- **Abrir aviso de Wi-Fi** - pode ativar ou desativar a notificação do produto que é apresentada sempre que estabelecer ligação a uma rede Wi-Fi não segura. O objetivo desta notificação é ajudá-lo a manter os seus dados privados e seguros utilizando a VPN de Bitdefender.

- **Definições da proteção na web**
  - **Contrato** - pode ler os termos de utilização do serviço Proteção na web de Bitdefender. Caso selecione **Já não concordo**, não poderá utiliza a VPN de Bitdefender até carregar em **Concordo**.
  - **Ativar notificações da Proteção na Web** - Será notificado(a) para lembrar que a Proteção na Web pode ser ativada após o fim de uma sessão VPN.
- Relatórios do produto

- **Comentários** — aqui pode iniciar o cliente de e-mail predefinido para nos enviar comentários sobre a aplicação.
- **Informações sobre a aplicação** — aqui tem acesso a informações sobre a versão instalada e o Contrato de Subscrição, Política de Privacidade e conformidade com licenças de código aberto.

16. VPN

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

A VPN funciona como um túnel entre o seu dispositivo e a rede à qual se liga, protegendo a sua ligação, encriptando os seus dados utilizando uma encriptação de nível bancário e escondendo o seu endereço IP onde quer que esteja. O seu tráfego é redirecionado por meio de um servidor separado, tornando o seu dispositivo quase impossível de ser identificado entre os incontáveis dispositivos que usam os nossos serviços. Além disso, enquanto estiver ligado à Internet com o Bitdefender VPN, pode aceder a conteúdos que normalmente são restritos em áreas específicas.

Nota
China, Iraque, EAU, Turquia, Bielorrússia, Omã, Irão e Rússia praticam a censura na Internet e, portanto, a utilização de VPN no seu território foi proibido por lei. Consequentemente, a funcionalidade do Bitdefender VPN não estará disponível no seu território.

Para ativar o Bitdefender VPN:

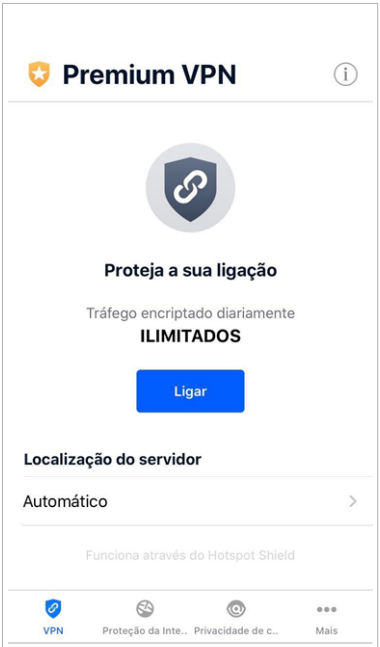
1. Toque no ícone na parte inferior do ecrã.
2. Pressione **Ligarr** sempre que quiser permanecer protegido enquanto estiver ligado às redes sem fios não seguras.

   Pressione **Desconectar** quando desejar desativar a ligação.

Nota
Na primeira vez que ligar o VPN, será solicitado a permitir que o Bitdefender faça configurações de VPN que monitorizarão o tráfego de rede. Prima **Permitir** para continuar. Se tiver sido configurado um método de autenticação (leitura de digital ou código PIN) para proteger o seu smartphone, será solicitado que o utilize.

O ícone VPN aparece na barra de estado quando a VPN está ativa.

Caso pretenda ligar-se a um servidor da sua preferência, pressione **Localização do servidor** na inerface da VPN e selecione a localização que pretende.



VPN

17. PROTEÇÃO DA INTERNET

A Proteção na Internet do Bitdefender garante uma experiência de navegação segura alertando-o sobre páginas da Internet maliciosas e quando aplicações instaladas menos seguras tentam aceder a domínios não fiáveis.

Quando um URL sinalizar uma página da Internet conhecida como phishing ou fraudulenta, ou como tendo conteúdo malicioso como spyware ou vírus, a página da Internet é bloqueada e é exibido um alerta. Acontece a mesma coisa quando aplicações instaladas tentam aceder a domínios maliciosos.

Importante
Se está numa área onde a utilização de um serviço VPN é limitado por lei, a função de Proteção na Internet não estará disponível.

Para ativar a Proteção na Internet:

1. Toque no ícone na parte inferior do ecrã.
2. Prima **Eu concordo**.
3. Ativar a chave de Proteção na Internet.

Nota
A primeira vez que ligar a Proteção na Internet, deverá permitir ao Bitdefender definir as configuração de VPN que irão monitorizar o tráfego de rede. Prima **Permitir** para continuar. Se tiver sido configurado um método de autenticação (leitura de digital ou código PIN) para proteger o seu smartphone, será solicitado que o utilize. Para poder detetar o acesso a domínios não fiáveis, a Proteção na Internet trabalha em conjunto com os serviços VPN.

Importante
A funcionalidade de Proteção na Web e o VPN não podem funcionar ao mesmo tempo. Sempre que um deles for ativado, o outro (caso esteja ativo nessa altura) será desativado.

17.1. Alertas de Bitdefender

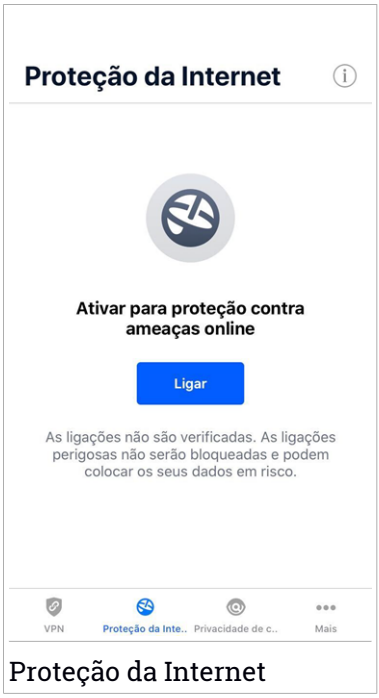
Sempre que tentar visitar um site classificado como não seguro, será bloqueado. Para avisá-lo sobre o evento, será notificado pelo Bitdefender no centro de Notificações e no seu navegador. A página de alertas contém informações como o URL do site e a ameaça detetada. Tem de decidir o que fazer a seguir.

Além disso, receberá notificações no Centro de Notificações quando uma aplicação menos segura tentar aceder a domínios não fiáveis. Clique na notificação exibida para ser redirecionado(a) para a janela onde poderá decidir o que fazer a seguir.

As seguintes opções estão disponíveis para os dois casos:

- Sair do site tocando em **VOLTAR À SEGURANÇA**.
- Ir para o site apesar do aviso tocando na notificação mostrada e, em seguida, em **Quero aceder à página**.

  Confirme a sua escolha.



Proteção da Internet

17.2. Assinaturas

A Proteção na Internet é uma função baseada em subscrição com a possibilidade de experimentá-la gratuitamente para poder decidir se satisfaz as suas necessidades. Existem dois tipos de subscrição disponíveis: anual e mensal.

Se asua subscrição da Proteção na Internet da Bitdefender expirar, não irá receber mais alertas ao aceder a conteúdo malicioso.

Se comprou um dos pacotes do Bitdefender, como o Bitdefender Total Security, terá acesso ilimitado à Proteção na Internet.

18. PRIVACIDADE DE CONTA

A Privacidade de Conta Bitdefender deteta se houve fuga de dados nas contas que utiliza para fazer pagamentos online, compras ou iniciar sessão em diferentes aplicações ou sites Web. Os dados armazenados numa conta podem ser palavras-passe, informações de cartão de crédito ou informações de conta bancária e, se não forem devidamente protegidos, pode sofrer roubo de identidade ou invasão de privacidade.

O estado de privacidade de uma conta é apresentado depois da validação.

Para verificar se qualquer conta foi invadida, toque em **Procurar fugas**.

Para começar a proteger informações pessoais:

1. Toque no ícone na parte inferior do ecrã.
2. Toque em **Adicionar conta**.
3. Digite o seu endereço de e-mail no campo correspondente e toque em **Seguinte**.

   Bitdefender necessita de validar esta conta antes de apresentar informações privadas. Portanto, é enviado um e-mail com um código de validação para o endereço de e-mail fornecido.
4. Verifique a caixa de entrada e digite o código recebido na área **Privacidade de Conta** da aplicação. Se não conseguir encontrar o e-mail de validação na pasta Caixa de Entrada, verifique a pasta Spam.

   O estado de privacidade da conta validada é apresentado.

Se forem detetadas fugas nas suas contas, recomendamos que altere as palavras-passe assim que possível. Para criar uma palavra-passe forte e segura, tenha em mente estas dicas:

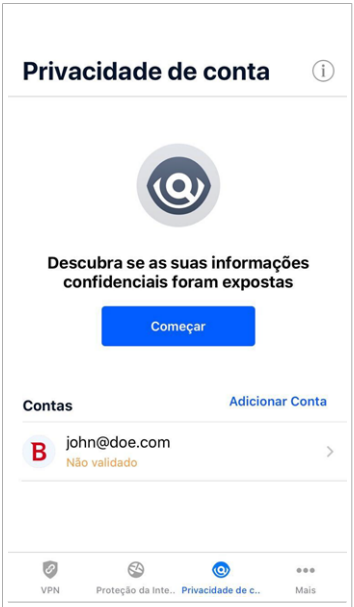
- Oito carateres no mínimo.
- Carateres maiúsculos e minúsculos.
- Pelo menos um número ou símbolo, como #, @, % ou !.

Ao proteger uma conta que constava de uma violação de privacidade, pode confirmar as alterações ao marcar a(s) fuga(s) identificada(s) como **Resolvido**. Para tal:

1. Toque em ··· ao lado da falha de segurança resolvida.

2. Toque em **Marcar como resolvido**.

Quando todas as fugas detetadas estiverem marcadas como **Resolvido**, a conta já não aparece como fuga, pelo menos até à deteção de uma nova fuga.



Privacidade de conta

19. BITDEFENDER CENTRAL

Bitdefender Central é a plataforma Web onde tem acesso às funcionalidades e serviços online do produto, e pode realizar remotamente tarefas importantes nos dispositivos em que o Bitdefender estiver instalado. Pode aceder à sua conta Bitdefender desde qualquer computador ou dispositivo móvel ligado à internet, indo para https://central.bitdefender.com, ou diretamente pela aplicação da Bitdefender Central em dispositivos Android e iOS.

Para instalar a aplicação da Bitdefender Central nos seus dispositivos:

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

Assim que iniciar sessão, pode começar a fazer o seguinte:

- Transfira e instale o Bitdefender nos sistemas operativos Windows, macOS, iOS e Android. Os produtos disponíveis para download são:
  - Bitdefender Mobile Security para Android
  - Bitdefender Mobile Security for iOS
  - O Antivírus Bitdefender para Mac
  - A linha de produtos Windows da Bitdefender
- Gerir e renovar as suas subscrições do Bitdefender.
- Adicionar novos dispositivos à sua rede e gerir as suas funcionalidades onde quer que esteja.

Aceder à sua conta Bitdefender

Há duas formas de aceder à Bitdefender Central

- Do seu navegador Web:
  1. Abrir um navegador em qualquer dispositivo com acesso à internet.
  2. Vá para: https://central.bitdefender.com.

3. Inicie sessão na sua conta com o seu endereço de e-mail e palavra-passe.

- No seu dispositivo Android ou iOS:

  Abra a aplicação da Bitdefender Central que instalou.

Nota
Neste material, recebe as opções e instruções disponíveis na plataforma web.

Autenticação de dois fatores

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

Ativar autenticação de dois fatores

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

Para ativar a autenticação de dois fatores:

1. Aceda Bitdefender Central.
2. Toque no ícone no canto superior direito do ecrã.
3. Clique em **Conta do Bitdefender** no menu deslizante.
4. Selecione o separador **Palavra-passe e segurança**.
5. Toque em **Autenticação em dois fatores**.
6. Toque em **INICIAR**.

   Selecione uma das seguintes opções:

   - **Aplicação de autenticação** - utilize uma apliação de autenticação para gerar um código sempre que quiser aceder à sua conta Bitdefender.

Caso queira utilizar a aplicação de autenticação, mas não tem a certeza de qual escolher, aparecerá uma lista com as aplicações de autenticação recomendadas.

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

b. Para uniciar sessão num dispositivo Android ou iOS, utilize o seu dispositivo para digitalizar o código QR.

Para iniciar sessão utilizando um portátil ou um computador, pode adicionar manualmente o código apresentado.

Toque em **CONTINUAR**.

c. Insira o código fornecido pela aplicação ou o apresentado no passo anterior e, em seguida, toque em **ATIVAR**.

- **E-mail** - sempre que iniciar sessão na sua conta Bitdefender, o código de verificação será enviado para a sua caixa de e-mail. Verifique a sua conta de e-mail e introduza o código fornecido.

a. Toque em **UTILIZAR E-MAIL** para começar.

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

Lembre que tem cinco minutos para verificar a sua conta de e-mail e introduzir o código gerado. Se o tempo expirar, deverá gerar uma nova hiperligação seguindo os mesmos passos.

c. Toque em **ATIVAR**.

d. Receberá dez códigos de ativação. Pode copiar, transferir ou imprimir a lista e usá-la caso perca o seu endereço de e-mail, caso contrário não poderá iniciar sessão. Cada código pode ser utilizado apenas uma vez.

e. Toque em **CONCLUÍDO**.

Caso queira deixar de utilizar a autenticação de dois fatores:

1. Toque em **DESATIVAR A AUTENTICAÇÃO EM DOIS FATORES**.
2. Verifique a sua aplicação ou conta de e-mail e introduza o código que recebeu.

   Caso tenha escolhido receber o código de autenticação por e-mail, terá cinco minutos para verificar a sua conta de e-mail e introduzir o código gerado. Se o tempo expirar, deverá gerar uma nova hiperligação seguindo os mesmos passos.

3. Confirme a sua escolha.

Adicionar dispositivos fiáveis

Para garantir que apenas pode aceder à sua conta Bitdefender, poderemos solicitar o código de segurança primeiro. Caso pretenda ignorar este passo sempre que se ligar com o mesmo dispositivo, recomendamos identificá-lo como um dispositivo fiável.

Para adicionar dispositivos como dispositivos fiáveis:

1. Aceda Bitdefender Central.
2. Toque no ícone no canto superior direito do ecrã.
3. Clique em **Conta do Bitdefender** no menu deslizante.
4. Selecione o separador **Palavra-passe e segurança**.
5. Toque em **Dispositivos fiáveis**.
6. Será mostrada a lista com os dispositivos Bitdefender instalados. Toque no dispositivo pretendido.

Pode adicionar os dispositivos que pretender, desde que tenham o Bitdefender instalado e a sua subscrição seja válida.

Meus dispositivos

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

Para identificar e gerir facilmente os seus dispositivos, pode personalizar o nome do dispositivo e criar ou atribuir um proprietário para cada um deles:

1. Pressione o ícone no canto superior esquerdo do ecrã e, em seguida, selecione **Os meus dispositivos**.
2. Toque no cartão de dispositivo pretendido e, em seguida, o ícone no canto superior direito do ecrã. Estão disponíveis as seguintes opções:
   - **Definições** - aqui pode alterar o nome do dispositivo selecionado.

- **Perfil** - aqui pode ser atribuído um perfil ao dispositivo selecionado. Toque em **Adicionar proprietário** e preencha os campos correspondentes. Defina o nome, e-mail, número de telefone, data de nascimento e até pode selecionar uma fotografia de perfil.
- **Remover** - a partir daqui, é possível remover um perfil juntamente com o dispositivo atribuído da sua conta Bitdefender.

Iniciar sessão com outra conta Bitdefender

Para iniciar sessão com outra conta Bitdefender:

1. Toque no ícone na parte inferior do ecrã.
2. Toque em **Terminar sessão**.
3. Introduza o endereço de e-mail e palavra-passe da sua conta Bitdefender nos campos correspondentes.
4. Pressione **ENTRAR**.

MOBILE SECURITY PARA ANDROID

20. FUNCIONALIDADES DA PROTECÇÃO

O Bitdefender Mobile Security protege o seu dispositivo Android com os seguintes recursos:

- Analisador de Malware
- Proteção da Internet
- VPN
- AntiFurto, incluindo:
  - Localização Remota
  - Bloqueio remoto do aparelho
  - Limpeza remota do aparelho
  - Alertas do aparelho remoto
- Privacidade de conta
- Bloqueio de Aplicativo
- Relatórios
- WearON

Pode utilizar os recursos do produto por 14 dias, sem nenhum custo. Quando o período expirar, é necessário comprar a versão completa para proteger o seu dispositivo móvel.

21. INTRODUÇÃO

Requisitos do Aparelho

O Bitdefender Mobile Security funciona em qualquer dispositivo com Android 4.1 ou superior. É necessária uma ligação ativa à internet para a análise de ameaça na nuvem.

A instalar Bitdefender Mobile Security

- **Da Bitdefender Central**
  - Android
    1. Vá para: https://central.bitdefender.com.
    2. Iniciar sessão na sua conta Bitdefender.
    3. Pressione ☰ no canto superior esquerdo do ecrã e, em seguida, selecione **Os meus dispositivos**.
    4. Toque em **INSTALAR A PROTEÇÃO** e, em seguida, toque em **Proteger este dispositivo**.
    5. Selecione o dono do dispositivo. Se o dispositivo pertencer a outra pessoa, pressione o respetivo botão.
    6. Será redirecionado para a aplicação do **Google Play**. No ecrã da Google Play, toque na opção de instalação.
  - No Windows, macOS, iOS
    1. Vá para: https://central.bitdefender.com.
    2. Iniciar sessão na sua conta Bitdefender.
    3. Pressione ☰ no canto superior esquerdo do ecrã e, em seguida, selecione **Os meus dispositivos**.
    4. Pressione **INSTALAR A PROTEÇÃO** e, em seguida, pressione **Proteger outros dispositivos**.
    5. Selecione o dono do dispositivo. Se o dispositivo pertencer a outra pessoa, pressione o respetivo botão.
    6. Pressione **Enviar Hiperligação de Download**.

7. Escreva um endereço de e-mail no campo correspondente e pressione **ENVIAR E-MAIL**. Observe que a hiperligação de download gerada será válida apenas durante as próximas 24 horas. Se a hiperligação expirar, precisará de gerar uma nova seguindo os mesmos passos.
8. No dispositivo em que deseja instalar o Bitdefender verifique a conta de e-mail que escreveu e pressione o botão de download correspondente.

- **Do Google Play**

  Pesquise por Bitdefender Mobile Security para localizar e instalar a aplicação.

  Alternativamente, analise o código QR:

Código QR

Antes de passar pelos passos de validação, deve concordar com o Acordo de Subscrição. Leia o Contrato de Subscrição com calma pois contém os termos e condições que regem a utilização do Bitdefender Mobile Security.

Toque em **CONTINUAR** para avançar para a janela seguinte.

Iniciar sessão na sua conta Bitdefender

Para utilizar o Bitdefender Mobile Security, deve associar o seu dispositivo a uma conta Bitdefender do Facebook, Google, Apple ou Microsoft iniciando sessão na conta a partir da aplicação. A primeira vez que abrir a aplicação, será pedido que inicie sessão numa conta.

Se instalou o Bitdefender Mobile Security a partir da sua conta Bitdefender, a aplicação tentará iniciar sessão automaticamente com essa conta.

Para associar o seu dispositivo a uma conta Bitdefender:

1. Introduza o endereço de e-mail e palavra-passe da sua conta Bitdefender nos campos correspondentes. Caso não tenha uma conta Bitdefender e deseje criar uma, pressione o link correspondente para criar uma.
2. Pressione **ENTRAR**.

Para entrar usando uma conta do Facebook, Google ou Microsoft, pressione o serviço que deseja usar na área **OU ENTRAR COM**. Será redirecionado para a página de login do serviço selecionado. Siga as instruções para vincular a sua conta ao Bitdefender Mobile Security.

Nota
O Bitdefender não obtém acesso a qualquer informação confidencial como a palavra-passe da conta que usa para iniciar sessão ou a informação particular dos seus amigos ou contactos.

Configurar proteção

Uma vez que consiga entrar na aplicação, a janela **Configurar proteção** aparecerá. Nós recomendamos que realize estes passos para proteger o seu dispositivo:

- **Estado de subscrição.** Para obter a proteção do Bitdefender Mobile Security, deve ativar o seu produto com uma subscrição, que especificará por quanto tempo poderá utilizar o produto. Assim que esse período acabar, a aplicação para de realizar as suas funções e proteger o seu dispositivo.

  Caso tenha um código de ativação, toque em **EU POSSUO UM CÓDIGO** e, em seguida, toque em **ATIVAR**.

  Se tiver entrado com uma nova conta Bitdefender e não tiver um código de ativação, poderá utilizar o produto por 14 dias gratuitamente.

- **Proteção Web.** Se o seu dispositivo precisar de acessibilidade para ativar a Proteção Web, toque em **ATIVAR**. Será redirecionado para o menu de Acessibilidade. Toque em Bitdefender Mobile Security e depois ligue o botão correspondente.

- **Analisador de Malware.** Realize uma análise única do seu dispositivo para se certificar que ele esteja livre de ameaças. Para iniciar o processo de análise, toque em **ANALISAR AGORA**.

  Assim que o processo de análise começar, o painel aparecerá. Aqui vê o estado de segurança do seu dispositivo.

Painel

Toque no ícone do Bitdefender Mobile Security na secção de aplicações do seu dispositivo para abrir a interface da aplicação.

O Painel fornece informações sobre o estado de segurança do seu dispositivo e através do Autopilot, ele ajuda a reforçar a segurança do seu dispositivo oferecendo recomendações de funcionalidades.

O cartão de estado no topo da janela informa sobre o estado de segurança do dispositivo utilizando mensagens explícitas e cores sugestivas. Se o Bitdefender Mobile Security não tiver alertas, o cartão de estado será verde. Quando um problema de segurança é detectado, a cor do cartão de estado muda para vermelho.

Para lhe oferecer uma operação efetiva e proteção reforçada enquanto realiza diferentes atividades, o **Bitdefender Autopilot** agirá como o seu consultor de segurança pessoal. Dependendo da atividade que você realizar, o Bitdefender do Autopilot fornecerá recomendações contextuais com base na utilização e necessidades do seu dispositivo. Isso irá ajudá-lo a descobrir e se beneficiar das vantagens trazidas pelas funcionalidades incluídas na aplicação do Bitdefender Mobile Security.

Quando houver um processo em curso ou uma função solicitar uma ação sua, é exibido um cartão com mais informações e ações possíveis no Painel de Controlo.

É possível aceder às funcionalidades de Bitdefender Mobile Security e navegar facilmente da barra de navegação inferior:

Analisador de Malware
Permite que inicie uma análise sob demanda e que ative o Armazenamento da Análise. Para mais informação, dirija-se a "*Analisador de Malware*" (p. 266).

Proteção da Internet
Garante uma experiência de navegação segura alertando-lhe sobre páginas Web potencialmente maliciosas. Para mais informação, dirija-se a "*Proteção da Internet*" (p. 269).

VPN
Encripta a comunicação na Internet, ajudando-o a manter a sua privacidade, não importando a rede à qual está ligado. Para mais informação, dirija-se a "*VPN*" (p. 271).

Anti-Theft
Permite que ative ou desative as características Anti Furto e configure as definições Anti Furto. Para mais informação, dirija-se a "*Funcionalidades Anti Furto*" (p. 274).

Privacidade de conta
Verifique se houve fuga de dados nas suas contas online. Para mais informação, dirija-se a "*Privacidade de conta*" (p. 278).

Bloqueio de Aplicativo
Permite que proteja as suas aplicações instaladas, através da configuração de um código PIN de acesso. Para mais informação, dirija-se a "*Bloqueio de Aplicativo*" (p. 280).

Relatórios
Mantém um registo de todas as ações importantes, mudanças de estado e outras mensagens críticas relacionadas com a atividade do seu dispositivo. Para mais informação, dirija-se a "*Relatórios*" (p. 285).

WearON
Comunica com o seu smartwatch para ajudá-lo a encontrar o seu telefone, caso o tenha perdido ou caso se tenha esquecido onde o deixou. Para mais informação, dirija-se a "*WearON*" (p. 286).

22. ANALISADOR DE MALWARE

Bitdefender protege o seu aparelho e dados de aplicações maliciosas utilizando a análise na instalação e análise sob pedido.

A interface do Verificador de Malware oferece uma lista de todos os tipos de ameaças analisadas pela Bitdefender, acompanhadas das suas definições. Basta tocar em qualquer ameaça para ver a sua definição.

Nota
Certifique-se de que o seu dispositivo móvel está ligado à internet. Se o seu dispositivo não estiver ligado à internet, o processo de análise não será iniciado.

- **Análise Na-Instalação**

  Sempre que instala uma aplicação, o Bitdefender Mobile Security verifica-o automaticamente utilizando a tecnologia na nuvem. O mesmo processo de verificação é iniciado toda vez que as aplicações instaladas são atualizadas.

  Se a aplicação for considerada maliciosa, irá aparecer um alerta solicitando que a desinstale. Toque em **Desinstalar** para aceder ao ecrã de desinstalação da aplicação.

- **Verificação por ordem**

  Sempre que quiser saber se as aplicações instaladas no seu dispositivo são seguras para utilização, pode executar uma análise.

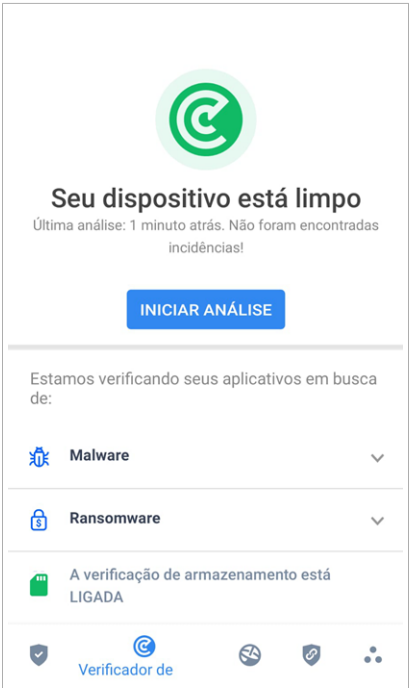
  Para iniciar uma análise sob demanda:

  1. Toque em **Scanner de Malware** na barra de navegação inferior.
  2. Pressione **INICIAR ANÁLISE**.

Nota
São necessárias permissões adicionais no Android 6 para a função Analisador de Malware. Após pressionar o botão **INICIAR ANÁLISE**, selecione **Permitir** para as seguintes opções:

- Permitir que o **Antivírus** faça e administre chamadas?
- Permitir que o **Antivírus** aceda a fotos, multimédia e ficheiros no seu dispositivo?

O processo da análise é exibido e poderá interrompê-lo a qualquer momento.



Análise de Malware

O Bitdefender Mobile Security já vem configurado para analisar o armazenamento interno do seu dispositivo, incluindo qualquer cartão SD ligado. Desta forma, quaisquer aplicações perigosas que estejam no cartão podem ser detetadas antes de causar danos.

Para desativar a definição Análise do armazenamento:

1. Toque **Mais** na barra de navegação inferior.
2. Toque em **Definições**.
3. Desative o interruptor **Análise do armazenamento** na área Scanner de Malware.

Caso sejam detetadas quaisquer aplicações maliciosas, serão exibidas informações sobre elas e poderá removê-las tocando no botão **DESINSTALAR**.

O cartão do analisador de Malware exibe o estado do seu dispositivo. Quando está seguro, o cartão fica verde. Quando o dispositivo necessitar de análise ou de alguma ação sua, o cartão ficará vermelho.

Se a sua versão do Android é a 7.1 ou posterior, pode aceder a um atalho para o Verificador de Malware, para poder executar as verificações de forma mais rápida, sem ter de abrir a interface do Bitdefender Mobile Security. Para isso, carregue continuamente no ícone do Bitdefender no seu ecrã de Início ou na gaveta de aplicações e, de seguida, selecione o ícone .

23. PROTEÇÃO DA INTERNET

A Segurança na Web usa os serviços em nuvem do Bitdefender para verificar as páginas da web que acede com o navegador padrão do Android, Google Chrome, Firefox, Opera, Opera Mini, Edge, Samsung Internet e Dolphin. Uma lista completa com os navegadores suportados está disponível na secção Segurança na Web.

Nota

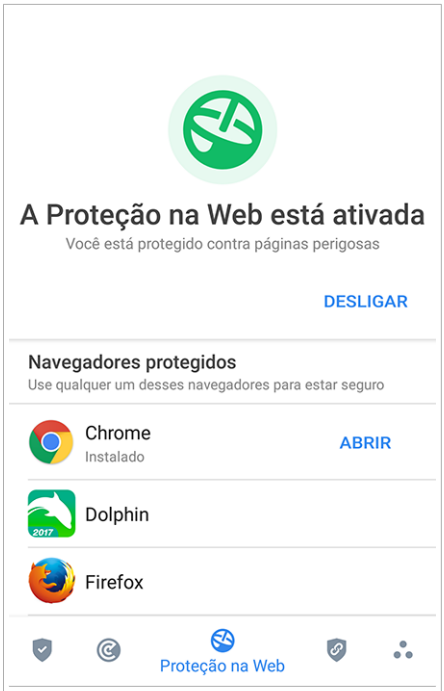
São necessárias permissões adicionais no Android 6 para a função Web Protection.

Ative a permissão para registar como serviço de Acessibilidade e pressione **LIGAR** quando solicitado. Toque em **Antivírus** e ative o botão, depois confirme que concorda com o acesso às permissões do seu dispositivo.

Cada vez que aceder a um site bancário, a Proteção Web Bitdefender está pronta para notificá-lo para utilizar Bitdefender VPN. A notificação aparece na barra de estado. Recomendamos que utilize a Bitdefender VPN enquanto tiver a sessão iniciada na sua conta bancária para que os seus dados possam permanecer seguros de possíveis quebras de segurança.

Para desativar a notificação Proteção Web:

1. Toque **Mais** na barra de navegação inferior.
2. Toque em **Definições**.
3. Desligue o interruptor correspondente na área de Proteção Web.



Proteção da Internet

24. VPN

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

A VPN funciona como um túnel entre o seu dispositivo e a rede à qual se liga, protegendo a sua ligação, encriptando os seus dados utilizando uma encriptação de nível bancário e escondendo o seu endereço IP onde quer que esteja. O seu tráfego é redirecionado por meio de um servidor separado, tornando o seu dispositivo quase impossível de ser identificado entre os incontáveis dispositivos que usam os nossos serviços. Além disso, enquanto estiver ligado à Internet com o Bitdefender VPN, pode aceder a conteúdos que normalmente são restritos em áreas específicas.

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

Há duas formas de ativar ou desativar o Bitdefender VPN:

- Toque em **LIGAR** na placa VPN do Painel.

  O estado do Bitdefender VPN é exibido.

- Toque em **VPN** na barra de navegação inferior e, em seguida, toque em **LIGAR**.

  Pressione **CONECTAR** sempre que quiser permanecer protegido enquanto estiver conectado a redes sem fios não seguras.

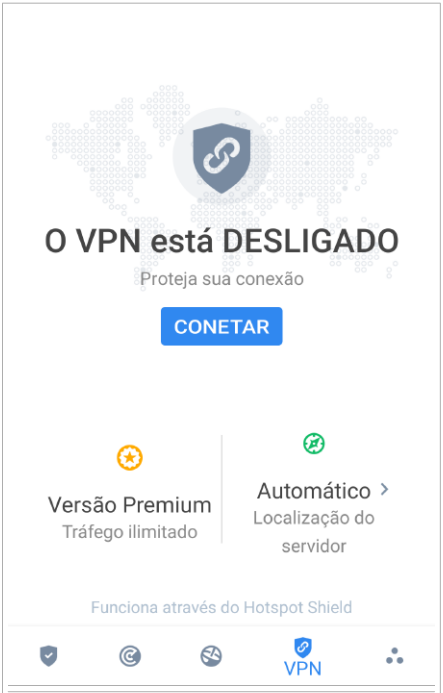
  Pressione **DESCONECTAR** quando desejar desativar a ligação.

Nota
Na primeira vez que ligar o VPN, deve permitir a solicitação do Bitdefender para configurar uma ligação VPN que monitorizará o tráfego de rede. Toque em **OK** para continuar.

Se a sua versão do Android é a 7.1 ou posterior, pode aceder a um atalho para o a VPN do Bitdefender sem ter de abrir a interface do Bitdefender Mobile Security. Para isso, carregue continuamente no ícone do Bitdefender no seu ecrã de Início ou na gaveta de aplicações e, de seguida, selecione o ícone .

Para economizar bateria, recomendamos que desligue a VPN quando não precisar de usá-la.

Caso pretenda ligar-se a um servidor da sua preferência, pressione **Localização do servidor** na inerface da VPN e selecione a localização que pretende.



VPN

Definições da VPN

Para uma configuração avançada da sua VPN:

1. Toque **Mais** na barra de navegação inferior.
2. Toque em **Definições**.

Nas área VPN, pode configurar as seguintes opções:

- Acesso rápido ao VPN - uma notificação aparecerá na barra de estado do seu dispositivo permitindo que ligue o VPN rapidamente.
- Alerta de Wi-Fi aberto - sempre que se ligar a uma rede Wi-Fi aberta, a barra de estado do seu dispositivo vai pedir-lhe para utilizar o VPN.

25. FUNCIONALIDADES ANTI FURTO

Bitdefender pode ajudá-lo a localizar o seu dispositivo e impedir que os seus dados pessoais caiam nas mãos erradas.

Tudo o que necessita de fazer é ativar o Anti-roubo a partir do dispositivo e, quando necessário, aceder à **Bitdefender Central** a partir de qualquer Web browser, em qualquer lugar.

> **Nota**
> A interface do Antifurto também inclui uma hiperligação para a nossa aplicação da Central Bitdefender no Google Play Store. Pode utilizar esta hiperligação para transferir a aplicação, caso ainda não o tenha feito.

Bitdefender Mobile Security oferece as seguintes funcionalidades Anti Furto:

Localização Remota

Visualize a localização atual do seu dispositivo no Google Maps. A localização é atualizada a cada 5 segundos para que possa controlá-lo se estiver em movimento.

A precisão da localização depende do quanto o Bitdefender é capaz de o determinar:

- Caso o GPS esteja ativado no dispositivo, a sua localização pode ser determinada no alcance de dois metros, desde que esteja ao alcance dos satélites GPS (ou seja, fora de um edifício).
- Se o dispositivo estiver dentro de um edifício, a sua localização pode ser determinada no alcance de 10 metros caso o Wi-Fi esteja ativado e existam rede sem fios disponíveis no seu alcance.
- Caso contrário, a localização será determinada utilizando apenas as informações da rede móvel, que pode oferecer uma precisão não melhor que várias centenas de metros.

Bloqueio Remoto

Bloqueie o ecrã do seu dispositivo e defina uma palavra-passe para desbloquear o mesmo.

Limpeza Remota

Remova todos os dados pessoais do seu dispositivo roubado.

Enviar alerta para o dispositivo (Scream)

Envie uma mensagem remotamente para ser exibida no ecrã do dispositivo ou para emitir um som alto no altifalante do dispositivo.

Caso venha a perder o seu dispositivo, pode informar a quem o encontrar como pode ser devolvido, exibindo uma mensagem no ecrã do dispositivo.

Caso tenha perdido o seu dispositivo e exista a possibilidade de não estar longe de si (por exemplo, em algum lugar em casa ou no escritório), que melhor maneira de encontrá-lo do que fazê-lo tocar um som alto? O som será reproduzido mesmo se o dispositivo estiver no modo silencioso.

A ativar o Anti Furto

Para ativar a função Anti Furto, basta completar o processo de configuração do cartão Anti Furto disponível no Painel de Controlo.

Também pode ativar a função Anti Furto seguindo estas instruções:

1. Toque **Mais** na barra de navegação inferior.
2. Toque em **Anti-roubo**.
3. Toque em **ATIVAR**.
4. O seguinte procedimento será iniciado para ajudá-lo na ativação desta função:

   Nota

   São necessárias permissões adicionais no Android 6 para a função Anti Furto. Para ativar, siga estes passos:

   a. Toque em **Ativar Anti Furto**, depois toque em **LIGAR**.

   b. Permite que o **Antivírus** aceda à localização deste dispositivo

   a. **Conceder privilégios de administrador**

      Estes privilégios são essenciais para o funcionamento da função Anti Furto e devem ser concedidas antes de continuar.

   b. **Definir PIN para a aplicação**

      Para evitar o acesso não autorizado ao seu dispositivo, tem de definir um código PIN. Sempre que for feita uma tentativa de acesso ao seu

dispositivo, é necessário introduzir o PIN primeiro. De forma alternativa, em dispositivos que suportam a autenticação por leitura de impressão digital, uma confirmação por digital pode ser utilizada em vez do código PIN configurado.

O mesmo código PIN é utilizado pelo Bloqueio de Aplicação para proteger as suas aplicações instaladas.

c. **Ativar o Tirar Foto**

Sempre que alguém tentar desbloquear o seu dispositivo sem sucesso enquanto Tirar Foto estiver ativado, o Bitdefender tira uma foto.

Dokładniej, za każdym razem, gdy kod PIN, hasło lub potwierdzenie odcisku palca, które ustawiłeś, aby chronić urządzenie, jest trzykrotnie błędnie wpisane, robione jest zdjęcie przy użyciu przedniego aparatu. A foto é guardada com o carimbo de data/hora e o motivo e pode ser vista quando abre Bitdefender Mobile Security da janela Antirroubo. Alternatywnie można wyświetlić zrobione zdjęcie w koncie Bitdefender:

i. Vá para: https://central.bitdefender.com.

ii. Aceda à sua conta.

iii. Pressione ☰ no canto superior esquerdo do ecrã e, em seguida, selecione **Os meus dispositivos**.

iv. Selecione o dispositivo Android e o separador **Antirroubo**.

v. Toque em ⋮ junto a **Verificar os instantâneos** para ver as últimas fotos tiradas.

Só são guardadas as duas fotografias mais recentes.

Ao ativar o recurso Anti-roubo, pode ativar ou desativar os comandos de Controlo Web de maneira individual na janela de Anti-roubo tocando nas opções correspondentes.

Usar as funcionalidades Anti-Roubo a partir da Bitdefender Central

Nota
Todas as funcionalidades de Anti Furto necessitam que a opção **Dados em segundo plano** esteja ativa nas configurações de Dados do seu dispositivo.

Para aceder às funções anti-furto da sua conta Bitdefender:

1. Aceda Bitdefender Central.
2. Pressione no canto superior esquerdo do ecrã e, em seguida, selecione **Os meus dispositivos**.
3. Na janela **OS MEUS DISPOSITIVOS**, selecione o cartão de dispositivo pretendido.
4. Selecione o separador **Anti Furto**.
5. No último campo da janela, toque no ícone e, em seguida, no botão com a função correspondente que deseja utilizar:

   Localizar - exibe a localização do seu dispositivo no Google Maps.

   Alerta - escreva uma mensagem para ser exibida no ecrã do seu dispositivo e/ou para fazer com que o seu dispositivo emita um alarme sonoro.

   Bloquear - bloqueie o seu dispositivo e defina um PIN para desbloqueá-lo.

   Limpar - eliminar todos os dados do seu dispositivo.

   Importante
   Após apagar toda a informação de um dispositivo, todas as funcionalidades Anti-Roubo deixam de funcionar.

   MOSTRAR IP - exibe o último endereço de IP para o dispositivo selecionado.

Funcionalidades Antirroubo

Se pretender ativar ou desativar os comandos remotos:

1. Toque **Mais** na barra de navegação inferior.
2. Toque em **Anti-roubo**.
3. Ative ou desative as opções pretendidas.

26. PRIVACIDADE DE CONTA

A Privacidade de Conta Bitdefender deteta se houve fuga de dados nas contas que utiliza para fazer pagamentos online, compras ou iniciar sessão em diferentes aplicações ou sites Web. Os dados armazenados numa conta podem ser palavras-passe, informações de cartão de crédito ou informações de conta bancária e, se não forem devidamente protegidos, pode sofrer roubo de identidade ou invasão de privacidade.

O estado de privacidade de uma conta é apresentado depois da validação.

A novas verificações automáticas são definidas para serem executadas em segundo plano, mas é possível executar análises manuais diariamente.

As notificações serão apresentadas sempre que são detetadas novas quebras que incluam qualquer uma das contas de e-mail validadas.

Para começar a proteger informações pessoais:

1. Toque **Mais** na barra de navegação inferior.
2. Toque em **Privacidade de conta**.
3. Toque em **INICIAR**.
4. O endereço de e-mail utilizado para criar a sua conta da Bitdefender aparece e é automaticamente adicionado à lista de contas monitorizadas.
5. Para adicionar outra conta, toque em **ADICIONAR CONTA** na janela de Privacidade da Conta e escreva o endereço de e-mail.

   Toque em **ADICIONAR** para continuar.

   Bitdefender necessita de validar esta conta antes de apresentar informações privadas. Portanto, é enviado um e-mail com um código de validação para o endereço de e-mail fornecido.

   Verifique a caixa de entrada e digite o código recebido na área **Privacidade de Conta** da aplicação. Se não conseguir encontrar o e-mail de validação na pasta Caixa de Entrada, verifique a pasta Spam.

   O estado de privacidade da conta validada é apresentado.

Se forem detetadas quebras nas suas contas, recomendamos que altere as palavras-passe assim que possível. Para criar uma palavra-passe forte e segura, tenha em mente estas dicas:

- Oito carateres no mínimo.
- Carateres maiúsculos e minúsculos.
- Pelo menos um número ou símbolo, como #, @, % ou !.

Ao proteger uma conta que constava de uma violação de privacidade, pode confirmar as alterações ao marcar a(s) quebra(s) identificada(s) como **Resolvido**. Para tal:

1. Toque **Mais** na barra de navegação inferior.
2. Toque em **Privacidade de conta**.
3. Toque na conta que acabou de proteger.
4. Toque na quebra de onde protegeu a conta.
5. Toque em **RESOLVIDO** para confirmar que a conta está protegida.

Quando todas as quebras detetadas estiverem marcadas como **Resolvido**, a conta já não aparece como quebra, pelo menos até à deteção de uma nova quebra.

Para parar de ser notificado sempre que são realizadas análises automáticas:

1. Toque **Mais** na barra de navegação inferior.
2. Toque em **Definições**.
3. Desligue o interruptor correspondente na área Privacidade da conta.

27. BLOQUEIO DE APLICATIVO

Aplicações instaladas, como e-mails, fotos ou mensagens, podem conter dados pessoais que gostaria que permanecessem privados, limitando o acesso a estes de forma seletiva.

O Bloqueio de Aplicação ajuda-o a bloquear o acesso indesejado às aplicações, através da configuração de um código PIN de acesso de segurança. O código PIN deve ter no mínimo 4 dígitos e no máximo 8 e será solicitado sempre que pretender aceder às aplicações restritas.

De forma alternativa, em dispositivos que suportam a autenticação por leitura de impressão digital, uma confirmação por digital pode ser utilizada em vez do código PIN configurado.

A ativar o Bloqueio de Aplicação

Para restringir o acesso a aplicações específicas, configure o Bloqueio de Aplicação através do cartão exibido no Painel de Controlo após a ativação da função Anti Furto.

Também pode ativar o Bloqueio de Aplicação seguindo estas instruções:

1. Toque **Mais** na barra de navegação inferior.
2. Toque em **Bloqueio da aplicação**.
3. Toque em **ATIVAR**.
4. Permitir acesso aos dados de utilização para Bitdefender Security.
5. Permitir **prioridade em relação a outras aplicações**.
6. Volte à aplicação, configure o código de acesso e pressione **DEFINIR PIN**.

   Nota
   Este passo será apenas necessário se não tiver configurado o PIN na função Anti Furto.

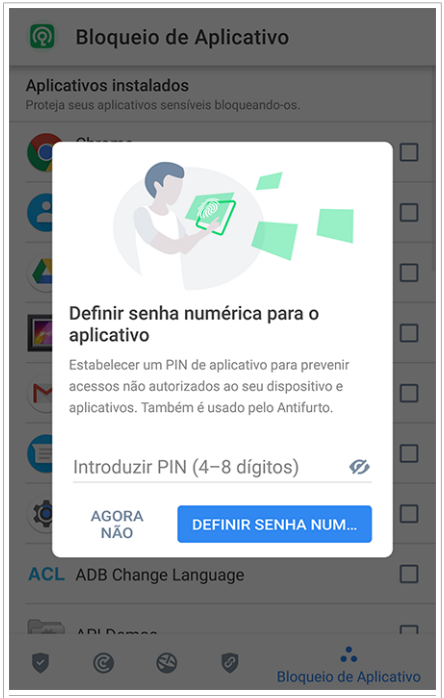
7. Permite que a opção Tirar Foto apanhe qualquer intruso que tente aceder aos seus dados pessoais.

Nota
São necessárias permissões adicionais no Android 6 para a função Tirar Foto.
Para ativá-la, permita que o **Antivírus** tire fotos e grave vídeos.

8. Selecione as aplicações que gostaria de proteger:

Utilizar o PIN ou a impressão digital errada cinco vez seguidas ativará uma pausa de 30 segundos. Dessa forma, qualquer tentativa de aceder às aplicações protegidas será bloqueada.

Nota
O mesmo código PIN é utilizado pelo Anti Furto para ajudá-lo a localizar o seu dispositivo.



Bloqueio de Aplicativo

MODO DE BLOQUEIO

A primeira vez que adicionar uma aplicação ao Bloqueio de aplicação, o ecrã Modo de bloqueio de aplicação aparece. Aqui pode escolher quando a função Bloqueio de Aplicações deve proteger as aplicações instaladas no seu dispositivo.

Pode selecionar entre uma das seguintes opções:

- **Necessita sempre de desbloqueio** - sempre que as aplicações bloqueadas são acedidas, o código PIN ou impressão digital que configurou será utilizado.
- **Manter desbloqueado até o ecrã apagar** - o acesso às suas aplicações será válido até o ecrã apagar.
- **Bloquear após 30 segundos** - é possível sair e aceder novamente às suas aplicações desbloqueadas num espaço de 30 segundos.

Caso pretenda alterar a definição selecionada:

1. Toque **Mais** na barra de navegação inferior.
2. Toque em **Definições**.
3. Toque em **Requer sempre desbloqueio** na área Bloqueio de aplicação.
4. Escolha a opção desejada.

Definições do Bloqueio de Aplicação

Para uma configuração avançada do Bloqueio de aplicação:

1. Toque **Mais** na barra de navegação inferior.
2. Toque em **Definições**.

Na área Bloqueio de aplicação, é possível configurar as opções seguintes:

- **Sugestão de aplicação confidencial** - receba uma notificação de bloqueio sempre que instalar uma aplicação confidencial.
- **Requer sempre desbloqueio** - escolha uma das opções de bloqueio e desbloqueio disponíveis.
- **Desbloqueio inteligente** - mantenha as aplicações desbloqueadas enquanto estiver ligado a redes Wi-Fi de confiança.

- **Teclado aleatório** - previne a leitura do PIN ao mostrar os números de forma aleatória.

Tirar foto

Com o Tirar Foto (Snap Photo) da Bitdefender pode apanhar os seus amigos ou familiares em flagrante. Assim pode educá-los a não bisbilhotar os seus ficheiros pessoais ou as aplicações que utiliza.

A função funciona de forma fácil: sempre que o código PIN ou a confirmação por impressão digital que definiu para proteger as suas aplicações for inserido de forma errada três vezes seguidas, será tirada uma foto com a câmara frontal. A foto será guardada com a informação sobre o dia, hora e motivo, e poderá ser visualizada quando abrir o Bitdefender Mobile Security e aceder à função do Bloqueio de Aplicação.

Nota

Esta função está disponível apenas para telefones que têm uma câmara frontal.

Para configurar a função de Instantâneo para Bloqueio de aplicação:

1. Toque **Mais** na barra de navegação inferior.
2. Toque em **Definições**.
3. Ative o interruptor correspondente na área Instantâneo.

As fotos tiradas quando é introduzido o PIN incorreto são exibidas na janela de Bloqueio de Aplicação e podem ser visualizadas em ecrã completo.

De forma alternativa, eles podem ser vistos na sua conta Bitdefender:

1. Vá para: https://central.bitdefender.com.
2. Aceda à sua conta.
3. Pressione no canto superior esquerdo do ecrã e, em seguida, selecione **Os meus dispositivos**.
4. Selecione o dispositivo Android e o separador **Antirroubo**.
5. Toque em junto a **Verificar os instantâneos** para ver as últimas fotos tiradas.

Só são guardadas as duas fotografias mais recentes.

Para parar o carregamento de fotos tiradas na sua conta Bitdefender:

1. Toque **Mais** na barra de navegação inferior.
2. Toque em **Definições**.
3. Desative **Carregar fotos** na área Instantâneo.

Desbloqueio Inteligente

Um método fácil para que a função Desbloqueio de Aplicação deixe de solicitar o código PIN ou a confirmação por impressão digital para as aplicações protegidas sempre que acede é ativar o Desbloqueio Inteligente.

Com o Desbloqueio Inteligente pode configurar as redes Wi-Fi que costuma utilizar como fiáveis e quando estiver ligado a elas, as definições de bloqueio do Bloqueio de Aplicação serão desativadas para as aplicações protegidas.

Para configurar a função Desbloqueio inteligente:

1. Toque **Mais** na barra de navegação inferior.
2. Toque em **Bloqueio da aplicação**.
3. Toque no botão .
4. Toque no interruptor ao lado do **Smart Unlock**, caso a funcionalidade ainda não esteja ativada

   Valide utilizando a sua impressão digital ou o seu PIN.

   A primeira vez que ativar a funcionalidade, deverá ativar a permissão de localização. Toque no botão **PERMITIR** e, em seguida, prima **PERMITIR** novamente.
5. Toque em **ADICIONAR** para configurar a ligação Wi-Fi que está a utilizar atualmente como sendo de confiança.

Sempre que mudar de opinião, desative a função e as redes Wi-Fi que configurou como fiáveis serão tratadas como não fiáveis.

28. RELATÓRIOS

O recurso Relatórios mantém um registo detalhado de eventos relacionados com a atividade de análise do seu dispositivo.

Sempre que acontecer algo relevante para a segurança do seu dispositivo, será adicionada uma nova mensagem aos Relatórios.

Para aceder à secção Relatórios:

1. Toque **Mais** na barra de navegação inferior.
2. Toque em **Relatórios**.

Os seguintes separadores estão disponíveis na janela Relatórios:

- **RELATÓRIOS SEMANAIS** - aqui tem acesso ao estado de segurança e às tarefas executadas da semana atual e anterior. O relatório semanal é gerado todos os domingos e irá receber uma notificação com a informação sobre a sua disponibilidade.

  Todas as semanas será exibida uma nova dica nesta secção, então lembre-se de conferir regularmente para obter o máximo do que a sua aplicação pode oferecer.

  Para parar de receber notificações sempre que um relatório é gerado:

  1. Toque **Mais** na barra de navegação inferior.
  2. Toque em **Definições**.
  3. Desative o interruptor **Notificação de novo relatório** na área Relatórios.

- **REGISTO DE ATIVIDADES** - aqui poderá aceder a informações detalhadas sobre as atividades da sua aplicação Bitdefender Mobile Security, desde quando foi instalada no seu dispositivo Android.

  Para eliminar o relatório de atividade disponível:

  1. Toque **Mais** na barra de navegação inferior.
  2. Toque em **Definições**.
  3. Toque em **Limpar relatório de atividade** e, em seguida, toque em **LIMPAR**.

29. WEARON

Com WearON do Bitdefender, pode encontrar facilmente o seu smartphone, esteja ele na sala de reunião do escritório ou sob uma almofada no sofá. O dispositivo pode ser encontrado mesmo se o modo silencioso estiver ativado.

Mantenha esta função ativada para garantir que terá sempre o seu smartphone por perto.

Nota
A função funciona com Android 4.3 e Android Wear.

A ativar o WearON

Para utilizar o WearON, só precisa de ligar o seu smartwatch à aplicação do Bitdefender Mobile Security e ativar a função com o seguinte comando de voz:

Start:<Where is my phone>

O **Bitdefender WearON** tem dois comandos:

1. **Alerta de Telefone**

   Com o recurso Alerta do Telefone encontra rapidamente o seu smartphone, sempre que se afastar muito dele.

   Se estiver com o seu smartwatch, ele detectará automaticamente a aplicação no seu telefone e irá vibrar sempre que estiver muito longe do seu relógio, mais precisamente, quando a ligação de Bluetooth for perdida.

   Para ativar esta função, abra o Bitdefender Mobile Security, toque em **Configurações Globais** no menu e selecione o botão correspondente na secção WearON.

2. **Toque alto**

   Encontrar o seu telefone nunca foi tão fácil. Quando se esquecer onde deixou o seu telefone, toque no comando Apitar no seu relógio para fazer o seu telefone apitar.

30. SOBRE

Para mais informações sobre a versão do Bitdefender Mobile Security que tem instalada, para aceder e ler o Acordo de subscrição e Política de privacidade, e visualizar as licenças Open-source:

1. Toque **Mais** na barra de navegação inferior.
2. Toque em **Definições**.
3. Toque na opção desejada na área Sobre.

31. BITDEFENDER CENTRAL

Bitdefender Central é a plataforma Web onde tem acesso às funcionalidades e serviços online do produto, e pode realizar remotamente tarefas importantes nos dispositivos em que o Bitdefender estiver instalado. Pode aceder à sua conta Bitdefender desde qualquer computador ou dispositivo móvel ligado à internet, indo para https://central.bitdefender.com, ou diretamente pela aplicação da Bitdefender Central em dispositivos Android e iOS.

Para instalar a aplicação da Bitdefender Central nos seus dispositivos:

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

Assim que iniciar sessão, pode começar a fazer o seguinte:

- Transfira e instale o Bitdefender nos sistemas operativos Windows, macOS, iOS e Android. Os produtos disponíveis para download são:
  - Bitdefender Mobile Security
  - Bitdefender Mobile Security for iOS
  - O Antivírus Bitdefender para Mac
  - A linha de produtos Windows da Bitdefender
- Gerir e renovar as suas subscrições do Bitdefender.
- Adicionar novos dispositivos à sua rede e gerir as suas funcionalidades onde quer que esteja.
- Proteja os dispositivos de rede e os seus dados contra roubo ou perda com o Anti-Roubo.

Aceder à sua conta Bitdefender

Há duas formas de aceder à Bitdefender Central

- Do seu navegador Web:
  1. Abrir um navegador em qualquer dispositivo com acesso à internet.

2. Vá para: https://central.bitdefender.com.
3. Inicie sessão na sua conta com o seu endereço de e-mail e palavra-passe.

- No seu dispositivo Android ou iOS:

  Abra a aplicação da Bitdefender Central que instalou.

Nota
Neste material, recebe as opções e instruções disponíveis na plataforma web.

Autenticação de dois fatores

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

Ativar autenticação de dois fatores

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

Para ativar a autenticação de dois fatores:

1. Aceda Bitdefender Central.
2. Toque no ícone no canto superior direito do ecrã.
3. Clique em **Conta do Bitdefender** no menu deslizante.
4. Selecione o separador **Palavra-passe e segurança**.
5. Toque em **Autenticação em dois fatores**.
6. Toque em **INICIAR**.

   Selecione uma das seguintes opções:

   - **Aplicação de autenticação** - utilize uma apliação de autenticação para gerar um código sempre que quiser aceder à sua conta Bitdefender.

Caso queira utilizar a aplicação de autenticação, mas não tem a certeza de qual escolher, aparecerá uma lista com as aplicações de autenticação recomendadas.

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

b. Para uniciar sessão num dispositivo Android ou iOS, utilize o seu dispositivo para digitalizar o código QR.

Para iniciar sessão utilizando um portátil ou um computador, pode adicionar manualmente o código apresentado.

Toque em **CONTINUAR**.

c. Insira o código fornecido pela aplicação ou o apresentado no passo anterior e, em seguida, toque em **ATIVAR**.

- **E-mail** - sempre que iniciar sessão na sua conta Bitdefender, o código de verificação será enviado para a sua caixa de e-mail. Verifique a sua conta de e-mail e introduza o código fornecido.

a. Toque em **UTILIZAR E-MAIL** para começar.

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

Lembre que tem cinco minutos para verificar a sua conta de e-mail e introduzir o código gerado. Se o tempo expirar, deverá gerar uma nova hiperligação seguindo os mesmos passos.

c. Toque em **ATIVAR**.

d. Receberá dez códigos de ativação. Pode copiar, transferir ou imprimir a lista e usá-la caso perca o seu endereço de e-mail, caso contrário não poderá iniciar sessão. Cada código pode ser utilizado apenas uma vez.

e. Toque em **CONCLUÍDO**.

Caso queira deixar de utilizar a autenticação de dois fatores:

1. Toque em **DESATIVAR A AUTENTICAÇÃO EM DOIS FATORES**.
2. Verifique a sua aplicação ou conta de e-mail e introduza o código que recebeu.

   Caso tenha escolhido receber o código de autenticação por e-mail, terá cinco minutos para verificar a sua conta de e-mail e introduzir o código gerado. Se o tempo expirar, deverá gerar uma nova hiperligação seguindo os mesmos passos.

3. Confirme a sua escolha.

Adicionar dispositivos fiáveis

Para garantir que apenas pode aceder à sua conta Bitdefender, poderemos solicitar o código de segurança primeiro. Caso pretenda ignorar este passo sempre que se ligar com o mesmo dispositivo, recomendamos identificá-lo como um dispositivo fiável.

Para adicionar dispositivos como dispositivos fiáveis:

1. Aceda Bitdefender Central.
2. Toque no ícone no canto superior direito do ecrã.
3. Clique em **Conta do Bitdefender** no menu deslizante.
4. Selecione o separador **Palavra-passe e segurança**.
5. Toque em **Dispositivos fiáveis**.
6. Será mostrada a lista com os dispositivos Bitdefender instalados. Toque no dispositivo pretendido.

Pode adicionar os dispositivos que pretender, desde que tenham o Bitdefender instalado e a sua subscrição seja válida.

Meus dispositivos

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

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

1. Aceda Bitdefender Central.
2. Pressione no canto superior esquerdo do ecrã e, em seguida, selecione **Os meus dispositivos**.
3. Toque no cartão de dispositivo pretendido e, em seguida, toque em no canto superior direito do ecrã.
4. Selecione **Definições**.

5. Introduza um novo nome no campo **Nome do dispositivo** e, em seguida, selecione **GUARDAR**.

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

1. Aceda Bitdefender Central.
2. Pressione ☰ no canto superior esquerdo do ecrã e, em seguida, selecione **Os meus dispositivos**.
3. Toque no cartão de dispositivo pretendido e, em seguida, toque em ⋮ no canto superior direito do ecrã.
4. Selecione **Perfil**.
5. Clique em **Add owner** e, em seguida, preencha os respetivos campos. Personalize o perfil adicionando uma fotografia e selecionando a data de nascimento.
6. Toque em **ADICIONAR** para guardar o perfil.
7. Selecione o proprietário pretendido na lista **Proprietário do dispositivo** e, em seguida, toque em **ATRIBUIR**.

Para mais ações remotas e informações sobre o seu produto Bitdefender num dispositivo específico, selecione o cartão de dispositivo pretendido.

Quando selecionar no cartão de dispositivo, ficam disponíveis os seguintes separadores:

- **Painel**. Nesta janela, pode visualizar os detalhes sobre o dispositivo selecionado, verificar o seu estado de proteção, o estado do Bitdefender VPN e quantas ameaças foram bloqueadas nos últimos sete dias. O estado de proteção pode estar verde, quando não houver problemas a afetar o seu dispositivo, amarelo, quando o dispositivo exigir a sua atenção, ou vermelho, quando o dispositivo estiver em risco. Quando houver problemas a afetar o seu dispositivo, clique a seta pendente na área de estado acima para saber mais detalhes. A partir daqui poderá resolver manualmente os problemas que afetam a segurança dos seus dispositivos.
- **Proteção**. a partir desta janela pode executar uma Análise remota no seu dispositivo. Toque no botão **ANALISAR** para iniciar o processo. Também pode conferir quando é que a última verificação foi realizada no dispositivo e aceder a um relatório da última verificação, contendo as informações mais importantes.

- **Antirroubo**. Caso tenha perdido o seu dispositivo, pode localizá-lo e realizar ações remotas com a função Anti Furto. Toque em **LOCALIZAR** para descobrir a localização do seu dispositivo. A última localização conhecida será exibida, juntamente com a hora e com a data. Para mais detalhes sobre esta função, aceda a "*Funcionalidades Anti Furto*" (p. 274).

As minhas subscrições

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

Verificar subscrições disponíveis

Para verificar as suas subscrições disponíveis:

1. Aceda Bitdefender Central.
2. Pressione ☰ no canto superior esquerdo do ecrã e, em seguida, selecione **As minhas subscrições**.

Aqui pode aceder às informações sobre a disponibilidade das subscrições que possui e o número de dispositivos a utilizar cada uma delas.

Pode adicionar um novo dispositivo a uma subscrição ou renová-la selecionando um cartão de subscrição.

Adicionar um novo dispositivo

Se a sua assinatura abranger mais de um dispositivo, pode adicionar um novo dispositivo e instalar nele o seu Bitdefender Mobile Security, conforme descrito em "A instalar Bitdefender Mobile Security" (p. 261).

Renew subscription

Se lhe restam menos de 30 dias de assinatura e desativou a renovação automática, é possível renová-la manualmente seguindo os seguintes passos:

1. Aceda Bitdefender Central.
2. Pressione ☰ no canto superior esquerdo do ecrã e, em seguida, selecione **As minhas subscrições**.
3. Selecione o cartão de subscrição pretendido.
4. Toque em **RENOVAR** para continuar.

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

32. PERGUNTAS FREQUENTES

Porque é que o Bitdefender Mobile Security requer a ligação à internet?

A aplicação precisa de comunicar com os servidores do Bitdefender para determinar o estado de segurança das aplicações que analisa e das páginas web que visita e também para receber os comandos da sua conta Bitdefender quando utilizar a função Anti Furto.

Para que é que o Bitdefender Mobile Security precisa de cada permissão?

- Acesso à Internet -> utilizado para comunicação na nuvem.
- Analisa o estado do telefone e identidade -> utilizado para detetar se o dispositivo está ligado à internet e para extrair determinadas informações do dispositivo necessárias para criar um ID exclusivo ao comunicar com Bitdefender nuvem.
- Ler e escrever marcadores do navegador -> o módulo Web Protection apaga sites maliciosos do seu histórico de navegação.
- Ler o registo de dados -> o Bitdefender Mobile Security deteta traços de atividades de ameaças dos registos Android.
- Localização -> Necessária para a localização remota.
- Câmara -> necessária para Tirar foto (Snap photo).
- Armazenamento -> utilizado para permitir que o Analisador de Malware verifique o cartão SD.

Como é que posso parar de submeter informações de Bitdefender sobre aplicações suspeitas?

Por predefinição, Bitdefender Mobile Security envia relatórios aos servidores de Bitdefender sobre aplicações suspeitas que esteja a instalar. Estas informações são essenciais para melhorar a deteção de ameaças e pode ajudar-nos a oferecer-lhe uma melhor experiência no futuro. Caso pretenda parar de enviar-nos informações sobre aplicações suspeitas:

1. Toque **Mais** na barra de navegação inferior.
2. Toque em **Definições**.
3. Desligue **Deteção dentro da nuvem** na área Scanner de Malware.

Onde posso ver mais informações sobre a atividade do aplicação?

O Bitdefender Mobile Security mantém um registo de todas as ações importantes, mudanças de estado e outras mensagens críticas relacionadas com a sua atividade. Para aceder, consulte a atividade da aplicação:

1. Toque **Mais** na barra de navegação inferior.
2. Toque em **Relatórios**.

   Na janela de RELATÓRIOS SEMANAIS, é possível aceder aos relatórios que foram gerados todas as semanas e na janela REGISTO DE ATIVIDADE, pode visualizar as informações sobre a atividade da sua aplicação Bitdefender.

Esqueci-me do código PIN que defini para proteger a minha aplicação. What do I do?

1. Aceda Bitdefender Central.
2. Pressione no canto superior esquerdo do ecrã e, em seguida, selecione **Os meus dispositivos**.
3. Toque no cartão de dispositivo pretendido e, em seguida, toque em no canto superior direito do ecrã.
4. Selecione **Definições**.
5. Recupere o PIN no campo **PIN da Aplicação**.

Como é que posso alterar o código PIN que definir para Bloqueio de aplicação e Antirroubo?

Se pretende alterar o código PIN que definir para Bloqueio de aplicação e Antirroubo:

1. Toque **Mais** na barra de navegação inferior.
2. Toque em **Definições**.
3. Toque em **CÓDIGO PIN** de segurança na área Antirroubo.
4. Introduza o código PIN atual.
5. Introduza o novo código PIN que pretende definir.

Como posso desligar a função Bloqueio de Aplicação?

Não há qualquer opção para desligar a função Bloqueio de Aplicação, mas pode desativá-la facilmente ao desmarcar as caixas próximas às aplicações selecionadas depois que validar o PIN ou impressão digital definida.

Como posso definir outra rede sem fios como fiável?

Em primeiro, tem de ligar o seu dispositivo à rede sem fios que pretende definir como de confiança. Em seguida, siga estes passos:

1. Toque **Mais** na barra de navegação inferior.
2. Toque em **Bloqueio da aplicação**.
3. Toque em no canto superior direito.
4. Toque em **ADICIONAR** ao lado da rede que pretende definir como de confiança.

Como posso parar de ver fotografias associadas tiradas nos meus dispositivos?

Para parar de tornar visíveis as fotografias associadas tiradas nos seus dispositivos:

1. Aceda Bitdefender Central.
2. Toque no canto superior direito do ecrã.
3. Clique em **A Minha Conta** no menu deslizante.
4. Selecione o separador **Definições**.
5. Desative a opção **Mostrar/não mostrar fotografias tiradas nos seus dispositivos** .

Como posso manter as minhas compras online seguras?

As compras online têm riscos elevados quando alguns detalhes são ignorados. Para não ser vítima de fraude, recomendamos o seguinte:

- Matenha a aplicação de segurança atualizada.
- Efetue pagamentos online apenas com proteção do comprador.
- Utilize uma VPN ao estabelecer ligação com a internet a partir de redes sem fios não protegidas e públicas.
- Preste atenção às palavras-passe que atribuiu às suas contas online. Têm de ser fortes e incluir letras maiúsculas e minúsculas, números e símbolos (@, !, %, #, etc.).

- Certifique-se de que as informações são enviadas por ligações seguras. A extensão do site Web online tem de ser HTTPS:// e não HTTP://.

Quando devo usar o Bitdefender VPN?

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

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

O Bitdefender VPN vai ter um impacto negativo na bateria do meu dispositivo?

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

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

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

Posso modificar a conta Bitdefender associada ao meu dispositivo?

Sim, pode alterar facilmente a conta Bitdefender associada ao seu dispositivo seguindo estes passos:

1. Toque **Mais** na barra de navegação inferior.

2. Toque no seu endereço de e-mail.
3. Toque em **Terminar sessão na sua conta**. Se tiver sido definido um código PIN, será solicitado a inseri-lo.
4. Confirme a sua escolha.
5. Escreva o endereço de e-mail e a palavra-passe da sua conta nos campos correspondentes e, em seguida, toque em **ENTRAR**.

Como é que o Bitdefender Mobile Security irá influenciar o desempenho do meu dispositivo e na autonomia da minha bateria?

O impacto é muito baixo. A aplicação só é executada quando é fundamental — inclusive durante a instalação e quando navega pela interface da aplicação — ou quando pretende realizar uma verificação de segurança. O Bitdefender Mobile Security não funciona em plano de fundo quando liga para amigos, envia mensagens ou joga.

O que é o Administrador do Dispositivo?

O Administrador do Dispositivo é uma função do Android que dá ao Bitdefender Mobile Security as permissões necessárias para realizar determinadas tarefas remotamente. Sem esses privilégios, o bloqueio remoto não funcionaria e a limpeza do dispositivo não conseguiria remover completamente os seus dados. Se pretende remover a aplicação, certifique-se de que retira esses privilégios antes de tentar desinstalar em **Definições > Segurança > Selecione os administradores do dispositivo**.

Como solucionar o erro "Nenhum Token Google" que aparece ao iniciar sessão no Bitdefender Mobile Security.

Este erro ocorre quando o dispositivo não está associado a uma conta Google, ou está associado, mas um problema temporário está a evitar que se ligue ao Google. Tente uma das seguintes soluções:

- Vá para as Definições > do Android; Aplicações > Gerir Aplicações > Bitdefender Mobile Security e toque em **Limpar dados**. Tente iniciar sessão novamente.
- Certifique-se de que o seu dispositivo está associado a uma conta Google.

  Para verificar isto, vá a Definições > Conta & sincronize e veja se a conta Google está listada sob **Gestão de Contas**. dicione a sua conta se não estiver listada, reinicie o seu dispositivo e então tente iniciar sessão no Bitdefender Mobile Security.

- Reinicie o seu dispositivo e, em seguida, tente iniciar sessão novamente.

Em que idiomas é que o Bitdefender Mobile Security está disponível?

Atualmente o Bitdefender Mobile Security está disponível nos seguintes idiomas:

- Brasileiro
- Checo
- Holandês
- Inglês
- Francês
- German
- Grego
- Húngaro
- Italiano
- Japonês
- Coreano
- Polaco
- Português
- Romanian
- Russo
- Spanish
- Sueco
- Tailandês
- Turco
- Vietnamita

Serão adicionados outros idiomas em versões futuras. Para alterar o idioma da interface do Bitdefender Mobile Security, aceda às definições do seu dispositivo **Idioma & teclado** e defina o idioma que pretende utilizar no dispositivo.

CONTACTE-NOS

33. PEDIR AJUDA

O 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 online para encontrar uma solução ou resposta. Ou, se preferir, poderá contactar a equipa de Suporte ao Cliente do Bitdefender. Os nossos técnicos de apoio responderão atempadamente às suas questões e dar-lhe-ão a ajuda que precisar.

A secção "*Resolver incidências comuns*" (p. 166) fornece as informações necessárias relativamente às incidências mais frequentes que poderá encontrar ao utilizar este produto.

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

- "Contate-nos diretamente desde o Bitdefender Total Security" (p. 302)
- "Contacte-nos através do nosso Centro de Suporte Online" (p. 303)

Contate-nos diretamente desde o Bitdefender Total Security

Se possuir uma ligação ativa à Internet, pode contactar o apoio do Bitdefender diretamente a partir da interface do produto.

Siga os seguintes passos:

1. Clique em **Apoio** no menu de navegação da interface do Bitdefender.
2. Tem as seguintes opções:
   - **GUIA DO UTILIZADOR**

     Aceda à nossa base de dados e procure a informação necessária.
   - **CENTRO DE SUPORTE**

     Aceda aos nossos artigos e vídeos de tutoriais online.
   - **CONTACTO DE SUPORTE**

     Clique **Contatar Suporte** para executar a Ferramenta de Suporte do Bitdefender e contatar o Departamento de Apoio ao Cliente.

     a. Complete o formulário de envio com os dados necessários:

        i. Selecione o tipo de problema que encontrou.

ii. Digite uma descrição do problema encontrado.

iii. Clique em **TENTAR REPRODUZIR ESTE PROBLEMA** caso esteja a encontrar um problema no produto. Reproduza o problema e, em seguida, clique em **FINALIZAR** no quadro REPRODUZINDO O PROBLEMA.

iv. Clique em **CONFIRMAR PEDIDO DE SUPORTE**.

b. Continue a preencher o formulário com os dados necessários:

i. Digite o seu nome completo.

ii. Digite o seu endereço de e-mail.

iii. Marque a caixa de verificação do acordo.

iv. Clique em **CRIAR PACOTE DE DEBUG**.

Aguarde alguns minutos enquanto o Bitdefender reúne informações relacionadas com o produto. Esta informação irá ajudar os nossos engenheiros a encontrar uma solução para o seu problema.

c. Clique em **FECHAR** para sair do assistente. Será contactado assim que possível por um dos nossos representantes.

Contacte-nos através do nosso Centro de Suporte Online

Se não conseguir aceder às informações necessárias com o produto Bitdefender, consulte o nosso Centro de Suporte online:

1. Vá para https://www.bitdefender.com/support/consumer.html.

   O Centro de Suporte da Bitdefender possui inúmeros artigos que contêm soluções para incidências relacionadas com o Bitdefender.

2. Utilize a barra de pesquisa na parte superior da janela para encontrar artigos que possam fornecer uma solução definitiva para o seu problema. Para pesquisar, basta digitar o termo na barra de pesquisa e clicar em **Pesquisar**.

3. Leia os artigos ou os documentos e experimente as soluções propostas.

4. Se a solução não resolver o seu problema, aceda a

https://www.bitdefender.com/support/contact-us.htmle contate os nossos representantes do suporte.

34. RECURSOS ONLINE

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

- Centro de Suporte Bitdefender:

  https://www.bitdefender.com/support/consumer.html

- Fórum de Suporte Bitdefender:

  https://forum.bitdefender.com

- o portal de segurança informática HOTforSecurity:

  https://www.hotforsecurity.com

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

34.1. Centro de Suporte Bitdefender

O Centro de Suporte do Bitdefender é um repositóio de informação online sobre os produtos Bitdefender. Armazena, num formato facilmente acessível, apresenta relatórios sobre os resultados do suporte técnico em curso e atividades de correção de falhas do suporte e equipas de desenvolvimento do Bitdefender, para além de artigos mais gerais sobre prevenção de ameaças, a gestão de soluções do Bitdefender com explicações detalhadas e muitos outros artigos.

O Centro de Suporte da Bitdefender está aberto ao público e é pesquisável. A informção extensiva que contém é mais um meio de proporcionar aos clientes do Bitdefender informações técnicas e conhecimento de que necessitam. Todos os pedidos válidos de informação 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 informacionais como suplemento dos ficheiros de ajuda.

O Centro de Suporte da Bitdefender encontra-se disponível a qualquer altura

https://www.bitdefender.com/support/consumer.html.

34.2. Fórum de Suporte Bitdefender

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

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

Os técnicos de apoio da Bitdefender supervisionam o fórum, à espera de novas mensagens para fornecer ajuda. Também pode receber uma resposta ou solução de um utilizador 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 **Proteção Casa & Casa/Escritório** para aceder à secção dedicada aos produtos de consumidor.

34.3. Portal HOTforSecurity

HOTforSecurity é uma fonte rica de informações sobre segurança de computadores. Aqui, pode ficar a conhecer as várias ameaças a que o seu computador fica exposto quando ligado à Internet (malware, phishing, spam, cibercriminosos).

Os novos artigos são publicados regularmente para o manter atualizado sobre as últimas ameaças descobertas, as atuais tendências de segurança e outras informações sobre a indústria de segurança informática.

A página web do HOTforSecurity é https://www.hotforsecurity.com.

35. CONTACT INFORMATION

Comunicação eficiente é a chave de um negócio bem-sucedido. Desde 2001, a BITDEFENDER estabeleceu uma reputação sólida ao visar constantemente uma melhor comunicação, excedendo, assim, as expetativas dos nossos clientes e parceiros. Por favor não hesite em contactar-nos acerca de qualquer questão ou assunto que nos queira colocar.

35.1. Endereços Web

Departamento Comercial: comercial@bitdefender.pt
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 os media: pr@bitdefender.com
Carreiras: jobs@bitdefender.com
Submissões de ameaças: virus_submission@bitdefender.com
Submeter Spam: spam_submission@bitdefender.com
Relatórios de Abusos: abuse@bitdefender.com
Website:https://www.bitdefender.com

35.2. Distribuidores locais

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

Para encontrar um distribuidor Bitdefender no seu país:

1. Vá para https://www.bitdefender.com/partners/partner-locator.html.
2. Escolha o seu país e cidade utilizando as opções correspondentes.
3. Se não encontrar um distribuidor Bitdefender no seu país, não hesite em contactar-nos por correio eletrónico através do endereço sales@bitdefender.com. Escreva a sua mensagem em inglês para podermos responder imediatamente.

35.3. Escritórios Bitdefender

Os escritórios locais Bitdefender estão preparados para responder a quaisquer dúvidas relacionadas com as suas áreas de operação, quer sejam

comerciais ou assuntos gerais. Os seus respectivos endereços e contactos estão listados abaixo.

E.U.A.

Bitdefender, LLC
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
Telefone (office&sales): 1-954-776-6262
Vendas: sales@bitdefender.com
Suporte Técnico: https://www.bitdefender.com/support/consumer.html
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
Email: info@bitdefender.co.uk
Phone: (+44) 2036 080 456
Vendas: sales@bitdefender.co.uk
Suporte Técnico: https://www.bitdefender.co.uk/support/
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
Web: https://www.bitdefender.de

Denmark

Bitdefender APS
Agern Alle 24, 2970 Hørsholm, Denmark
Escritório: +45 7020 2282

Suporte Técnico: http://bitdefender-antivirus.dk/
Web: http://bitdefender-antivirus.dk/

Espanha

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Phone: +34 902 19 07 65
Vendas: comercial@bitdefender.es
Suporte Técnico: https://www.bitdefender.es/support/consumer.html
Website: https://www.bitdefender.es

Roménia

BITDEFENDER SRL
Orhideea Towers, 15A Orhideelor Street, Sector 6
Bucharest
Fax: +40 21 2641799
Telefone Comercial: +40 21 2063470
Email vendas: sales@bitdefender.ro
Suporte Técnico: https://www.bitdefender.ro/support/consumer.html
Website: https://www.bitdefender.ro

Emirados Árabes Unidos

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Telefone Comercial: 00971-4-4588935 / 00971-4-4589186
Email vendas: mena-sales@bitdefender.com
Suporte Técnico: https://www.bitdefender.com/support/consumer.html
Website: https://www.bitdefender.com

Glossário

ActiveX

O ActiveX é um modelo para fazer programas de forma a que outros programas e o sistema operativo os possam chamar. A tecnologia do ActiveX é usada com o Microsoft Internet Explorer para criar páginas da Web interactivas, que parecem e comportam-se como programas de computador, em vez de páginas estáticas. Com o ActiveX, os utilizadores podem efectuar perguntas ou responder a questões, usando botões para carregar, e interagir de outras formas com a página da web. Os controlos do ActiveX são frequentemente escritos utilizando o Visual Basic.

O Active X é notável para um leque completo de controlos de segurança; os especialistas de segurança dos computadores desencorajam o seu uso na Internet.

Adware

O adware é com frequência combinado com uma aplicação hospedeira que é fornecida sem custo desde que o utilizador concorde em aceitar o adware. Por causa das aplicações adware serem normalmente instaladas após o utilizador concordar com uma licença de uso que define o propósito da aplicação, nenhuma ilegalidade é na verdade cometida.

No entanto, anúncios tipo pop-up podem tornar-se bastante incomodativos, e em alguns casos podem mesmo degradar a performance do sistema. Também, a informação que algumas dessas aplicações recolhem podem causar algumas preocupações de privacidade aos utilizadores que não estão completamente conscientes dos termos da licença de uso.

Ameaça

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

perigoso é aquele que é capaz de se transmitir através de uma rede ou contornando sistemas de segurança.

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 detetada durante um longo período de tempo, sendo capaz de monitorizar e recolher informações importantes sem danificar as máquinas atacadas. O método utilizado para injetar a ameaça na rede é através de um ficheiro PDF ou documento do Office que pareça inofensivo, de forma a que todo os utilizadores possam abrir os ficheiros.

Arquivo

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

Um ficheiro que contém um ou mais ficheiros num formato comprimido.

Ataque de dicionário

Foi utilizado um ataque de adivinhação de palavras-passe para invadir o sistema de um computador introduzindo uma combinação de palavras comuns para gerar possíveis palavras-passe. É utilizado o mesmo método para adivinhar palavras-passe de mensagens ou documentos encriptados. Os ataques de dicionário funcionam devido à tendência de muitas pessoas escolherem palavras-passe curtas ou de uma palavra que acabam por ser fáceis de serem adivinhadas.

Ataque de força bruta

Foi utilizado um ataque de adivinhação de palavras-passe para invadir o sistema de um computador introduzindo possíveis combinações de palavras-passe, começando pelas mais fáceis de adivinhar.

Atualização

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

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

Atualização das informações sobre a ameaça

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

Boot sector

Um sector no início de cada disco que identifica a arquitectura do disco (tamanho do sector, tamanho do grupo, e por aí fora). Para discos de inicialização, o sector de saída também contém um programa que carrega o sistema operativo.

Botnet

O termo "botnet" é composto pelas palavras "robot" (robô) e "network" (rede). Os botnets são dispositivos ligados à Internet infetados com ameaças e podem ser utilizados para enviar e-mails de spam, roubar dados, controlar remotamente dispositivos vulneráveis e outros tipos de ameaças. O objetivo é infetado o máximo de dispositivos ligados possível, tais como PC, servidores, dispositivos móveis ou IoT que pertencem a grandes empresas ou indústrias.

Caixa do sistema

Introduzido com o Windows 95, o tabuleiro do sistema está localizado na barra de tarefas do Windows (normalmente em baixo, junto ao relógio) e contém ícones em miniatura para um acesso fácil às funções do sistema, tais como fax, impressora, modem, volume, etc. Faça duplo-clique ou clique com o botão direito sobre o ícone para ver e aceder aos detalhes e controlos.

Caminho

As direcções exactas para um ficheiro num computador. Estas direções são normalmente descritas por meios de preenchimento hierárquico do topo para baixo.

A rota entre dois dados pontos, tal como os canais de comunicação entre dois.

Cliente de mail

Um cliente de e-mail é uma aplicação que lhe permite enviar e receber e-mail.

Código de activação

É um código exclusivo que pode ser adquirido a retalho e utilizado para ativar um produto ou serviço específico. Um código de ativação permite a ativação de uma subscrição válida por um determinado período de tempo e determinados dispositivos, e também pode ser utilizado para prolongar uma subscrição com a condição de ser gerada para o mesmo produto ou serviço.

Componente (drive) do disco

É uma máquina que lê os dados do disco e escreve dados num disco.

Uma componente de disco rígido lê e escreve discos rígidos.

Uma componente de disquetes acede às disquetes.

As componentes do disco tanto podem ser internas (dentro do computador) ou externas (vêm numa caixa em separado que se liga ao computador).

Cookie

Dentro da indústria da Internet, as cookies são descritas como pequenos ficheiros, que contêm informação acerca de computadores individuais, que podem ser analizados e usados pelos publicitários para seguir o rasto online do seus interesses e gostos. Neste domínio, a tecnologia das cookies ainda está a ser desenvolvida e a sua intenção é procurar atingi-lo com publicidade naquilo que disse serem os seus interesses. É uma espada de dois gumes para muitas pessoas, porque, por um lado é eficiente e pertinente já que apenas vê anúncios do seu interesse. Por outro lado, envolve realmente "seguir o rasto" e "perseguir" onde vai e no que clica. Compreensivelmente, existe um debate acerca da privacidade e muitas pessoas sentem-se ofendidas ao terem a noção que estão a ser vistas como um "número SKU " (sabe, o código de barras por detrás das embalagens que é verificado na mercearia). Apesar deste ponto de vista parecer ser extremo, em alguns casos é exacto.

Cyberbullying

Quando colegas ou estranhos cometem atos abusivos contra crianças de propósito para as ferir fisicamente. Para causar danos emocionais,

os agressores enviam mensagens ou fotos mal-intencionadas, que fazem com que as suas vítimas se isolem de outros e se sintam frustradas.

Download

Para copiar dados (normalmente um ficheiro interno) de uma fonte principal para um aparelho periférico. O termo é frequentemente utilizado para descrever o processo de copiar um ficheiro de um serviço online para o seu próprio computador. O download também se pode referir à cópia de um ficheiro de um servidor de ficheiros de rede, para um computador na rede.

Email

Correio electrónico. É um serviço que envia mensagens de computadores via redes locais ou globais.

Escrita

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

Eventos

Uma ação ou ocorrência detetada por um programa. Os eventos podem ser ações do utilizador, tais como clicar no botão do rato ou carregar numa tecla, ou ocorrências do sistema, tal como ficar sem memória.

Explorações

Uma forma de se aproveitarem de diferentes bugs ou vulnerabilidades presentes num computador (software ou hardware). Assim, os hackers podem obter controlo de computadores ou redes.

Extensão do nome do ficheiro

A porção de um nome de ficheiro, que segue o ponto final, a qual indica o tipo de dados armazenados no ficheiro.

Muitos sistemas operativos usam extensões do nome do ficheiro, por ex. Unix, VMS, e MS-DOS. Elas são normalmente de uma a três letras (alguns SOs antigos não suportam mais do que três). Os exemplos incluem ".c" para C de código da fonte, ".ps" para PostScript, ".txt" para texto arbitrário.

Falso positivo

Ocorre quando o verificador identifica um ficheiro como infectado, quando na verdade ele não está.

Ficheiro de reporte

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

Heurístico

Um método baseado em regras de identificação de novas ameaças. Este método de verificação não utiliza uma base de dados de informações de ameaças específico. A vantagem da análise heurística é que não se deixa enganar por uma nova variante de uma ameaça existente. Contudo, pode reportar ocasionalmente códigos suspeitos em programas normais, gerando o chamado "falso positivo".

IP

Internet Protocol - Um rótulo de protocolo no protocolo TCP/IP séquito que é responsável dos endereços de IP, rotas, e a fragmentação e reabertura dos pacotes de IP.

Itens de Arranque

Qualquer ficheiro colocado nesta pasta, irá abrir quando o computador iniciar. Por exemplo, um ecrã de arranque, um ficheiro de som a ser reproduzido quando o computador arranca, um calendário de lembretes ou aplicações podem ser itens de arranque. Normalmente, é colocado um pseudónimo deste ficheiro nesta pasta, em vez do ficheiro em si.

Java applet

Um programa em Java é desenhado para funcionar apenas numa página web. Para usar uma applet numa página web, deverá especificar o nome da applet e o tamanho (comprimento e largura - em pixels) que a applet pode utilizar. Quando a página da web é acedida, o motor de busca descarrega a applet de um servidor e executa-a na máquina do utilizador (o cliente). As applets diferem das aplicações, pois são administradas por um protocolo de segurança restrito.

Por exemplo, apesar de as applets se executarem no cliente, elas não podem escrever nem ler dados na máquina do cliente. Adicionalmente,

as applets são restritas para que possam apenas ler e escrever dados provenientes do mesmo domínio do qual elas são servidas.

Keylogger

Um keylogger é uma aplicação que regista tudo o que digita.

Os keyloggers não são por natureza maliciosos. Podem ser usados com objectivos legítimos, tais como monitorizar a actividade de funcionários ou das crianças. No entanto, são cada vez mais usados por cibercriminosos com objectivos maliciosos (por exemplo, para recolher dados privados, tais como credenciais de acesso e números da segurança social).

Linha de comando

Numa interface de linha do comando, o utilizador introduz comandos no espaço providenciado diretamente no ecrã, usando a linguagem de comando.

Macro vírus

Um tipo de ameaça de computador que está codificado como uma macro retido num documento. Muitas aplicações, tais como Microsoft Word e Excel, contêm poderosas linguagens macro.

Estas aplicações permitem-lhe reter uma macro num documento, e ter a macro pronta a ser executada sempre que o documento for aberto.

Memória

Áreas internas de armazenamento no computador. O termo memória identifica armazenamento de dados que vêm na forma de chips, e a palavra armazenar é usada para a memória que existe em cassetes ou discos. Todo o computador vem com uma certa quantidade de memória física, normalmente referida como memória principal ou RAM.

Minhoca

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

Não-heurístico

Este método de verificação não depende de uma base de dados de informações de ameaças específica. A vantagem da análise não

heurística é que não pode ser enganada por algo que pode parecer uma ameaça e não gera falsos alarmes.

Navegador

É um software de aplicação utilizado para localizar e mostrar páginas da Web. Os navegadores mais populares são o Microsoft Internet Explorer, Mozilla Firefox e Google Chrome. Estes são motores de busca gráficos, o que significa que eles tanto podem mostrar gráficos como texto. Em adição, a maioria dos motores de busca modernos podem apresentar informação multimédia, incluíndo som e vídeo, apesar de requererem plug-ins para alguns formatos.

Phishing

O acto de enviar um e-mail onde são proferidas declarações falsas relativamente à origem e natureza do cargo desempenhado pelo remetente, numa tentativa de burlar o remetente e assim obter ilicitamente informação privada que será utilizada em esquemas de roubo de identidade. O email encaminha o utilizador para um site onde lhé solicitada a actualização de informação pessoal - palavras passe, cartão de crédito, segurança social, contas bancárias - que a entidade legítima já possui. O site web, no entanto, é falso e está feito apenas para roubar a informação ao utilizador.

Photon

Photon é uma tecnologia inovadora não intrusiva da Bitdefender, concebida para minimizar o impacto da solução de segurança. Ao monitorizar a atividade do seu PC em segundo plano, ele cria padrões de utilização que ajudam a otimizar os processos de arranque e de análise.

Porta

Uma interface num computador, à qual se liga um dispositivo. Os computadores pessoais têm vários tipos de portas. Internamente, existem várias portas para ligar as drives de disco, ecrãs, e teclados. Externamente, os computadores pessoais têm portas para ligar modems, impressoars, ratos, e outros dispositivos periféricos.

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

Porta das traseiras

Um buraco na segurança de um sistema deliberadamente criado pelos desenhadores ou responsáveis da manutenção. A motivação para tais buracos não é sempre sinistra; alguns sistemas operativos, por exemplo, que trazem contas privilegiadas, criadas para serem usadas pelos técnicos de serviço ou pelo vendedor dos programas de manutenção.

Pote de mel

Um sistema de computador "decoy" estabelecido para atrair hackers, destinado a estudar a forma como agem e identificar os métodos que utilizam para recolher informações do sistema. As empresas e corporações estão mais interessadas em implementar e utilizar "potes de mel" para melhorar o seu estado geral de segurança.

Predadores online

Pessoas que procuram atrair menores de idade ou adolescentes para conversas com o objetivo de os envolver em atividades sexuais ilegais. As redes sociais são o local ideal para caçar e seduzir facilmente crianças vulneráveis para realizar atividades sexuais, tanto online como cara a cara.

Programas compactados

Um ficheiro num formato compactado. Muitos sistemas operativos e aplicações contêm comandos que lhe permitem compactar um ficheiro, para que ocupe menos memória. Por exemplo, suponha que tem um ficheiro de texto contendo dez espaços de caracteres consecutivos. Normalmente, isto iria requerer dez bytes de armazenamento.

Contudo, um programa que compacta ficheiros iria substituir o espaço dos caracteres por uma série-de-espaços de caracteres especial, seguida pelo número de espaços a serem substituidos. Neste caso, os dez espaços iriam requerer apenas dois bytes. Esta é apenas uma técnica de compactar - existem muitas mais.

Ransomware

Ransomware é um programa malicioso que tenta lucrar com os utilizadores através do bloqueio dos seus sistemas vulneráveis. CryptoLocker, CryptoWall e TeslaWall são apenas algumas variantes que perseguem os sistemas pessoais dos utilizadores.

A infeção pode ser espalhada através do acesso a um e-mail de spam, transferência de anexos de e-mail ou da instalação de aplicações, sem que o utilizador saiba o que está a acontecer no seu sistema. Os utilizadores diários e as empresas são os alvos dos hackers ransomware.

Rede Privada Virtual (VPN)

É uma tecnologia que ativa uma ligação direta temporária e encriptada para uma certa rede sobre uma rede menos segura. Desta forma, enviar e receber dados é seguro e encriptado, difícil de se tornar alvo de espiões. Uma prova de segurança é a autenticação, que pode ser feita somente com a utilização de um nome de utilizador e palavra-passe.

Rootkit

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

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

Os rootkits não são maliciosos por natureza. Por exemplo, os sistemas e mesmo algumas aplicações ocultam ficheiros críticos usando rootkits. No entanto, são principalmente utilizados para ocultar ameaças ou esconder a presença de um intruso no sistema. Quando combinados com ameaças, os rootkits são uma grande ameaça à integridade e à segurança de um sistema. Eles podem monitorizar tráfego, criar backdoors no sistema, alterar ficheiros e relatórios e evitarem ser detetados.

Spam

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

Spyware

Qualquer software que encobertamente reune informação do utilizador através da ligação à Internet do utilizador sem o seu conhecimento, normalmente para propósitos de publicidade. As aplicações de spyware

são tipicamente adicionadas como um elemento oculto de programas freeware ou shareware que podem ser download a partir da Internet; no entanto salientamos que a maioria das aplicações freeware ou shareware não possuem spyware. Uma vez instalado, o spyware monitoriza a actividade do utilizador na Internet e transmite essa informação em background para alguém. O spyware pode também ser capaz de obter endereços de e-mail e até mesmo palavras-passe e números de cartão de crédito.

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

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

Subscrição

Acordo de compra que dá ao utilizador o direito de utilizar um produto ou serviço específico num número específico de dispositivos e durante um período de tempo determinado. Uma subscrição expirada pode ser automaticamente renovada utilizando as informações fornecidas pelo utilizador na primeira compra.

TCP/IP

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

Tróiano

Um programa destrutivo que se mascara de aplicação benigna. Ao contrário de programas de software maliciosos e worms, os Trojans não

se replicam, mas podem ser igualmente destrutivos. Um dos tipos mais insidiosos de ameaças de cavalo de Troia é um programa que afirma remover as ameaças do seu computador, mas, em vez disso, introduz ameaças no seu computador.

O termo provém de uma história da Ilíada de Homero, na qual os Gregos deram um cavalo gigante de Madeira aos seus inimigos, os Troianos, como uma oferta majestosa. Mas após os Troianos levarem o cavalo para dentro das muralhas da sua cidade, os soldados Gregos saíram para fora do cavalo e abriram os portões da cidade, permitindo que os seus compatriotas entrassem e dominassem Tróia.

Vírus de saída

Uma ameaça que infeta o setor de arranque de um disco fixo ou de uma unidade de disquetes. A tentativa de arrancar por uma disquete infetada por um vírus de arranque irá causar a ativação da ameaça em memória. Sempre que iniciar o seu sistema a partir daquele ponto, terá a ameaça ativa em memória.

Vírus polimórfico

Uma ameaça que muda a sua forma com cada ficheiro que infeta. Como não têm um padrão binário consistente, essas ameaças são difíceis de identificar.