Bitdefender®

ANTIVIRUS PLUS 2016

MANUAL DO UTILIZADOR

Bitdefender Antivirus Plus 2016
Manual do Utilizador

Editado 10/07/2015

Aviso Legal

Bitdefender

Índice

INSTALAÇÃO

1. A PREPARAR A INSTALAÇÃO

Antes de instalar o Bitdefender Antivirus Plus 2016, complete estes procedimentos para assegurar uma boa instalação:

- Assegure-se que o computador onde vai instalar o Bitdefender contém os requisitos minimos do sistema. Se o seu computador não contém os requisitos mínimos do sistema, o Bitdefender não será instalado ou, se instalado, não trabalhará corretamente e provocará lentidão e instabilidade no sistema. Para ver a lista completa dos requisitos mínimos do sistema, por favor consulte o "*Requisitos do sistema*" (p. 3).
- Ligue-se ao computador utilizando uma conta de Administrador.
- Remova quaisquer outros softwares semelhantes do seu computador. 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.
- Recomenda-se que o seu computador esteja ligado à Internet durante a instalação, mesmo quando realiza 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.

2. REQUISITOS DO SISTEMA

Só pode instalar o Bitdefender Antivirus Plus 2016 nos computadores que tenham os seguintes sistemas operativos:

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

Antes da instalação, certifique-se de que o seu computador cumpre os requisitos mínimos de hardware e software.

Nota

Para descobrir qual o sistema operativo executado no seu computador e as informações de hardware, siga estes passos:

- No **Windows 7**, clique com o botão direito em **O meu Computador** na área de trabalho e depois selecione **Propriedades** no menu.
- No **Windows 8 e 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. Selecione Propriedades no menu inferior. Procure por informações sobre o tipo do sistema na área do Sistema.
- No **Windows 10**, introduza "Sistema" na caixa de pesquisa da barra de tarefas e clique no ícone correspondente. Procure por informações sobre o tipo do sistema na área do Sistema.

2.1. Requisitos mínimos do sistema

- 1 GB de espaço disponível no disco rígido (pelo menos 800 MB na unidade do sistema)
- Processador de 1.6 GHz
- 1 GB de memória (RAM)

2.2. Requisitos de sistema recomendados

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

2.3. Requisitos de Software

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

- Internet Explorer 10 ou superior
- Mozilla Firefox 14 ou superior
- Google Chrome 20 ou superior
- Skype 6.3 ou superior
- Yahoo Messenger 9 ou superior

3. INSTALAÇÃO DO SEU PRODUTO BITDEFENDER

Pode instalar o Bitdefender utilizando o disco de instalação, ou pelo instalador Web transferindo-o para o seu computador da conta Bitdefender Central.

Se a sua compra abrange mais do que um computador (por exemplo, adquiriu o Bitdefender Antivirus Plus 2016 para 3 PCs), repita o processo de instalação e ative o seu produto com a mesma conta em cada um dos computadores. A conta a ser utilizada deve ser igual à que contém a sua subscrição ativa do Bitdefender.

3.1. Instale a partir Bitdefender Central

Através da conta Bitdefender Central pode transferir o kit de instalação correspondente à subscrição adquirida. Uma vez que o processo de instalação estiver concluído, o Bitdefender Antivirus Plus 2016 é ativado.

Para transferir o Bitdefender Antivirus Plus 2016 da sua conta Bitdefender Central, siga estes passos:

1. Aceder à sua conta Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.
3. Na janela **Os Meus Dispositivos**, clique em **INSTALAR Bitdefender**.
4. Escolha **Windows**, em seguida, escolha uma das duas opções disponíveis:
   - Eu gostaria de instalar o Bitdefender **Neste dispositivo**.

     Selecione o Bitdefender Antivirus Plus 2016 da lista **Produto a ser instalado** e, em seguida, clique em **Download** para continuar.
   - Eu gostaria de instalar o Bitdefender **Noutro dispositivo**.

     Selecione o Bitdefender Antivirus Plus 2016 da lista **Produto a ser instalado**. Escreva um endereço de e-mail no campo correspondente e clique em **ENVIAR**.
5. Aguarde pela conclusão da transferência, em seguida, execute o instalador:

A validar a instalação

O Bitdefender irá primeiro verificar o seu sistema para validar a instalação.

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

Se for detetado um programa antivírus incompatível ou uma versão anterior do Bitdefender, será avisado para o remover do seu sistema. Por favor siga as instruções para remover o software do seu sistema, evitando assim que ocorram problemas mais tarde. Pode necessitar de reiniciar o seu computador para concluir a remoção dos programas antivírus detetados.

O pacote de instalação do Bitdefender Antivirus Plus 2016 é continuamente atualizado. Clique em **Sim** quando solicitado de forma a permitir que o Bitdefender faça download dos ficheiros, assegurando assim que está a instalar a versão mais recente do software.

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

Uma vez que a instalação seja validada, o assistente de instalação aparecerá. Siga os passos para instalar o Bitdefender Antivirus Plus 2016.

Passo 1 – instalação do Bitdefender

O ecrã de instalação do Bitdefender permite-lhe escolher que tipo de instalação que pretende fazer.

Para uma experiência de instalação livre de problemas, basta clicar no botão **Instalar**. O Bitdefender será instalado na localização por defeito com as definições por defeito e você saltará directamente para o Passo 3 do assistente.

Caso queira modificar as definições de instalação, clique em **Personalizar**

Podem ser realizadas duas tarefas adicionais neste passo:

- Por favor leia o Acordo de Licença de Utilizador antes de prosseguir com a instalação. O Acordo de Licença contém os termos e condições ao abrigo dos quais pode usar o Bitdefender Antivirus Plus 2016.

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

- Ativar enviar **Relatórios anónimos de utilização**. Ao ativar 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.

Passo 2 - Personalizar definições da instalação

> **Nota**
> Este passo apenas aparece se escolheu personalizar a instalação durante o passo anterior.

Estão disponíveis as seguintes opções:

Instalar caminho

Por defeito, o Bitdefender Antivirus Plus 2016 será instalado em C:\Programas\Bitdefender\Bitdefender 2016\. Se deseja alterar este caminho de instalação, clique em **Alterar** e selecione a pasta na qual pretende que o Bitdefender seja instalado.

Configurar definições de proxy

O Bitdefender Antivirus Plus 2016 requer o acesso à Internet para registo do produto, descarregar atualizações de segurança e de produtos, componentes de deteção na nuvem, etc. Se usar uma ligação por proxy em vez de uma ligação direta à Internet, deve selecionar esta opção e configurar as definições.

As definições podem ser importadas do navegador por defeito ou pode introduzi-las manualmente.

Clique em **Instalar** para confirmar as suas preferências e iniciar a instalação. Caso mude de ideias, clique no botão **Utilizar predefinições** correspondente.

Passo 3 - Instalação em curso

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

As áreas críticas do seu sistema são analisadas, as versões mais recentes dos ficheiros da aplicação são descarregadas e instaladas e os serviços do Bitdefender iniciam-se. Este passo pode demorar alguns minutos.

Passo 4 - Instalação terminada

O seu produto Bitdefender foi instalado com sucesso.

É apresentado um resumo da instalação. Se tiver sido detetado malware activo e removido durante a instalação, pode ser necessário reiniciar o sistema. Clique em **OK** para continuar.

Passo 5 - Introdução

Na janela Introdução, pode ver a validade da sua subscrição.

Podem ser realizadas duas tarefas adicionais neste passo:

- Compre uma nova subscrição – esta ligação redireciona-o para a página do Bitdefender de onde pode comprar uma nova subscrição.
- Tenho um código de ativação – esta ligação redireciona-o para a sua conta Bitdefender Central. Clique em **CÓDIGO DE ATIVAÇÃO** na janela A Minha Subscrição que aparece. Escreva o seu código de ativação, em seguida, clique em **SUBMETER**.

Clique em **Finalizar** para aceder à interface do Bitdefender Antivirus Plus 2016.

3.2. Instalar a partir do disco de instalação

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

Deve aparecer um ecrã de instalação em alguns momentos. Siga as instruções para iniciar a instalação.

Nota

O ecrã de instalação fornece uma opção para copiar o pacote de instalação a partir do disco de instalação para um dispositivo de armazenamento USB. Isto é útil se precisar de instalar Bitdefender num computador que não possui uma drive de disco (por exemplo, num netbook). Insira a pen USB na drive respetiva e depois clique em **Copiar para a USB**. Depois, vá até ao computador sem a drive de disco, insira a pen USB e faça duplo clique no ficheiro runsetup.exe que se encontra na pasta onde guardou o pacote de instalação.

Se o ecrã de instalação não aparecer, utilize o Explorador do Windows para navegar até ao diretório de raiz do disco e clique duas vezes no ficheiro autorun.exe.

A validar a instalação

O Bitdefender irá primeiro verificar o seu sistema para validar a instalação.

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

Se for detetado um programa antivírus incompatível ou uma versão anterior do Bitdefender, será avisado para o remover do seu sistema. Por favor siga as instruções para remover o software do seu sistema, evitando assim que ocorram problemas mais tarde. Pode necessitar de reiniciar o seu computador para concluir a remoção dos programas antivírus detetados.

O pacote de instalação do Bitdefender Antivirus Plus 2016 é continuamente atualizado. Clique em **Sim** quando solicitado de forma a permitir que o Bitdefender faça download dos ficheiros, assegurando assim que está a instalar a versão mais recente do software.

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

Uma vez que a instalação seja validada, o assistente de instalação aparecerá. Siga os passos para instalar o Bitdefender Antivirus Plus 2016.

Passo 1 – Instalação do Bitdefender

O ecrã de instalação do Bitdefender permite-lhe escolher que tipo de instalação que pretende fazer.

Para uma experiência de instalação livre de problemas, basta clicar no botão **Instalar**. O Bitdefender será instalado na localização por defeito com as definições por defeito e você saltará directamente para o Passo 3 do assistente.

Caso queira modificar as definições de instalação, clique em **Personalizar**

Podem ser realizadas duas tarefas adicionais neste passo:

- Leia o Contrato de Licença do Utilizador Final antes de prosseguir com a instalação. O Acordo de Licença contém os termos e condições ao abrigo dos quais pode usar o Bitdefender Antivirus Plus 2016.

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

- Selecione **Enviar relatórios anónimos de utilização**. Ao ativar 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.

Passo 2 - Personalizar definições da instalação

> **Nota**
> Este passo apenas aparece se escolheu personalizar a instalação durante o passo anterior.

Estão disponíveis as seguintes opções:

Instalar caminho

Por defeito, o Bitdefender Antivirus Plus 2016 será instalado em C:\Programas\Bitdefender\Bitdefender 2016\. Se deseja alterar este caminho de instalação, clique em **Alterar** e selecione a pasta na qual pretende que o Bitdefender seja instalado.

Configurar definições de proxy

O Bitdefender Antivirus Plus 2016 requer acesso à Internet para a ativação do produto, transferência de atualizações de segurança e de produtos, componentes de deteção na nuvem, etc. Se usar uma ligação por proxy em vez de uma ligação direta à Internet, deve selecionar esta opção e configurar as definições.

As definições podem ser importadas do navegador por defeito ou pode introduzi-las manualmente.

Clique em **Instalar** para confirmar as suas preferências e iniciar a instalação. Caso mude de ideias, clique no botão **Utilizar predefinições** correspondente.

Passo 3 - Instalação em curso

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

As áreas críticas do seu sistema são analisadas, as versões mais recentes dos ficheiros da aplicação são descarregadas e instaladas e os serviços do Bitdefender iniciam-se. Este passo pode demorar alguns minutos.

Passo 4 - Instalação terminada

É apresentado um resumo da instalação. Se tiver sido detetado malware activo e removido durante a instalação, pode ser necessário reiniciar o sistema. Clique em **OK** para continuar.

Passo 5 - Bitdefender Central

Após concluir a configuração inicial, a janela Bitdefender Central aparece. Uma conta Bitdefender Central é necessária para ativar o produto e utilizar as suas ferramentas online. Para mais informação, por favor consulte o "*Bitdefender Central*" (p. 38).

Proceda consoante a sua situação.

Já tenho uma conta Bitdefender Central

Escreva o endereço de e-mail e a palavra-passe da sua conta Bitdefender Central, e, em seguida, clique em **ENTRAR**.

Se se esquecer da palavra-passe da sua conta ou se quiser simplesmente redefinir a palavra-passe anterior, clique na ligação **Redefinir palavra-passe**. Escreva o seu endereço de e-mail, em seguida, clique no botão **REDEFINIR PALAVRA-PASSE**.

Quero criar a conta Bitdefender Central

Para criar uma conta Bitdefender Central, clique na ligação **Registar-se** localizada na parte inferior da janela. Escreva as informações necessárias nos campos correspondentes e, em seguida, clique no botão **CRIAR CONTA**.

Os dados que nos fornecer serão mantidos confidenciais.

A palavra-passe tem de ter, pelo menos, 8 carateres e incluir um número.

Nota
Uma vez a conta criada, poderá utilizar o endereço de e-mail fornecido e a palavra-passe para entrar na sua conta em https://central.bitdefender.com.

Passo 6 - Introdução

Na janela Introdução, pode ver a validade da sua subscrição.

Podem ser realizadas duas tarefas adicionais neste passo:

- Compre uma nova subscrição – esta ligação redireciona-o para a página do Bitdefender de onde pode comprar uma nova subscrição.
- Tenho um código de ativação – esta ligação redireciona-o para a sua conta Bitdefender Central. Clique em **CÓDIGO DE ATIVAÇÃO** na janela A Minha Subscrição que aparece. Escreva o seu código, em seguida, clique em **SUBMETER**.

Clique em **Finalizar** para aceder à interface do Bitdefender Antivirus Plus 2016.

INTRODUÇÃO

4. OS BÁSICOS

Assim que instalar o Bitdefender Antivirus Plus 2016, o seu computador ficará protegido contra todos os tipos de malware (tais como vírus, spyware e cavalos de tróia).

A aplicação utiliza a tecnologia Photon para melhorar a velocidade e o desempenho do processo de análise do antimalware. 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.

Pode ligar o Autopilot para disfrutar de uma segurança silenciosa onde não necessita de configurar absolutamente nada. No entanto, poderá querer usufruir das definições do Bitdefender para otimizar e melhorar a sua proteção.

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.

Bitdefender tomará por si a maioria das decisões relacionadas com segurança e raramente surgirão alertas pop-up. Os pormenores sobre as ações tomadas e informações sobre o funcionament do programa encontram-se disponíveis na janela Eventos. Para mais informação, por favor consulte o "*Eventos*" (p. 17).

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 computador e os seus dados.

Para utilizar as funcionalidades online do Bitdefender Antivirus Plus 2016, gerir as suas subscrições e os dispositivos, aceda à sua conta Bitdefender Central. Para mais informação, por favor consulte o "*Bitdefender Central*" (p. 38).

A "Como" (p. 47) 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. 131) secção de possíveis soluções para os problemas mais comuns.

4.1. A abrir a janela do Bitdefender

Para aceder à interface principal do Bitdefender Antivirus Plus 2016, siga os passos abaixo:

- No **Windows 7**:
  1. Clique em **Iniciar** e vá para **Todos os Programas**.
  2. Clique em **Bitdefender 2016**.
  3. Clique em **Bitdefender Antivirus Plus 2016** ou, mais rápido, clique duas vezes no ícone do Bitdefender no tabuleiro do sistema.
- No **Windows 8 e Windows 8.1**:

  A partir do ecrã Iniciar do Windows, localize Bitdefender Antivirus Plus 2016 (por exemplo, pode começar a digitar "Bitdefender" diretamente no menu Iniciar) e, em seguida, clique no seu ícone. Em alternativa, abra a aplicação do ambiente de trabalho e, em seguida, clique duas vezes no ícone do Bitdefender no tabuleiro do sistema.
- No **Windows 10**:

  Introduza "Bitdefender" na caixa de pesquisa da barra de tarefas e, em seguida, clique no ícone correspondente. 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, por favor consulte *"Interface Bitdefender"* (p. 26).

4.2. A reparar problemas

O Bitdefender utiliza um sistema de emissão de monitoramento para detectar e informá-lo sobre os problemas que podem afectar a segurança do seu computador e dos seus dados. Por defeito, ele irá acompanhar apenas algumas questões que são consideradas muito importantes. No entanto, pode sempre configurá-lo conforme necessário, escolhendo as questões específicas sobre que deseja ser notificado.

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

- **Incidências críticas** - impedem que o Bitdefender o proteja contra o malware ou representem um risco de segurança importante.

- **Incidências menores (não críticas)** - podem afetar a sua proteção num futuro próximo.

O ícone Bitdefender na área de notificação indica incidências pendentes alterando a sua cor conforme se indica a seguir:

Incidências críticas estão a afectar a segurança do seu sistema. Eles requerem a sua atenção máxima e devem ser corrigidos o mais rapidamente possível.
Incidências não críticas estão a afetar a segurança do seu sistema. Deve verificar e repará-las quando tiver oportunidade.

Além disso, se mover o cursor do rato sobre o ícone, uma janela pop-up irá confirmar a existência de questões pendentes.

Quando abre a interface do Bitdefender, a área de estado da segurança na barra de ferramentas superior irá indicar a natureza dos problemas que afetam seu sistema.

4.2.1. Assistente Reparar Todas as Incidências

Para resolver as incidências detetadas siga o assistente **Reparar todas as incidências**.

1. Para abrir o assistente, faça uma das seguintes coisas:
   - Clique com o botão direito do rato no ícone do Bitdefender na área de notificação e selecione **Ver problemas de segurança**.
   - Abra a interface do Bitdefender e clique em qualquer lugar dentro da área de estado de segurança na barra de ferramentas superior (por exemplo, pode clicar na ligação **Corrigir todos os problemas!**).
2. Pode verificar as incidências que afectam a segurança do seu computador e dos dados. Todas as incidências atuais foram selecionadas para serem reparadas.

   Se não quiser resolver uma incidência específica de imediato, limpe a caixa correspondente. Será notificado para especificar durante quanto tempo pretende adiar a reparação da incidência. Escolha a opção desejada no menu e clique em **OK**. Para parar de monitorizar a categoria de problema respetiva, escolha **Permanentemente**.

   O estado do problema irá mudar para **Adiado** e não será tomada nenhuma ação para corrigir o problema.

3. Para corrigir todos os problemas selecionados, clique em **Corrigir**. Algumas ocorrências são tratadas imediatamente. Para outras, o assistente ajuda-o a resolvê-las.

A incidência que este assistente o ajuda a tratar pode ser agrupada numa destas categorias:

- **Desativar definições de segurança.** Tais incidências são reparadas imediatamente, ao ativar as respetivas definições de segurança.
- **Ferramentas preventivas de segurança que deve realizar.** Quando reparar a incidência, o assistente ajuda-o a completar com sucesso a tarefa.

4.2.2. Configurar os alertas de estado

O Bitdefender informa-o quando são detetadas incidências no funcionamento dos seguintes componentes do programa:

- Antivírus
- Atualização
- Segurança do Navegador

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

1. Clique no ícone  na parte superior da interface do Bitdefender e selecione **Definições Gerais** no menu suspenso.
2. Na janela **Definições Gerais** selecione a barra **Avançadas**.
3. Clique no link de **Configurar estado dos alertas**.
4. Clique nos botões para ligar ou desligar os alertas de estado de acordo com as suas preferências.

4.3. Eventos

O Bitdefender mantém um registo detalhado dos eventos relacionados com a sua atividade no seu computador. Sempre que algo de relevante para a segurança do seu sistema ou informação acontece, uma nova mensagem é adicionada aos Eventos do Bitdefender, de forma similar a um novo e-mail que aparece na sua pasta A receber.

Os eventos são uma ferramenta importante na monitorização e gestão da proteção do seu Bitdefender. Por exemplo, pode facilmente verificar se a actualização foi executada com sucesso, se foi encontrado malware no seu computador, se as suas tarefas de backup se executaram sem erros, etc. Adicionalmente, pode tomar outras ações se necessário ou alterar ações tomadas pelo Bitdefender.

Para aceder aos registos dos Eventos, faça o seguinte:

1. Clique no ícone  na parte superior da interface do Bitdefender e selecione **Eventos** no menu suspenso.

As mensagens são agrupadas de acordo com o módulo do Bitdefender cuja atividade se relacione com:

- **Atualização**
- **Antivírus**
- **Proteção da Internet**
- **Vulnerabilidade**
- **Proteção contra Ransomware**

Sempre que ocorrer um evento, pode ser visto um ponto no ícone  na parte superior da interface do Bitdefender.

Encontra-se disponível uma lista de eventos para cada categoria. Para obter informações sobre um evento em particular da lista, clique no ícone  e selecione **Eventos** do menu suspenso. Os detalhes dos eventos são apresentados no lado direito da janela. Cada evento surge com a seguinte informação: uma breve descrição, a ação do Bitdefender quando este aconteceu e a data e hora em que ocorreu. Pode ser fornecidas opções para tomar mais ações, caso seja necessário.

Pode filtrar eventos por importância e ordem de acontecimento. Existem três tipos de eventos filtrados por importância, sendo cada tipo indicado com um ícone específico:

■ 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.

Para visualizar eventos que ocorreram em determinado período de tempo, selecione o período de tempo pretendido no campo correspondente.

Para o ajudar a gerir facilmente os eventos registados, casa secção da janela de Eventos proporciona opções para eliminar ou marcar como lidos todos os eventos daquela secção.

4.4. Autopilot

Para todos os utilizadores que desejam apenas que a sua solução de segurança os proteja sem os incomodar, o Bitdefender Antivirus Plus 2016 foi concebido com um modo AutoPilot incorporado.

Em Autopilot, o Bitdefender aplica uma configuração de segurança ótima e toma, por si, todas as decisões relacionadas com a segurança. Isto significa que não verá pop-ups nem alertas e não terá de configurar quaisquer definições.

No modo Autopilot, o Bitdefender repara automaticamente incidências críticas, ativa opões e gere tranquilamente:

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

Para ligar ou desligar o Autopilot, siga os seguintes passos:

1. Clique no botão **Autopilot** na barra de ferramentas superior da interface do Bitdefender.

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

Importante
Enquanto o Autopilot estiver ligado, se modificar alguma das definições este será desligado.

Para ver o histórico das ações executadas pelo Bitdefender enquanto o Autopilot estava ligado, abra a janela Eventos.

4.5. Perfis e Modo de Bateria

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.

Para se adaptar a estas situações especiais, o Bitdefender Antivirus Plus 2016 inclui dois modos de funcionamento especial:

- Perfis
- Modo de Bateria

4.5.1. Perfis

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.

A ativar e a desativar perfis

Para ativar ou desativar perfis, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Ferramentas**.
3. Clique no módulo de **Perfis**.
4. Na janela **Perfis**, selecione o separador **Definições de Perfis**.

5. Ative ou desative os perfis clicando no botão correspondente.

Configure o Autopilot para monitorizar os perfis

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

Para permitir o Autopilot gerir os perfis, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Ferramentas**.
3. Clique no módulo de **Perfis**.
4. Na janela **Perfis**, selecione o separador **Definições de Perfis**.
5. Marque a caixa correspondente **Permitir o Autopilot gerir os meus perfis**.

Caso não queira que o seu Perfil seja controlado automaticamente, deixe a caixa desmarcada e escolha manualmente a partir da lista suspensa **PERFIS** na interface do Bitdefender.

Para obter mais informações sobre os Perfis, consulte o"*Perfis*" (p. 124)

4.5.2. Modo de Bateria

O 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 que selecionou.

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.
- A Miniaplicação de Segurança é desligada.

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.

Para ativar ou desativar o Modo de Bateria, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Ferramentas**.
3. Clique no módulo **Perfis**, em seguida, selecione o separador **Modo de Bateria**.
4. Ative ou desative o Modo de Bateria automático clicando no botão correspondente.

   Arraste o cursor correspondente pela escala para definir quando o sistema deve começar a funcionar em Modo de Bateria. Por defeito, o modo é ativado quando o nível da bateria cai abaixo dos 30%.

Nota
O Modo de Bateria é ativado, por defeito, em portáteis e tablets.

A configurar o Modo de Bateria

Para configurar o Modo de Bateria, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Ferramentas**.
3. Clique no módulo **Perfis**, em seguida, selecione o separador **Modo de Bateria**.
4. Ative a funcionalidade clicando no botão correspondente.
5. Clique no botão **Configurar**.
6. 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.
7. Clique em **Guardar** para guardar as alterações e fechar a janela.

4.6. Definições de proteção da palavra-passe de Bitdefender

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

Para configurar a proteção de palavra-passe para as definições do Bitdefender, siga os seguintes passos:

1. Clique no ícone  na parte superior da interface do Bitdefender e selecione **Definições Gerais** no menu suspenso.
2. Na janela **Definições Gerais**, selecione o separador **Definições Gerais**.
3. Ative a Proteção por palavra-passe clicando no botão correspondente.
4. Insira a palavra-passe nos dois campos e depois 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 da palavra-passe, siga os seguintes passos:

1. Clique no ícone  na parte superior da interface do Bitdefender e selecione **Definições Gerais** no menu suspenso.
2. Na janela **Definições Gerais**, selecione o separador **Definições Gerais**.
3. Desligue a protecção por palavra-passe, clicando no botão. Digite a nova palavra-passe e depois clique em **OK**.

Nota

Para alterar a palavra-passe para o seu produto, clique na hiperligação **Alterar palavra-passe**.

4.7. Relatórios anónimos de utilização

Por defeito, o Bitdefender envia relatórios que contêm informação sobre como o usar nos 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.

Caso queira parar de enviar Relatórios Anónimos de utilização, siga os seguintes passos:

1. Clique no ícone  na parte superior da interface do Bitdefender e selecione **Definições Gerais** no menu suspenso.
2. Na janela **Definições Gerais** selecione a barra **Avançadas**.
3. Clique no botão para ligar os Relatórios anónimos de utilização.

4.8. Ofertas especiais e notificações de produto

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.

Adicionalmente, as notificações do produto poderão aparecer quando o utilizador fizer alterações no produto.

Para ativar ou desativar as ofertas especiais e as notificações do produto, siga estes passos:

1. Clique no ícone  na parte superior da interface do Bitdefender e selecione **Definições Gerais** no menu suspenso.
2. Na janela **Definições Gerais**, selecione o separador **Definições Gerais**.
3. Ative ou desative as ofertas especiais e as notificações do produto clicando no botão correspondente.

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

Nota

Depois de desativar as ofertas especiais e as notificações do produto, o Bitdefender irá continuar a mantê-lo informado sobre as ofertas especiais quando utilizar uma versão de avaliação, quando a sua subscrição expirar ou ao utilizar uma versão do produto expirada.

5. INTERFACE BITDEFENDER

O Bitdefender Antivirus Plus 2016 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.

Para ver o estado do produto e realizar tarefas essenciais, encontra-se disponível o ícone na área de notificação do sistema do Bitdefender a qualquer momento.

A janela principal permite o acesso a informações importantes do produto, a módulos do program e permite-lhe realizar tarefas comuns. Da janela principal, pode aceder aos módulos do Bitdefender para configurações detalhadas e tarefas administrativas avançadas, e gerir o comportamento do produto utilizando o Autopilot e Perfis.

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

5.1. 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.

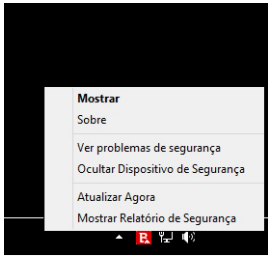
Nota

O ícone do Bitdefender poderá não estar visível a toda a hora. Para fazer com que o ícone apareça sempre, faça o seguinte:

- 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 Agent**.
- No **Windows 10**:
  1. Clique com o botão direito do rato na barra de tarefas e seleccione **Propriedades**.
  2. Clique em **Personalizar** na janela da barra de tarefas.
  3. Clique no link de **Selecione quais ícones aparecem na barra de ferramentas** na janela de **Notificações e ações**.

4. Ative o botão ao lado do **Agente do Bitdefender**.

Se 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.



Ícone Tray

- **Mostrar** - abre a janela principal do Bitdefender.
- **Acerca** - abre uma janela onde pode ver informação acerca do Bitdefender e onde procurar ajuda caso algo de inesperado lhe apareça.
- **Ver problemas de segurança** - ajuda-o a remover as vulnerabilidades de segurança. Se a opção não está disponível, é porque não há incidências a reparar. Para mais informações, por favor consulte "*A reparar problemas*" (p. 15).
- **Ocultar / Mostrar Dispositivo Segurança** - ativa / desativa Dispositivo Segurança.
- **Atualizar agora** - executa uma atualização imediata. Pode seguir o estado das atualizações no painel de Atualizações da janela principal do Bitdefender.
- **Mostrar Relatório de Segurança** - abre uma janela onde pode visualizar o estado semanal e recomendações para o seu sistema. Pode seguir as recomendações para melhorar a segurança do seu sistema.

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

Incidências críticas estão a afectar a segurança do seu sistema. Eles requerem a sua atenção máxima e devem ser corrigidos o mais rapidamente possível.
Incidências não críticas estão a afetar a segurança do seu sistema. Deve verificar e repará-las quando tiver oportunidade.
O Autopilot do Bitdefender está ligado.

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 licença de chave expira. Também pode ocorrer quando os serviços

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

5.2. Janela Principal

A janela principal do Bitdefender 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 está organizada em duas áreas principais:

Barra de ferramentas superior
: Aqui é onde pode verificar o estado de segurança do seu computador, configurar o comportamento do Bitdefender em casos especiais e aceder a tarefas importantes.

Área dos botões de ação
: Aqui é onde pode aceder à conta do dashboard Bitdefender Central e executar diferentes tarefas para manter o seu sistema protegido e a funcionar na velocidade ideal.

O ícone  no canto inferior esquerdo da interface principal dá-lhe acesso aos módulos do produto para que possa iniciar a configuração das definições do produto.

O ícone  na parte superior da interface principal permite-lhe gerir a sua conta e aceder às funcionalidades online do seu produto a partir do dashboard da conta. Aqui pode também aceder aos Eventos, ao Relatório de Segurança semanal e à página de Ajuda & Suporte.

Link	Descrição
Número de dias que faltam	O tempo restante antes da sua subscrição atual expirar é exibido. Clique no link para abrir a janela onde pode ver mais informação acerca da sua chave de licença ou registar o seu produto com a nova chave de licença.

5.2.1. Barra de ferramentas superior

A barra de ferramentas superior contém os seguintes elementos:

- A **Área de Estado da Segurança** do lado esquerdo da barra de ferramentas, informa se existem incidências a afetar a segurança do seu computador e ajuda a repará-las.

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

  - **A área está colorida de verde.** Não existem incidências para reparar. O seu computador e os seus dados estão protegidos.
  - **A área está colorida de amarelo.** Incidências não críticas estão a afetar a segurança do seu sistema. Deve verificar e repará-las quando tiver oportunidade.
  - **A área está colorida de vermelho.** Incidências críticas estão a afectar a segurança do seu sistema. Deve resolver estas incidências imediatamente.

  Ao clicar em qualquer lugar na área de estado de segurança, poderá aceder a um assistente que irá ajudar a remover facilmente quaisquer ameaças do seu computador. Para mais informações, por favor consulte "*A reparar problemas*" (p. 15).

- O **Autopilot** permite-lhe executar o Autopilot e desfrutar da segurança de forma completamente silenciosa. Para mais informações, por favor consulte "*Autopilot*" (p. 19).
- Os **Perfis** permitem-lhe trabalhar, jogar ou ver filmes poupando tempo ao configurar o sistema para adiar tarefas de manutenção. Para mais informações, por favor consulte "*Perfis*" (p. 124).

5.2.2. Botões de ação

Pode utilizar os botões de ação para aceder rapidamente à sua conta Bitdefender Central e realizar tarefas importantes.

Os botões de ação disponíveis nesta área são:

- **Ir para Bitdefender Central**. Aceda à sua conta Bitdefender Central para verificar as suas subscrições e realizar tarefas de segurança nos dispositivos que controla.
- **Análise Rápida**. Execute uma análise rápida para garantir que o seu computador está livre de vírus.

- **Ver Vulnerabilidades**. Verifique o seu computador para identificar vulnerabilidades e garantir que todas as aplicações instaladas, para além do sistema operativo, estão atualizadas e a funcionar corretamente.
- **Safepay**. Abra o Bitdefender Safepay™ para proteger os seus dados pessoais enquanto efetua transações online.
- **Atualização**. Atualize o seu Bitdefender para garantir que tem as assinaturas de malware mais recentes.

5.3. Os módulos do Bitdefender

O Bitdefender vem com vários módulos úteis para protegê-lo enquanto trabalha, navega na Web, joga ou realiza pagamentos online.

Sempre que quiser aceder aos módulos ou começar a configurar o seu produto, clique no ícone  no canto inferior esquerdo da interface do Bitdefender.

Os módulos são separados em três separadores, com base nas funções que oferecem:

- Proteção
- Privacidade
- Ferramentas

5.3.1. **Proteção**

Neste separador pode configurar o seu nível de segurança e definir quais vulnerabilidades do sistema devem ser corrigidas.

Os módulos que pode gerir no Painel de Proteção são:

Antivírus

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

Do módulo Antivírus pode aceder facilmente às seguintes tarefas de análise:

- Análise Rápida
- Análise do Sistema
- Gerir Análises
- Modo de Recuperação

Para mais informações sobre tarefas de análise e como configurar a proteção antivírus, por favor consulte "*Proteção Antivírus*" (p. 73).

Proteção da Internet

A proteção da Web 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 "*Proteção da Internet*" (p. 98).

Vulnerabilidade

O módulo de Vulnerabilidade ajuda-o a manter o sistema operativo e as aplicações que utiliza regularmente atualizados.

Clique em **Análise de Vulnerabilidade** no módulo de Vulnerabilidade para começar a identificar atualizações críticas do Windows, atualizações de aplicações e palavras-passe fracas em contas do Windows.

Para mais informações sobre como configurar a proteção de vulnerabilidade, consulte "*Vulnerabilidade*" (p. 102).

Proteção contra Ransomware

O módulo de Proteção contra Ransomwares protege os seus ficheiros pessoais contra ataques de hackers.

Para mais informações sobre como configurar a Proteção contra Ransomwares para proteger o seu sistema contra ataques de ransomware, consulte "*Proteção contra Ransomware*" (p. 106).

5.3.2. Privacidade

No Separador de privacidade, pode proteger as suas transações online e manter a sua experiência de navegação segura.

Os módulos que podem ser geridos no Painel de Privacidade são:

Proteção de dados

O módulo de Proteção de dados permite-lhe apagar os ficheiros permanentemente.
Clique em **Destruidor de Ficheiros** sob o módulo de proteção de dados para iniciar o assistente que irá permitir-lhe eliminar completamente os ficheiros do seu sistema.

Para mais informações sobre como configurar a Proteção de Dados, consulte "*Proteção de dados*" (p. 100).

Gestor de palavras-passe

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.

A partir do Gestor de palavras-passe pode selecionar as seguintes tarefas:

- **Abrir Carteira** - abre a base de dados existente da Carteira.
- **Bloquear carteira** - bloqueia a base de dados existente da Carteira.
- **Exportar Carteira** - permite-lhe guardar a base de dados existente numa localização do seu sistema.
- **Criar nova Carteira** - inicia um assistente que lhe permite criar uma nova base de dados da Carteira.

Para mais informações sobre como configurar o Gestor de palavras-passe, consulte "*Proteção do Gestor de palavras-passe para as suas credenciais*" (p. 114).

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.

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

Para mais informações sobre o Bitdefender Safepay™, consulte "*Segurança Safepay para transações online*" (p. 109).

5.3.3. Ferramentas

No separador Ferramentas, pode configurar o seu perfil de trabalho.

Os módulos que pode gerir no separador das Ferramentas são:

Perfis

Os Perfis do Bitdefender ajudam-lhe a ter uma experiência de utilizador simplificada enquanto trabalha, vê um filme ou joga, através da monitorização do produto e das ferramentas de trabalho do sistema. Clique em **Ativar agora** na barra de ferramentas superior da interface do Bitdefender para começar a utilizar este recurso.

O Bitdefender permite-lhe configurar os seguintes perfis:

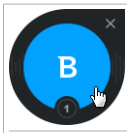
- Perfil Trabalho
- Perfil de Filme
- Perfil de Jogo

Para mais informações sobre como configurar o módulo dos perfis, consulte "*Perfis*" (p. 124).

5.4. Dispositivo de Segurança

Dispositivo Segurança é a forma rápido e fácil de controlar o Bitdefender Antivirus Plus 2016. Adicionar este dispositivo pequeno e não intrusivo ao seu ambiente de trabalho deixa-o ver informação critica e levar a cabo tarefas chave em qualquer altura:

- abrir a janela principal do Bitdefender.
- monitorizar a atividade de análise em tempo-real.
- monitorizar o estado de segurança do seu sistema e reparar qualquer incidência que exista.
- ver quando uma atualização está em curso.
- ver os avisos e obter acesso aos mais recentes eventos reportados pelo Bitdefender.
- analisar ficheiros ou pastas ao arrastar e largar um ou vários itens sobre o dispositivo.



Dispositivo de Segurança

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


Incidências críticas estão a afectar a segurança do seu sistema.

Eles requerem a sua atenção máxima e devem ser corrigidos o mais rapidamente possível. Clique no ícone do estado para começar a reparar as incidências reportadas.

 Incidências não críticas estão a afetar a segurança do seu sistema. Deve verificar e repará-las quando tiver oportunidade. Clique no ícone do estado para começar a reparar as incidências reportadas.

 O seu sistema está protegido.

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

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

O lado inferior do dispositivo apresenta o contador de eventos não lidos (o número de eventos importantes comunicados pelo Bitdefender, caso haja algum). Clique no contador de eventos, por exemplo, 1 para um evento não lido, para abrir a janela de Eventos. Para mais informação, por favor consulte o "*Eventos*" (p. 17).

5.4.1. Analisar ficheiros e pastas

Pode usar o Dispositivo de Segurança para analisar rapidamente ficheiros e pastas. Arraste qualquer ficheiro ou pasta que deseje analisar e largue-o sobre o **Dispositivo Segurança**.

O Assistente de Análise Antivírus irá surgir e guiá-lo através do processo de análise. As opções de análise estão pré-configuradas para obter os melhores resultados de deteção e não podem ser alterados Se forem detectados ficheiros infectados, o Bitdefender irá tentar desinfectá-los (remover o código de malware). Se a desinfecção falha, o assistente de análise antivírus irá permitir-lhe definir outras acções a serem levadas a cabo sobre os ficheiros infectados.

5.4.2. Ocultar / mostrar Dispositivo de Segurança

Quando não desejar mais ver o dispositivo, clique em ⊗.

Para restaurar o Widget de Segurança, utilize um dos seguintes métodos:

- Do tabuleiro do sistema:
  1. Clique com o botão direito do rato no ícone do Bitdefender no ícone do tabuleiro do sistema.

2. Clique em **Mostrar Dispositivo Segurança** no menu contextual que aparece.

- A partir da interface do Bitdefender:

1. Clique no ícone  na parte superior da interface do Bitdefender e selecione **Definições Gerais** no menu suspenso.
2. Na janela **Definições Gerais**, selecione o separador **Definições Gerais**.
3. Ligar **Exibir Widget de Segurança** ao clicar no botão correspondente.

5.5. Relatório de Segurança

O Relatório de Segurança fornece um estado semanal para o seu produto e diversas dicas para melhorar a proteção do sistema. Estas dicas são importantes para gerir a proteção geral e poderá facilmente identificar as ações que pode tomar para o seu sistema.

O relatório é gerado uma vez por semana e resume informações relevantes sobre as atividades do produto para que possa facilmente compreender o que ocorreu durante este período.

As informações oferecida pelo Relatório de Segurança dividem-se em duas categorias:

- Área de **Proteção** - veja as informações relacionadas com a proteção do seu sistema.
  - **Ficheiros analisados**

    Permite-lhe visualizar os ficheiros analisados pelo Bitdefender durante a semana. Pode ver detalhes como o número de ficheiros analisados e o número de ficheiros limpos pelo Bitdefender.

    Para obter mais informações sobre a proteção antivírus, consulte "*Proteção Antivírus*" (p. 73).

  - **Sites Web Analisados**

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

    Para mais informações sobre a Proteção da Internet, consulte "*Proteção da Internet*" (p. 98).

- **Vulnerabilidades**

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

  Para obter mais informações sobre a análise de vulnerabilidade, consulte "*Vulnerabilidade*" (p. 102).

- **Linha Cronológica de Eventos**

  Permite que tenha uma imagem geral de todos os processos de análise e problemas corrigidos pelo Bitdefender durante a semana. Os eventos são separados por dias.

  Para mais informações sobre um registo detalhado de eventos relativos à atividade no seu computador, consulte Eventos.

- Área de **Otimização** - veja informações relacionadas com o espaço libertado, aplicações otimizadas e quanta bateria do computador economizou utilizando o Modo de Bateria.

  - **Bateria economizada**

    Permite-lhe ver quanta bateria economizou enquanto o sistema funcionou em Modo de Bateria.

    Para mais informações sobre o Modo de Bateria, consulte "*Modo de Bateria*" (p. 21).

  - **Aplicações otimizadas**

    Permite-lhe ver o número de aplicações utilizadas nos Perfis.

    Para mais informações sobre Perfis, consulte "*Perfis*" (p. 124).

5.5.1. A verificar o Relatório de Segurança

O Relatório de Segurança utiliza um sistema de rastreio de problemas para detectar e o informar sobre os problemas que podem afetar a segurança do seu computador e dados. As incidências detetadas incluem definições de proteção importantes que estão desligadas e outras condições que podem representar um risco de segurança. Ao utilizar o relatório, pode configurar componentes específicos do Bitdefender ou tomar ações preventivas para proteger o seu computador e dados privados.

Para verificar o Relatório de Segurança, siga estes passos:

1. Aceder ao relatório:

- Clique no ícone  na parte superior da interface do Bitdefender e, em seguida, selecione **Relatório de Segurança** no menu suspenso.
- Clique com o botão direito do rato no ícone do Bitdefender no tabuleiro do sistema e selecione **Mostrar relatório de segurança**.
- Após a conclusão de um relatório receberá uma notificação pop-up. Clique em **Mostrar** para aceder ao relatório de segurança.

  Abrir-se-á uma página Web no navegador Web onde pode visualizar o relatório gerado.

2. Observe a parte superior da janela para visualizar o estado geral de segurança.
3. Verifique as nossas recomendações na parte inferior da página.

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

- **A área está verde.** Não existem problemas a corrigir. O seu computador e os seus dados estão protegidos.
- **A área está amarela.** A segurança do seu sistema está a ser afetada por problemas não críticos. Deve verificar e repará-las quando tiver oportunidade.
- **A área está vermelha.** A segurança do seu sistema está a ser afetada por problemas críticos. Deve resolver estas incidências imediatamente.

5.5.2. Ativar ou desativar a notificação do Relatório de Segurança

Para ligar ou desligar a notificação do Relatório de Segurança, siga estes passos:

1. Clique no ícone  na parte superior da interface do Bitdefender e selecione **Definições Gerais** no menu suspenso.
2. Na janela **Definições Gerais**, selecione o separador **Definições Gerais**.
3. Clique no botão correspondente para ativar ou desativar a notificação do Relatório de Segurança.

   A notificação do Relatório de Segurança está ativada por defeito.

6. 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 iniciar sessão na sua conta Bitdefender Central a partir de qualquer computador ou dispositivo móvel ligado à Internet através https://central.bitdefender.com. Assim que tiver obtido acesso, pode realizar o seguinte:

- Transferir e instalar o Bitdefender nos sistemas operativos Windows, OS X e Android. Os produtos disponíveis para download são:
  - Bitdefender Antivirus Plus 2016
  - O Antivírus Bitdefender para Mac
  - Bitdefender Mobile Security
- Gerir e renovar as suas subscrições do Bitdefender.
- Adicionar novos dispositivos à sua rede e gerir as suas funcionalidades onde quer que esteja.

6.1. Aceder à sua conta Bitdefender Central

Há várias formas de aceder à sua conta Bitdefender Central. Dependendo da tarefa que quiser realizar, pode utilizar qualquer uma das seguintes opções:

- A partir da interface principal do Bitdefender:
  1. Clique na ligação **Ir para Bitdefender Central** na lateral esquerda da interface do Bitdefender.
- Das Informações da conta:
  1. Clique no ícone  na parte superior da interface do Bitdefender e, em seguida, selecione **Informações da conta** no menu suspenso.
  2. Clique na ligação **Ir para Bitdefender Central** na parte inferior da janela que abrirá.
- 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 seu conta com o seu endereço de e-mail e palavra-passe.

6.2. As minhas subscrições

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

6.2.1. Verificar subscrições disponíveis

Para verificar as suas subscrições disponíveis:

1. Aceder à sua conta 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 produtos diferentes.

6.2.2. Adicionar um novo dispositivo

Caso a sua subscrição cubra mais do que um dispositivo, pode adicionar um novo dispositivo e instalar o seu Bitdefender Antivirus Plus 2016 no mesmo, conforme descrito abaixo:

1. Aceder à sua conta Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.
3. Na janela **Os Meus Dispositivos**, clique em **INSTALAR Bitdefender**.
4. Escolha **Windows**, em seguida, escolha uma das duas opções disponíveis:
   - Eu gostaria de instalar o Bitdefender **Neste dispositivo**.

     Selecione o Bitdefender Antivirus Plus 2016 da lista **Produto a ser instalado** e, em seguida, clique em **Download** para continuar.
   - Eu gostaria de instalar o Bitdefender **Noutro dispositivo**.

Selecione o Bitdefender Antivirus Plus 2016 da lista **Produto a ser instalado**. Escreva um endereço de e-mail no campo correspondente e clique em **ENVIAR**.

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

6.2.3. Renovar subscrição

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

1. Aceder à sua conta 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.

6.2.4. Ativar subscrição

Uma subscrição pode ser ativada durante o processo de instalação utilizando a sua conta Bitdefender Central. 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 da sua subscrição do Bitdefender, desde que o código e a subscrição sejam do mesmo produto.

Para ativar uma subscrição com um código de ativação, siga os passos abaixo:

1. Aceder à sua conta 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 **SUBMETER**.

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

6.3. Meus dispositivos

A seção **Os Meus Dispositivos** na sua conta Bitdefender Central 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 o tempo disponível da sua subscrição.

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

1. Aceder à sua conta Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.
3. Clique no ícone ⋮ no cartão de dispositivo pretendido e, em seguida, selecione **Definições**.
4. Altere o nome do dispositivo no campo correspondente e, em seguida, selecione **Guardar**.

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

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

1. Aceder à sua conta Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.
3. Clique no ícone ⋮ no cartão de dispositivo pretendido e, em seguida, selecione **Perfil**.
4. Clique em **Adicionar proprietário** e preencha os campos correspondentes. Defina o Sexo, Data de nascimento e selecione até uma Foto de perfil.
5. Clique em **ADICIONAR** para guardar o perfil.
6. Selecione o proprietário pretendido na lista **Proprietário do dispositivo** e, em seguida, clique em **ATRIBUIR**.

Para atualizar o Bitdefender remotamente num dispositivo, siga os seguintes passos:

1. Aceder à sua conta Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.

3. Clique no ícone ⋮ no cartão de dispositivo pretendido e, em seguida, 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 verificar o estado da proteção dos seus produtos Bitdefender e o número de dias restantes na sua subscrição. O estado da proteção pode estar a verde, quando não houver problemas que afetem o seu dispositivo, ou a vermelho quando o dispositivo estiver em risco. Quando houver problemas a afetar o seu produto, clique em **Visualizar problemas** para descobrir 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*" (p. 81) e "*Executar uma Análise Rápida*" (p. 80).
- **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 alguma seja encontrada, deve realizar uma nova verificação de vulnerabilidades no dispositivo problemático e, em seguida, realizar as ações recomendadas. Para mais detalhes sobre esta funcionalidade, consulte "*Vulnerabilidade*" (p. 102).

7. MANTENHA O SEU BITDEFENDER ATUALIZADO.

Todos os dias são encontrados e identificados novos vírus. Esta é a razão pela qual é muito importante manter o Bitdefender actualizado com as últimas assinaturas de malware.

Se está ligado à Internet através de banda larga ou ADSL, o Bitdefender executa esta operação sozinho. Por defeito, quando liga o computador verifica se há actualizações e depois disso fá-lo a cada **hora** . Se forem detectadas actualizações, serão automaticamente descarregadas e instaladas no seu computador.

O processo de actualização é executado "on the fly", o que significa que os ficheiros são substituídos progressivamente. Desta forma, o processo de actualização não afectará o funcionamento do produto e, ao mesmo tempo, exclui qualquer possibilidade de vulnerabilidade.

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

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

- Se o seu computador se ligar a Internet através de um servidor proxy, você deve configurar as definições do proxy conforme escrito em "*Como posso configurar Bitdefender para usar um proxy de ligação à Internet?*" (p. 67).
- Se não possui uma ligação à Internet, pode atualizar Bitdefender manualmente conforme descrito em "*O Meu Computador não está ligado à Internet. Como posso actualizar o Bitdefender?*" (p. 138). O ficheiro de atualização manual é publicado uma vez por semana.
- Podem ocorrer erros ao descarregar atualizações com uma ligação lenta à Internet. Para saber como ultrapassar tais erros, consulte "*Como atualizar o Bitdefender numa ligação à Internet lenta*" (p. 137).
- 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, por favor consulte o "*A efetuar uma atualização*" (p. 44).

7.1. Verifique se o Bitdefender está atualizado

Para verificar a data da última atualização do seu Bitdefender, observe a **Área do Estado da Segurança**, do lado esquerdo da barra de ferramentas.

Para informações mais detalhadas acerca das mais recentes actualizações, verifique os eventos de actualização:

1. Na janela principal, clique no ícone  na parte superior da interface do Bitdefender e selecione **Eventos** no menu suspenso.
2. Na janela **Eventos**, selecione **Atualizar** no menu suspenso correspondente.

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

7.2. A efetuar uma atualização

Para realizar actualizações, é necessária uma ligação à Internet.

Para iniciar uma atualização, faça o seguinte:

- Abra a interface do Bitdefender e clique no botão de ação **Atualizar**.
- Clique com o botão direito no ícone  do Bitdefender na barra de sistema e selecione **Atualizar Agora**.

O módulo Actualização irá ligar-se ao servidor de actualização de Bitdefender e verificará se existem actualizações. 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 computador quando a actualização 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 num dispositivo, siga os seguintes passos:

1. Aceder à sua conta Bitdefender Central.

2. Selecione o painel **Os Meus Dispositivos**.
3. Clique no ícone ⋮ no cartão de dispositivo pretendido e, em seguida, selecione **Atualizar**.

7.3. Ligar ou desligar a atualização automática

Para ativar ou desativar a análise automática, siga estes passos:

1. Clique no ícone na parte superior da interface do Bitdefender e selecione **Definições Gerais** no menu suspenso.
2. Na janela de **Definições Gerais**, selecione o separador **Atualizar**.
3. Clique no botão para ativar ou desativar a atualização automática.
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 a atualização automática durante 5, 15 ou 30 minutos, por uma hora, permanentemente ou até ao reinício 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.

7.4. 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, siga estes passos:

1. Clique no ícone na parte superior da interface do Bitdefender e selecione **Definições Gerais** no menu suspenso.

2. Na janela **Definições Gerais**, 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.

Atualizar localização

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

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

Pode voltar à localização de atualização genérica da Internet clicando em **Predefinição**.

Regras de atualização

Pode escolher entre três formas para descarregar e instalar atualizações:

- **Atualização silenciosa** - O Bitdefender faz automaticamente o download e a implementação da atualização.
- **Avisar antes de descarregar** - sempre que uma atualização está disponível, será consultado antes do download ser feito.
- **Avisar antes de instalar** - cada vez que uma atualização for descarregada, será consultado antes da instalação ser feita.

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 computador. Isto serve para evitar que o processo de actualização de Bitdefender interfira com o trabalho do utilizador.

Se quiser ser avisado quando uma atualização requere um reinício, desligue a opção **Adiar reiniciar** clicando no botão correspondente.

COMO

8. INSTALAÇÃO

8.1. Como instalo o Bitdefender num segundo computador?

Caso a subscrição que comprou cubra mais do que um computador, pode utilizar a sua conta Bitdefender Central para registar um segundo PC.

Para instalar o Bitdefender num segundo computador, faça o seguinte:

1. Aceder à sua conta Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.
3. Na janela **Os Meus Dispositivos**, clique em **INSTALAR Bitdefender**.
4. Escolha **Windows**, em seguida, escolha uma das duas opções disponíveis:
   - Eu gostaria de instalar o Bitdefender **Neste dispositivo**.

     Na lista **Produto a ser instalado**, selecione o Bitdefender Antivirus Plus 2016 e, em seguida, clique em **Download** para continuar.
   - Eu gostaria de instalar o Bitdefender **Noutro dispositivo**.

     Selecione o Bitdefender Antivirus Plus 2016 da lista **Produto a ser instalado**. Escreva um endereço de e-mail no campo correspondente e clique em **ENVIAR**.
5. Execute o Bitdefender que transferiu. Aguarde até que o processo de instalação esteja concluído e feche a janela.

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

8.2. Quando é que devo reinstalar o Bitdefender?

Nalgumas situações poderá ter de reinstalar o seu produto Bitdefender.

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

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

Para reinstalar o Bitdefender, pode utilizar o disco de instalação que adquiriu ou transferir uma nova versão da sua conta Bitdefender Central.

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

8.3. Onde posso transferir o meu produto Bitdefender?

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

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

Para instalar o Bitdefender da conta Bitdefender Central, siga estes passos:

1. Aceder à sua conta Bitdefender Central.
2. Selecione o painel **Os Meus Dispositivos**.
3. Na janela **Os Meus Dispositivos**, clique em **INSTALAR Bitdefender**.
4. Escolha **Windows**, em seguida, escolha uma das duas opções disponíveis:
   - Eu gostaria de instalar o Bitdefender **Neste dispositivo**.

     Selecione o Bitdefender Antivirus Plus 2016 da lista **Produto a ser instalado** e, em seguida, clique em **Download** para continuar.
   - Eu gostaria de instalar o Bitdefender **Noutro dispositivo**.

     Selecione o Bitdefender Antivirus Plus 2016 da lista **Produto a ser instalado**. Escreva um endereço de e-mail no campo correspondente e clique em **ENVIAR**.
5. Execute o Bitdefender que transferiu.

8.4. 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, será necessário reinstalar o produto utilizando a versão mais recente disponível.

  Para resolver esta situação, siga estes passos:

  1. Remova o Bitdefender seguindo estes passos:
     - No **Windows 7**:
       a. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
       b. Encontre o **Bitdefender Antivirus Plus 2016** e selecione **Desinstalar**.
       c. Clique em **Remover** na janela que aparece e, em seguida, selecione **Eu quero reinstalá-lo**.
       d. Clique em **Seguinte** para continuar.
       e. Aguarde que o processo de desinstalação termine, depois reinicie o seu 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 Antivirus Plus 2016** e selecione **Desinstalar**.
       d. Clique em **Remover** na janela que aparece e, em seguida, selecione **Eu quero reinstalá-lo**.
       e. Clique em **Seguinte** para continuar.

f. Aguarde que o processo de desinstalação termine, depois reinicie o seu 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 Antivirus Plus 2016** e selecione **Desinstalar**.

d. Clique em **Desinstalar** novamente para confirmar a sua escolha.

e. Clique em **Remover** e, em seguida, selecione **Eu quero reinstalá-lo**.

f. Clique em **Seguinte** para continuar.

g. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

2. Transfira o ficheiro de instalação:

a. Aceder à sua conta Bitdefender Central.

b. Selecione o painel **Os Meus Dispositivos**.

c. Na janela **Os Meus Dispositivos**, clique em **INSTALAR Bitdefender**.

d. Escolha **Windows**, em seguida, escolha uma das duas opções disponíveis:

- Eu gostaria de instalar o Bitdefender **Neste dispositivo**.

  Selecione o Bitdefender Antivirus Plus 2016 da lista **Produto a ser instalado** e, em seguida, clique em **Download** para continuar.

- Eu gostaria de instalar o Bitdefender **Noutro dispositivo**.

  Selecione o Bitdefender Antivirus Plus 2016 da lista **Produto a ser instalado**. Escreva um endereço de e-mail no campo correspondente e clique em **ENVIAR**.

3. Localize e clique duas vezes no instalador para iniciar o processo de instalação.

- 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. Aceder à sua conta Bitdefender Central.
   b. Selecione o painel **Os Meus Dispositivos**.
   c. Na janela **Os Meus Dispositivos**, clique em **INSTALAR Bitdefender**.
   d. Escolha **Windows**, em seguida, escolha uma das duas opções disponíveis:
      - Eu gostaria de instalar o Bitdefender **Neste dispositivo**.

        Selecione o Bitdefender Antivirus Plus 2016 da lista **Produto a ser instalado** e, em seguida, clique em **Download** para continuar.
      - Eu gostaria de instalar o Bitdefender **Noutro dispositivo**.

        Selecione o Bitdefender Antivirus Plus 2016 da lista **Produto a ser instalado**. Escreva um endereço de e-mail no campo correspondente e clique em **ENVIAR**.
2. Localize e clique duas vezes no instalador para iniciar o processo de instalação.

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

8.5. Como reparo o Bitdefender?

Caso pretenda reparar o Bitdefender Antivirus Plus 2016 a partir do menu Iniciar do Windows, siga estes passos:

- No **Windows 7**:
  1. Clique em **Iniciar** e vá para **Todos os Programas**.
  2. Encontre o **Bitdefender Antivirus Plus 2016** e selecione **Desinstalar**.
  3. Clique em **Reparar** na janela que aparece.

     Isto irá demorar vários minutos.
  4. Precisará de reiniciar o computador 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 Antivirus Plus 2016** e selecione **Desinstalar**.
4. Clique em **Reparar** na janela que aparece.

   Isto irá demorar vários minutos.
5. Precisará de reiniciar o computador 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 Antivirus Plus 2016** e selecione **Desinstalar**.
4. Clique em **Desinstalar** novamente para confirmar a sua escolha.
5. Clique em **Reparar**.

   Isto irá demorar vários minutos.
6. Precisará de reiniciar o computador para concluir o processo

9. ASSINATURAS

9.1. Que produto Bitdefender estou a usar?

Para descobrir que programa do Bitdefender instalou:

1. Abra a interface do Bitdefender.
2. No cimo da janela deverá ver um dos seguintes:
   - Bitdefender Antivirus Plus 2016
   - Bitdefender Internet Security 2016
   - Bitdefender Total Security 2016

9.2. Como é que ativo a minha subscrição do Bitdefender através da chave de licença?

Se tiver uma chave de licença e desejar utilizá-la para ativar uma subscrição do Bitdefender Antivirus Plus 2016, há dois possíveis casos que podem ser aplicáveis:

- Atualizou uma versão anterior do Bitdefender para a mais recente:
  1. Assim que a atualização para o Bitdefender Antivirus Plus 2016 estiver concluída, será solicitado que aceda à sua conta Bitdefender Central.
  2. Escreva as suas credenciais de acesso e clique em **ENTRAR**
  3. Uma notificação a informar-lhe de que uma assinatura foi criada aparece no ecrã da sua conta. A subscrição criada será válida pelo número de dias restantes na sua chave de licença e para o mesmo número de utilizadores.

     Dispositivos que utilizem versões anteriores do Bitdefender e que estiverem registadas com a chave de licença que converteu para uma subscrição necessitam de registar o produto na mesma conta Bitdefender Central.
- O Bitdefender não foi instalado anteriormente no sistema:
  1. Assim que o processo de instalação estiver concluído, será solicitado que aceda à sua conta Bitdefender Central.
  2. Escreva as suas credenciais de acesso e clique em **ENTRAR**

3. Selecione o painel **As Minhas Subscrições**.
4. Clique no botão **Adicionar chave de licença** e escreva a sua chave de licença.
5. Uma subscrição com a mesma validade e número de utilizadores da sua chave de licença está associada à sua conta.

10. BITDEFENDER CENTRAL

10.1. Como é que é inicio sessão na Bitdefender Central utilizando outra conta online?

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

Para utilizar outra conta com sucesso, siga estes passos:

1. Clique no ícone  na parte superior da interface do Bitdefender e selecione **Informações da conta** no menu suspenso.
2. Clique no botão **Alternar conta** para alterar a conta vinculada ao computador.
3. Escreva o endereço de e-mail e a palavra-passe da sua conta nos campos correspondentes, em seguida, clique em **ENTRAR**.

Nota
O produto Bitdefender do seu dispositivo muda automaticamente de acordo com a subscrição associada à nova conta Bitdefender Central.
Se não houver uma subscrição associada à nova conta Bitdefender Central ou caso pretenda transferi-la da conta anterior, pode contatar o Bitdefender para obter suporte, como descrito na secção "*Pedir Ajuda*" (p. 155).

10.2. Como reponho a palavra-passe da conta Bitdefender Central?

Para definir uma nova palavra-passe para a sua conta Bitdefender Central, siga estes passos:

1. Clique no ícone  na parte superior da interface do Bitdefender e selecione **Informações da conta** no menu suspenso.
2. Clique no botão **Alternar conta** para alterar a conta vinculada ao computador.

   Aparece uma nova janela.
3. Clique na ligação **Redefinir palavra-passe**.

4. Escreva o endereço de e-mail utilizado para criar a sua conta Bitdefender Central, em seguida, clique no botão **REDEFINIR PALAVRA-PASSE**.
5. Verifique o seu e-mail e clique na hiperligação fornecida.
6. Escreva o seu endereço de e-mail no campo respetivo.
7. Digite a nova palavra-passe. A palavra-passe tem de ter, pelo menos, 8 carateres e incluir números.
8. Clique em **DEFINIR PALAVRA-PASSE**.

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

11. A ANALISAR COM BITDEFENDER

11.1. 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 da Internet ficheiros que julga serem perigosos.
- Quer analisar uma partilha de rede antes de copiar os ficheiros para o seu computador.

11.2. Como posso analisar o seu sistema?

Para realizar uma análise completa ao sistema, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. No módulo **Antivírus**, selecione a **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, por favor consulte o "*Assistente de Análise Antivírus*" (p. 85).

11.3. 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 computador.

Para programar uma verificação, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. No módulo **Antivírus**, selecione **Gerir Análises**.
4. Escolha o tipo de verificação que deseja realizar, Verificação de Sistema ou Verificação Rápida, em seguida, clique em **Opções de verificação**.

   Como alternativa, pode criar um tipo de verificação que corresponda às suas necessidades clicando em **Nova tarefa personalizada**.
5. Ativar o botão **Programar**.

   Selecione uma das opções correspondentes para definir uma agenda:

   - No iniciar do sistema
   - Uma vez
   - Periodicamente

Na janela **Verificar alvos**, pode selecionar os locais que pretenda verificar.

11.4. Como posso criar uma tarefa de análise personalizada?

Se quer analisar localizações específicas no seu computador 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. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. No módulo **Antivírus**, selecione **Gerir Análises**.
4. Clique em **Nova tarefa personalizada**. Insira um nome para a análise na aba **Básico** e selecione as localizações a serem analisadas.

5. Se desejar configurar detalhadamente as opções de análise, selecione o separador **Avançado**.

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

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

6. Clique em **OK** para guardar as alterações e fechar a janela.
7. Utilize o botão correspondente se pretender definir uma agenda para a sua tarefa de verificação.
8. Clique em **Iniciar Análise** e siga o assistente de análise para a concluir. No final da análise, será notificado para escolher as ações que devem ser tomadas nos ficheiros detetados, caso os haja.
9. Se quiser, pode voltar a executar rapidamente uma análise personalizada anterior ao clicar na entrada correspondente na lista disponível.

11.5. Como posso 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, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. Clique no módulo **Antivírus**, em seguida, selecione o separador **Exclusões**.
4. Assegure-se de que as **Exclusões ficheiros** está ligada através de clicar no botão.

5. Clique na ligação **Ficheiros e pastas excluídos**.
6. Clique no botão **Adicionar** , localizado no cimo da tabela de exceções.
7. Clique em **Explorar**, selecione a pasta que deseja excluir da análise e depois clique **OK**.
8. Clique em **Adicionar** e, em seguida, em **OK** para guardar as alterações e fechar a janela.

11.6. 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 no ícone  no canto inferior direito da interface do Bitdefender.
   b. Selecione o separador **Proteção**.
   c. Clique no módulo **Antivírus**.
   d. Na janela **Antivírus**, selecione o separador **Escudo**.
   e. Clique no botão para desligar **Análise no-acesso**.

      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 fazer isto, consulte "*Como posso mostrar objetos ocultos no Windows?*" (p. 68).
3. Restaurar o ficheiro da área de Quarentena:
   a. Clique no ícone  no canto inferior direito da interface do Bitdefender.
   b. Selecione o separador **Proteção**.
   c. Clique no módulo **Antivírus**, em seguida, selecione o separador **Quarentena**.
   d. Selecione um ficheiro e clique em **Restaurar**.

4. Adicionar o ficheiro à lista de Exceções. Para saber como fazer isto, consulte "*Como posso excluir uma pasta da análise?*" (p. 60).
5. Ligue a proteção antivírus em tempo real do Bitdefender.
6. Contacte os nossos representantes do suporte para que possamos remover a assinatura de deteção. Para saber como fazer isto, consulte "*Pedir Ajuda*" (p. 155).

11.7. Como posso saber que vírus 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 directamente no assistente de análise, assim que esta terminar, clicando em **Mostrar Relatório**.

Para analisar mais tarde um relatório de análise ou qualquer infeção detetada, siga estes passos:

1. Clique no ícone  na parte superior da interface do Bitdefender e selecione **Eventos** no menu suspenso.
2. Na janela **Eventos**, selecione **Antivírus** do menu suspenso correspondente.

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

   Caso pretenda realizar a mesma análise novamente, clique no botão **Verificar novamente**.

12. CONTROLO DE PRIVACIDADE

12.1. 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, faça o seguinte:

1. Clique no botão de ação **Safepay** na interface do Bitdefender.
2. Clique no ícone para aceder ao **Teclado Virtual**.
3. Use o **Teclado Virtual** quando inserir informação sensível tal como palavras-passe.

12.2. 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 computador usando o menu contextual Windows, seguindo 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. Aparece uma janela de confirmação. Clique em **Sim** para iniciar o assistente do Destruidor de Ficheiros.
3. Aguarde que o Bitdefender termine a destruição dos ficheiros.
4. Os resultados são apresentados. Clique em **Fechar** para sair do assistente.

13. INFORMAÇÕES ÚTEIS

13.1. Como testo a minha solução antivírus?

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 proteção antivírus utilizando um ficheiro de segurança desenvolvido para este fim.

Para testar a sua solução antivírus, siga estes passos:

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 um vírus).

   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 um vírus.

   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. 155).

13.2. Como posso remover o Bitdefender?

Caso pretenda remover o Bitdefender Antivirus Plus 2016, siga os seguintes 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 Antivirus Plus 2016** e selecione **Desinstalar**.

3. Clique em **Remover** e, em seguida, selecione **Eu quero removê-lo permanentemente**.
4. Clique em **Seguinte** para continuar.
5. Aguarde que o processo de desinstalação termine, depois reinicie o seu 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 Antivirus Plus 2016** e selecione **Desinstalar**.
4. Clique em **Remover** e, em seguida, selecione **Eu quero removê-lo permanentemente**.
5. Clique em **Seguinte** para continuar.
6. Aguarde que o processo de desinstalação termine, depois reinicie o seu 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 Antivirus Plus 2016** e selecione **Desinstalar**.
4. Clique em **Desinstalar** novamente para confirmar a sua escolha.
5. Clique em **Remover** e, em seguida, selecione **Eu quero removê-lo permanentemente**.
6. Clique em **Seguinte** para continuar.
7. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

13.3. Como desligo automaticamente o meu computador 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 malware. Analisar todo o computador pode levar muito mais tempo a completar dependendo do hardware do seu sistema e da configuração do seu software.

Por essa razão, o Bitdefender permite-lhe configurar o Bitdefender para desligar o computador assim que a análise terminar.

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

Eis como define o Bitdefender para desligar o seu computador no final da análise:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. No módulo **Antivírus**, selecione **Gerir Análises**.
4. Na janela **Gerir Tarefas de Análise**, clique em **Nova tarefa personalizada** para introduzir um nome para a análise e selecione os locais a serem analisados.
5. Se desejar configurar detalhadamente as opções de análise, selecione o separador **Avançado**.
6. Opte por desligar o computador sempre que a análise terminar e se não forem encontradas ameaças.
7. Clique em **OK** para guardar as alterações e fechar a janela.
8. Clique no botão **Iniciar Análise** para verificar o seu sistema.

Se não forem encontradas ameaças, o computador desliga-se.

Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas. Para mais informação, por favor consulte o "*Assistente de Análise Antivírus*" (p. 85).

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

Se o seu computador se ligar a Internet através de um servidor proxy, você 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, siga os seguintes passos:

1. Clique no ícone  na parte superior da interface do Bitdefender e selecione **Definições Gerais** no menu suspenso.
2. Na janela **Definições Gerais** selecione a barra **Avançadas**.
3. Ative a utilização de proxy clicando no botão.
4. Clique na ligação **Gerir proxies**.
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 as definições de proxy dos navegadores mais populares, incluindo as versões mais recentes de Internet Explorer, Mozilla Firefox e Opera.

   - **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.

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

Para saber se tem um sistema operativo de 32 bit ou 64 bit, siga os seguintes passos:

- 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 e Windows 8.1**:
  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.
  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.

13.6. Como posso mostrar objetos ocultos no Windows?

Estes passos são úteis nos casos de malware e 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**.

13.7. Como posso remover outras soluções de segurança?

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

Quando utiliza mais do que uma solução de segurança no mesmo computador, o sistema torna-se instável. O instalador do Bitdefender Antivirus Plus 2016 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, siga os seguintes passos:

- 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 que o processo de desinstalação termine, depois reinicie o seu 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 que o processo de desinstalação termine, depois reinicie o seu 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 nome do programa que pretende remover e selecione **Desinstalar**.
4. Clique em **Desinstalar** novamente para confirmar a sua escolha.
5. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

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

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

Para iniciar o Windows no Modo de Segurança:

1. Reinicie o computador.
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.

GERIR A SUA SEGURANÇA

14. PROTEÇÃO ANTIVÍRUS

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

- Análise no acesso - previne que novas ameaças de malware 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 malware, sendo um componente essencial de qualquer programa informático de segurança.

  Importante
  Para prevenir a infecção de vírus no seu computador, mantenha ativada a **análise no acesso**.

- Análise a-pedido - permite detetar e remover malware que já se encontra a residir no seu 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 média removível que esteja ligado ao computador para garantir um acesso em segurança. Para mais informação, por favor consulte o "*Análise automática de média removíveis*" (p. 89).

Os utilizadores avançados podem configurar as exceções da análise se não quiserem que certos ficheiros ou tipos de ficheiros sejam analisados. Para mais informação, por favor consulte o "*Configurar exceções da análise*" (p. 91).

Quando deteta um vírus ou outro malware, o Bitdefender irá tentar remover automaticamente o código de malware 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, por favor consulte o "*Gerir ficheiros da quarentena*" (p. 93).

Se o seu computador estiver infectado com malware, por favor consulte "*Remover malware do seu sistema*" (p. 145). Para o ajudar a limpar o malware

do computador que não pode ser removido no sistema operativo Windows, o Bitdefender proporciona-lhe o Modo de Recuperação. Este é um ambiente fiável, concebido sobretudo para a remoção de malware, que lhe permite arrancar o seu computador independentemente do Windows. Quando o computador estiver a ser executado no Modo de Recuperação, o malware do Windows está inativo, tornando-se mais fácil a sua remoção.

Para o proteger contra aplicações desconhecidas maliciosas, o Bitdefender utiliza o Controlo Ativo de Ameaças, uma tecnologia heurística avançada, o qual monitoriza continuamente as aplicações executadas no seu sistema. O Controlo Ativo de Ameaças bloqueia automaticamente aplicações que exibem comportamento semelhante a malware para as impedir de danificar o seu computador. Ocasionalmente, as aplicações legítimas podem ser bloqueadas. Em tais situações, pode configurar o Controlo Ativo de Ameaças para não bloquear aquelas aplicações de novo criando regras de exclusão. Para saber mais, por favor consulte "*Controlo Ativo de Ameaças*" (p. 95).

14.1. Análise no acesso (proteção em tempo real)

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

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

14.1.1. Ligar ou desligar a proteção em tempo real

Para ativar ou desativar a proteção em tempo real contra o malware, siga os seguintes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. Clique no módulo **Antivírus**, em seguida, selecione o separador **Escudo**.
4. Clique no botão para ativar ou desativar a análise no acesso.

5. 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 do malware.

14.1.2. Ajustar o nível de proteção em tempo real

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

Para ajustar o nível de proteção em tempo real, siga estes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. Clique no módulo **Antivírus**, em seguida, selecione o separador **Escudo**.
4. Arraste o cursor pela escala para definir o nível de proteção pretendido. Utilize a descrição do lado direito da escala para escolher o nível de proteção que melhor se adequa às suas necessidades de segurança.

14.1.3. Configurar as definições da 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 da proteção em tempo-real, siga os seguintes passos:

1. Clique no ícone no canto inferior direito da interface do Bitdefender.

2. Selecione o separador **Proteção**.
3. Clique no módulo **Antivírus**, em seguida, selecione o separador **Escudo**.
4. Clique em **Personalizar**.
5. Configure as definições de análise como necessário.
6. Clique em **OK** para guardar as alterações e fechar a janela.

Informação sobre as opções de análise

Poderá achar esta informação útil:

- Se não está familiarizado com alguns dos termos, procure-os no glossário. Pode também encontrar informação útil pesquisando a Internet.
- **Opções de análise para ficheiros acedidos.** Pode configurar o Bitdefender para analisar todos os ficheiros ou apenas aplicações (ficheiros de programas) acedidos. A análise de todos os ficheiros acedidos proporciona uma maior segurança, enquanto a análise apenas das aplicações pode ser utilizada para melhorar o desempenho do sistema.

  Por defeito, ambas as pastas locais e partilhas de rede são sujeitas a análise no acesso. Para um melhor desempenho do sistema, pode excluir os locais de rede da análise no acesso.

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

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

- **Analisar dentro dos 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. O malware só pode afetar o seu sistema se o ficheiro infectado for extraído do arquivo e executado sem que a proteção em tempo real esteja ativada.

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

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

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

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

- **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 um vírus infecta o sector de saída, a drive pode tornar-se inacessível ou poderá não conseguir iniciar o seu sistema e aceder aos seus dados.

- **Analisar só ficheiros alterados.** Ao analisar apenas ficheiros novos e modificados, pode melhorar significativamente o desempenho do seu sistema sem comprometer a sua 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.

- **Verificar no arranque do sistema.** Selecionar a opção de análise antecipada no arranque para analisar o seu sistema ao iniciar antes que todos os seus serviços essenciais sejam carregados. A finalidade desta funcionalidade é melhorar a deteção de vírus no arranque do sistema e o tempo de inicialização do sistema.

Ações tomadas em malware detetado

Pode configurar as ações a serem levadas a cabo pela proteção em tempo-real.

Para configurar as ações, siga os seguintes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. Clique no módulo **Antivírus**, em seguida, selecione o separador **Escudo**.
4. Clique em **Personalizar**.
5. Selecione o separador **Ações** e configure as definições de análise conforme necessário.
6. Clique em **OK** para guardar as alterações e fechar a janela.

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 infectados correspondem a uma assinatura de malware na Base de Dados de Assinaturas de Malware do Bitdefender. Bitdefender tentará automaticamente remover o código malware 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, por favor consulte o "*Gerir ficheiros da quarentena*" (p. 93).

Importante
Para determinados tipos de malware, a desinfecção não é possível por o ficheiro detectado 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 malware da Bitdefender. Se a presença de malware for confirmada, é emitida uma assinatura para possibilitar a remoção do malware.

- **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 ficheiros 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, por favor consulte o "*Gerir ficheiros da quarentena*" (p. 93).

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

14.1.4. Restaurar as predefinições

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

Para restaurar as definições da proteção em tempo real, siga os seguintes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. Clique no módulo **Antivírus**, em seguida, selecione o separador **Escudo**.
4. Clique em **Predefinição**.

14.2. Verificação por ordem

O objectivo principal do Bitdefender é manter o seu computador livre de vírus. Isto é feito ao manter os novos vírus fora do seu computador e ao analisar as suas mensagens de e-mail e quaisquer novos ficheiros transferidos ou copiados para o seu sistema.

Há o risco de o vírus já ter acedido ao seu sistema, antes mesmo de ter instalado o Bitdefender. Este é o motivo, pelo qual é uma excelente ideia verificar vírus residentes no seu computador depois de instalar o Bitdefender. E é definitivamente uma boa ideia, analisar frequentemente o seu computador em busca de vírus.

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 computador 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 computador ou configurar as opções de análise, pode configurar e executar uma análise personalizada.

14.2.1. Procurar malware 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.

14.2.2. Executar uma Análise Rápida

A Análise Rápida utiliza a análise nas nuvens para detetar malware em execução no seu sistema. Normalmente, a realização de uma Análise Rápida

demora menos de um minuto e utiliza uma fação dos recursos do sistema necessários para uma análise de vírus normal.

Para executar uma Análise Rápida, siga os seguintes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. No módulo **Antivírus**, selecione **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.

Ou mais rápido, clique no botão **Análise Rápida** da interface do Bitdefender.

14.2.3. Executar uma Análise do Sistema

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

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 usar o seu computador.

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

- Certifique-se de que o Bitdefender apresenta as assinaturas de malware actualizadas. Analisar o seu computador usando assinaturas desactualizadas pode impedir que o Bitdefender detecte novo malware encontrado desde a última actualização. Para mais informação, por favor consulte o "*Mantenha o seu Bitdefender atualizado.*" (p. 43).
- Encerre todos os programas abertos.

Se quer analisar localizações específicas no seu computador ou configurar as opções de análise, pode configurar e executar uma análise personalizada. Para mais informação, por favor consulte o "*Configurar uma análise personalizada*" (p. 82).

Para levar a cabo uma Análise do Sistema, siga os seguintes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. No módulo **Antivírus**, selecione a **Análise do Sistema**.
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.

14.2.4. Configurar uma análise personalizada

Para configurar uma análise ao malware em detalhe e depois executá-la, siga os seguintes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. No módulo **Antivírus**, selecione **Gerir Análises**.
4. Clique em **Nova tarefa personalizada**. Insira um nome para a análise na aba **Básico** e selecione as localizações a serem analisadas.
5. Se desejar configurar detalhadamente as opções de análise, selecione o separador **Avançado**. Aparece uma nova janela. Siga os seguintes passos:
   a. Pode facilmente configurar as opções de análise ajustando o nível de análise. Arraste o cursor pela escala para definir o nível de análise pretendido. Utilize a descrição do lado direito da escala para escolher o nível de análise que melhor se adequa às suas necessidades.

      Os utilizadores avançados podem aproveitar as definições que o Bitdefender oferece. Para configurar as opções de análise em pormenor, clique em **Personalizar**. Pode encontrar informação sobre as mesmas no final desta secção.

   b. Também pode configurar as seguintes opções gerais:

      - **Executar a tarefa com prioridade baixa .** Diminui a prioridade do processo de análise. Irá permitir que outros programas funcionem com maior rapidez e aumenta o tempo necessário para terminar o processo da análise.

- **Minimizar a janela da análise para a área de notificação .** Minimiza a janela da análise para a área de notificação. Faça duplo-clique sobre o ícone Bitdefender para o abrir.
- Especifique a ação a aplicar se não forem encontradas ameaças.

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

6. Se pretender agendar a tarefa de análise, utilize o botão **Agendar** na janela Básica. Selecione uma das opções correspondentes para definir uma agenda:
   - No iniciar do sistema
   - Uma vez
   - Periodicamente
7. Clique em **Iniciar Análise** e siga o assistente de Análise Antivírus para completar a análise. Dependendo das localizações a serem analisadas, a análise pode demorar um pouco. No final da análise, será notificado para escolher as ações que devem ser tomadas nos ficheiros detetados, caso os haja.
8. Se quiser, pode voltar a executar rapidamente uma análise personalizada anterior ao clicar na entrada correspondente na lista disponível.

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.
- **Análise de ficheiros.** Pode configurar o Bitdefender para analisar todos os tipos de ficheiros ou apenas aplicações (ficheiros de programas). A análise de todos os ficheiros proporciona uma maior segurança, enquanto a análise das aplicações só pode ser utilizada numa análise mais rápida.

  As aplicações (ou ficheiros de programa) são muito mais vulneráveis a ataques de malware do que qualquer outro tipo de ficheiros. Esta categoria inclui as seguintes extensões de ficheiro: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar;

js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

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

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

- **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 um vírus infecta o sector de saída, a drive 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 computador.
- **Analisar só ficheiros alterados.** Ao analisar apenas ficheiros novos e modificados, pode melhorar significativamente o desempenho do seu sistema sem comprometer a sua segurança.

- **Ignorar keyloggers comerciais.** Selecione esta opção se tiver instalado e usar programas de controlo e registo comerciais no seu computador. Os programas de controlo e registo comerciais são software legítimo de monitorização do computador cuja função mais básica é registar tudo o que é digitado no teclado.
- **Analisar em busca de rootkits.** Selecione esta opção para analisar rootkits e objetos ocultos usando tal software.

14.2.5. 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.
- **Passar todos os itens protegidos por palavra-passe sem os analisar.** 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 executa uma análise rápida ou uma análise completa ao sistema, o Bitdefender toma automaticamente as ações recomendadas nos ficheiros detetados durante a análise. Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas.

Os objetos infectados são apresentados em grupos, baseados no tipo de malware com que estão infectados. Clique no link correspondente a uma ameaça para descobrir mais informação 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 infectados correspondem a uma assinatura de malware na Base de Dados de Assinaturas de Malware do Bitdefender. Bitdefender tentará automaticamente remover o código malware 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, por favor consulte o "*Gerir ficheiros da quarentena*" (p. 93).

Importante
Para determinados tipos de malware, a desinfecção não é possível por o ficheiro detectado 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 malware da Bitdefender. Se a presença de malware for confirmada, é emitida uma assinatura para possibilitar a remoção do malware.

- **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.

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

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 o malware, por favor consulte "*Remover malware do seu sistema*" (p. 145).

14.2.6. 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 directamente no assistente de análise, assim que esta terminar, clicando em **Mostrar Relatório**.

Para analisar mais tarde um relatório de análise ou qualquer infeção detetada, siga estes passos:

1. Clique no ícone  na parte superior da interface do Bitdefender e selecione **Eventos** no menu suspenso.
2. Na janela **Eventos**, selecione **Antivírus** do menu suspenso correspondente.

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

3. Na lista de eventos, pode ver as análises que foram recentemente efectuadas. Clique no evento para visualizar detalhes sobre o mesmo.
4. Para abrir o relatório da análise, clique em **Ver Relatório**. Caso pretenda realizar a mesma análise novamente, clique no botão **Verificar novamente**.

14.3. Análise automática de média removíveis

O Bitdefender deteta automaticamente quando um dispositivo de armazenamento removível se liga ao computador e analisa-o em segundo plano. Isto é recomendado para prevenir que virus e malware infectem o seu computador.

Os dispositivos detetados encaixam-se numa destas categorias:

- CDs/DVDs
- Dispositivos de armazenamento USB, tais como pens 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.

14.3.1. Como funciona?

Quando deteta dispositivos de armazenamento removíveis, o Bitdefender começa a verificar se existe malware em segundo plano (desde que a análise automática esteja ativada para aquele tipo de dispositivo). Um ícone de análise do Bitdefender irá aparecer no tabuleiro do sistema Pode clicar nesse ícone para abrir a janela da análise e ver o seu progresso.

Se o Piloto Automático estiver ativado, não será incomodado com a análise. A análise será apenas registada e a informação sobre a mesma ficará disponível na janela Eventos.

Se o Piloto Automático estiver desativado:

1. Será notificado através de uma janela de pop-up que um novo dispositivo foi detetado e está a ser analisado.

2. Na maioria dos casos, o Bitdefender remove automaticamente o malware detetado ou isola os ficheiros infectados 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.

3. 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.

Esta informação pode ser útil para si:

- Por favor tenha cuidado ao usar um CD/DVD infectado com malware, porque o malware não pode ser removido do disco (é apenas de leitura). Certifique-se que a proteção em tempo real está ativada para evitar que o malware se propague no seu sistema. Será melhor copiar os dados mais importantes do disco para o seu sistema e depois eliminá-los do disco.
- Em alguns casos, o Bitdefender poderá não conseguir remover o malware 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 como lidar com malware, por favor consulte "*Remover malware do seu sistema*" (p. 145).

14.3.2. Gerir análise de média removível

Para gerir a análise automática dos média removíveis, siga os seguintes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. Clique no módulo **Antivírus**, em seguida, selecione o separador **Exclusões**.

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

As opções de análise estão pré-configuradas para obter os melhores resultados de deteção. Se forem detectados ficheiros infectados, o Bitdefender tentará desinfectá-los (remover o código malware) 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.

14.4. Configurar exceções da 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 usadas por utilizadores com conhecimentos informáticos avançados ou sob as recomendações de um representante da Bitdefender.

Pode configurar as exceções para aplicar apenas na análise no acesso ou a pedido, ou ambos. Os objetos excluídos da análise a-pedido não serão analisados, independentemente de eles serem 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**.

14.4.1. Excluir pastas e ficheiros da análise

Para excluir ficheiros ou pastas específicas da análise, siga os seguintes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. Clique no módulo **Antivírus**.
4. Na janela **Antivírus**, selecione o separador **Exceções**.
5. Ative as exceções para os ficheiros que utilizem o respetivo botão.

6. Clique na ligação **Ficheiros e pastas excluídos**. Na janela que surge, pode gerir os ficheiros e pastas excluídos da análise.
7. Adicionar exceções seguindo estes passos:
   a. Clique no botão **Adicionar** , localizado no cimo da tabela de exceções.
   b. Clique em **Explorar**, selecione o ficheiro ou pasta que deseja excluir da análise e depois clique **OK**. Alternativamente, pode digitar (ou copiar e colar) o caminho para o ficheiro ou pasta no campo editar.
   c. Por defeito, o ficheiro ou pasta é excluída da análise no acesso e a pedido. Para alterar a aplicação da exclusão, selecione uma das outras opções.
   d. Prima **Adicionar**.
8. Clique em **OK** para guardar as alterações e fechar a janela.

14.4.2. 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 computador. A exclusão também se aplica a ficheiros em média removíveis, tais como CDs, DVDs, dispositivos de armazenamento USB ou drives da rede.

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

Para excluir extensões de ficheiros da análise, siga os seguintes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. Clique no módulo **Antivírus**.
4. Na janela **Antivírus**, selecione o separador **Exceções**.
5. Ative as exceções para os ficheiros que utilizem o respetivo botão.
6. Clique na ligação **Extensões excluídas**. Na janela que surge, pode gerir as extensões de ficheiros excluídas da análise.
7. Adicionar exceções seguindo estes passos:

a. Clique no botão **Adicionar** , localizado no cimo da tabela de exceções.

b. Introduza as extensões que deseja excluir da análise, separando-as com ponto e vírgula (;). Eis um exemplo:

txt;avi;jpg

c. Por defeito, todos os ficheiros com as extensões especificadas são excluídas na análise no acesso e a pedido. Para alterar a aplicação da exclusão, selecione uma das outras opções.

d. Prima **Adicionar**.

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

14.4.3. Gerir exceções da análise

Se as exceções de análise configuradas já não forem necessárias, recomenda-se que elimine ou desative as exceções da análise.

Para gerir as exceções da análise, siga os seguintes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. Clique no módulo **Antivírus**, em seguida, selecione o separador **Exclusões**. Use a opções na secção **Ficheiros e pastas** para gerir as exceções de análise.
4. Para remover ou editar exceções da análise, clique numa das ligações disponíveis. Proceder da seguinte forma:
   - Para eliminar um item da lista, selecione-o e clique no botão **Remover**.
   - Para editar uma entrada da lista, clique duas vezes (ou selecione-a e clique no botão **Editar**). Uma nova janela aparece quando muda a extensão ou o caminho a ser excluído e o tipo de verificação que deseja que sejam excluídos, conforme necessário. Faça as alterações necessárias, depois clique em **Modificar**.
5. Para desativar exceções da análise, utilize o respetivo botão.

14.5. Gerir ficheiros da quarentena

O Bitdefender isola os ficheiros infectados com malware que não consegue desinfectar numa área segura denominada quarentena. Quando o vírus se

encontra na quarentena não pode provocar nenhum mal, porque não pode ser nem lido nem executado.

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

Além disso, o Bitdefender analisa os ficheiros em quarentena após cada atualização das assinaturas de malware. Os ficheiros limpos são automaticamente repostos no seu local de origem.

Para verificar e gerir ficheiros da quarentena, siga os seguintes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. Clique no módulo **Antivírus**, em seguida, selecione o separador **Quarentena**.
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 da quarentena de acordo com as suas preferências.

   Analisar quarentena após nova atualização
   Mantenha esta opção ligada para analisar automaticamente os ficheiros da quarentena após cada atualização das definições de vírus. Os ficheiros limpos são automaticamente repostos no seu local de origem.

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

   Apagar conteúdo com mais de {30} dias
   Por defeito, os ficheiros da quarentena com mais de 30 dias são automaticamente eliminados. Se quiser alterar este intervalo, digite um novo valor no campo correspondente. Para desativar a eliminação automática dos antigos ficheiros da quarentena, tipo 0.

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**.

14.6. Controlo Ativo de Ameaças

O Controlo Ativo de Ameaças da Bitdefender é uma tecnologia de deteção proativa inovadora que usa métodos heurísticos para detetar novas e potenciais ameaças em tempo real.

O Controlo Ativo de Ameaças monitoriza as aplicações executados no computador, procurando ações identificáveis como malware. Cada uma destas acções é classificada e é calculada uma pontuação geral para cada processo. Quando a classiificação geral para um processo atinge um dado limite, o processo é considerado perigoso e é bloqueado automaticamente.

Se o Piloto Automático estiver desativado, será notificado através de uma janela de pop-up acerca da aplicação bloqueada. Caso contrário, a aplicação será bloqueada sem qualquer notificação. Pode verificar que aplicações foram detetadas pelo Controlo Ativo de Ameaças na janela Eventos.

14.6.1. Verificar aplicações detetadas

Para verificar as aplicações detetadas pelo Controlo Ativo de Ameaças, siga os seguintes passos:

1. Clique no ícone  na parte superior da interface do Bitdefender e selecione **Eventos** no menu suspenso.
2. Na janela **Eventos**, selecione **Antivírus** do menu suspenso correspondente.
3. Clique no evento para visualizar detalhes sobre o mesmo.
4. Se confiar na aplicação, pode configurar o Controlo Ativo de Ameaças para não a bloquear, clicando em **Permitir e monitorizar**. O Controlo Ativo de Ameaças irá continuar a monitorizar as aplicações excluídas. Se uma aplicação excluída for detectada a realizar actividades suspeitas, o evento será simplesmente registado e comunicado à Nuvem do Bitdefender como uma detecção de erro.

14.6.2. Ligar ou desligar o Controlo Ativo de Ameaças

Para ligar ou desligar o Controlo Ativo de Ameaças, siga os seguintes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. Clique no módulo **Antivírus**.
4. Na janela **Antivírus**, selecione o separador **Escudo**.
5. Clique no botão para ativar ou desativar o Controlo Ativo de Ameaças.

14.6.3. Ajustar a proteção de Controlo Ativo de Ameaças

Se verificar que o Controlo Ativo de Ameaças deteta frequentemente aplicações legítimas, deve definir um nível de proteção inferior.

Para ajustar a proteção do Controlo Ativo de Ameaças, arraste o marcador ao longo da escala para definir o nível de proteção pretendido.

Utilize a descrição do lado direito da escala para escolher o nível de proteção que melhor se adequa às suas necessidades de segurança.

Nota
Quando define um nível de proteção superior, o Controlo Ativo de Ameaças irá necessitar de menos sinais de comportamento malware para comunicar um processo. Isto provocará um aumento do número de aplicações que são comunicadas e, ao mesmo tempo, a um aumento da probabilidade de falsos positivos (aplicações limpas detectadas como maliciosas).

14.6.4. Gerir processos excluídos

Pode configurar as regras de exclusão para aplicações de confiança para que o Controlo Ativo de Ameaças não as bloqueie, se realizarem ações como as do malware. O Controlo Ativo de Ameaças irá continuar a monitorizar as aplicações excluídas. Se uma aplicação excluída for detectada a realizar actividades suspeitas, o evento será simplesmente registado e comunicado à Nuvem do Bitdefender como uma detecção de erro.

Para gerir o processo de exceções do Controlo Ativo de Ameaças, siga os seguintes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. Clique no módulo **Antivírus**, em seguida, selecione o separador **Exclusões**.

4. Clique na hiperligação **Processos Excluídos**. Na janela que aparece, pode gerir as exceções do processo de Controlo Ativo de Ameaças.
5. Adicionar exceções seguindo estes passos:
   a. Clique no botão **Adicionar** , localizado no cimo da tabela de exceções.
   b. Clique em **Explorar**, procure e selecione a aplicação que quer excluir e depois clique em **OK**.
   c. Manter a opção **Permitir** selecionada para evitar que o Controlo Ativo de Ameaças bloqueie a aplicação.
   d. Prima **Adicionar**.
6. Para remover ou editar exceções, proceda da seguinte forma:
   - Para eliminar um item da lista, selecione-o e clique no botão **Apagar**.
   - Para editar uma entrada da lista, clique duas vezes (ou selecione-a) e clique no botão **Modificar**. Faça as alterações necessárias, depois clique em **Modificar**.
7. Guardar as alterações e fechar a janela.

15. PROTEÇÃO DA INTERNET

A Proteção da Internet do Bitdefender garante uma experiência de navegação segura, alertando-o sobre possíveis páginas de phishing.

O Bitdefender fornece proteção da Internet em tempo real para:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

Para configurar as definições de Proteção da Internet, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. Clique no módulo **Proteção da Internet**.

Clique nos botões para ligar ou desligar:

- 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
  - Twitter

- Analisar tráfego web SSL.

Ataques mais sofisticados podem usar tráfego da web seguro para enganar as suas vítimas. É, por isso, recomendado que ative a análise SSL.

- Proteção contra fraudes.
- Proteção contra phishing.

Pode criar uma lista de páginas que não serão analisadas pelos motores antimalware, antiphishing e antifraude do Bitdefender. A lista deve conter apenas os sites web em que confia plenamente. Por exemplo, adicione os websites onde costuma frequentemente fazer compras on-line.

Para configurar e gerir páginas Web utilizando a proteção da Internet fornecida pelo Bitdefender, clique no link **Lista Branca**. Aparece uma nova janela.

Para adicionar um site à lista branca, insira o seu endereço no campo correspondente e depois clique em **Adicionar**.

Para remover um site web desta lista, selecione-o na lista e clique na hiperligação **Remover** correspondente.

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

15.1. Alertas de Bitdefender no navegador

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

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

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

- Navegue para fora da página web clicando em **Leve-me de volta à segurança**.
- Desativar o bloquear de páginas que contenham phishing ao clicar em **Desativar filtro Antiphishing**.
- Desativar o bloquear de páginas que contenham malware ao clicar em **Desativar filtro Antimalware**.
- Adicione a página à lista branca Antiphishing, clicando em **Adicionar à Lista Branca**. Esta página já não será analisada pelos motores Antiphishing do Bitdefender.
- Prosseguir para a página web, apesar do aviso, clicando em **Eu compreendo os riscos, avançar de qualquer forma**.

16. PROTEÇÃO DE DADOS

16.1. 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 computador usando 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. Aparece uma janela de confirmação. Clique em **Sim** para iniciar o assistente do Destruidor de Ficheiros.
4. Aguarde que o Bitdefender termine a destruição dos ficheiros.
5. Os resultados são apresentados. Clique em **Fechar** para sair do assistente.

Alternativamente pode destruir os ficheiros a partir da interface do Bitdefender.

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Privacidade**.
3. No módulo **Proteção de Dados**, selecione **Triturador de Ficheiros**.
4. Siga o assistente do Destruidor de Ficheiros:
   a. **Adicionar Pasta(s)**

      Adicione os ficheiros ou as pastas que pretende remover permanentemente.

   b. Clique em **Seguinte** e confirme que pretende continuar com o processo.

      Aguarde que o Bitdefender termine a destruição dos ficheiros.

   c. **Resultados**

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

17. VULNERABILIDADE

Um passo importante na proteção do seu computador contra as pessoas e aplicações maliciosas é manter atualizado o seu sistema operativo e as aplicações que usa regularmente. Também deve considerar desativar as definições do Windows que tornam o sistema mais vulnerável ao malware. Mais ainda, para evitar acesso físico não-autorizado ao seu computador, palavras-passe fortes (palavras-passe que não são fáceis de adivinhar) devem de ser criadas para cada conta de utilizador do Windows.

O Bitdefender verifica automaticamente o seu sistema por vulnerabilidades e alerta-o sobre eles. As vulnerabilidades do sistema incluem:

- aplicações desatualizada no seu computador.
- actualizações do Windows em falta.
- Senhas fracas para as contas de utilizador do Windows.

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**.
- Se usar a monitorização da vulnerabilidade automática, pode verificar e resolver vulnerabilidades detetadas na janela Eventos.

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

17.1. Procurar vulnerabilidades no seu sistema

Para corrigir as vulnerabilidades do sistema utilizando a opção Análise de Vulnerabilidade, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. No módulo **Vulnerabilidade**, selecione **Análise de Vulnerabilidade**.
4. Aguarde para o Bitdefender analisar as vulnerabilidades do seu sistema. Para interromper o processo de análise, clique no botão **Saltar** na parte superior da janela.

Ou mais rápido, clique no botão de ação **Análise de Vulnerabilidade** da interface do Bitdefender.

- **Atualizações Críticas do Windows**

  Clique em **Ver detalhes** para ver uma lista de atualizações críticas do Windows que não estão instaladas no seu computador.

  Para iniciar a instalação das atualizações selecionadas, clique em **Instalar atualizações**. Note que a instalação das atualizações poderá demorar um pouco e poderá ser necessário reiniciar o sistema para concluir a instalação. Se necessário, reinicie o sistema quando lhe convier.

- **Atualização de aplicações**

  Se a aplicação não estiver atualizada, clique na ligação **Transferir a nova versão** para transferir a versão mais recente.

  Clique em **Ver detalhes** para ver informações sobre a aplicação que necessita de ser atualizada.

- **Palavras-passe fracas de contas do Windows**

  Pode ver a lista dos utilizadores de contas Windows configurados no seu computador e o nível de proteção que as suas palavras-passe garantem.

  Clique em **Alterar palavra-passe ao iniciar sessão** para definir uma nova palavra-passe para o seu sistema.

  Clique em **Ver detalhes** para modificar as palavras-passe fracas. 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 obter uma palavra-passe forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).

No canto superior direito da janela, pode filtrar os resultados de acordo com as suas preferências.

17.2. Usar monitorização de vulnerabilidade automática

O Bitdefender analisa regularmente as vulnerabilidades do seu sistema, em segundo plano, e mantém registos das incidências detetadas na janela Eventos.

Para verificar e resolver os problemas detetados, siga estes passos:

1. Clique no ícone  na parte superior da interface do Bitdefender e selecione **Eventos** no menu suspenso.
2. Na janela **Eventos**, selecione **Vulnerabilidade** da lista Selecionar Eventos.
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 houver alguma atualização do Windows disponível, clique em **Atualizar agora**.
   - 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.

Para configurar as definições de monitorização de vulnerabilidade, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. Clique no módulo **Vulnerabilidade**.

4. Clique no botão para ativar ou desativar a análise de Vulnerabilidade.

> **Importante**
> Para ser notificado automaticamente sobre vulnerabilidades do sistema ou de aplicações, mantenha a opção **Análise de Vulnerabilidade** ativada.

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

Atualizações Críticas do Windows
Verifique se o seu sistema 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 fracas
Verifique se as palavras-passe das 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 @).

Autorun dispositivos media
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 malware usam Autorun para se propagar automaticamente dos média removíveis do PC. Por isso, recomenda-se a desactivação desta janela.

> **Nota**
> Se desativar a monitorização de uma vulnerabilidade específica, as incidências relacionadas deixarão de ser registadas na janela de Eventos.

18. PROTEÇÃO CONTRA RANSOMWARE

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.

A infeção pode espalhar-se através de e-mails de spam, transferência de anexos ou ao visitar sites infetados e instalar aplicações maliciosas sem informar o utilizador sobre o que está a acontecer com o seu sistema.

Ransomwares podem ter um dos seguintes comportamentos, prevenindo que o utilizador aceda ao seu sistema:

- Encriptar dados privados e pessoais sem a possibilidade de desencriptação até que um resgate seja pago pela vítima.
- Bloquear o ecrã do computador e exibir uma mensagem a solicitar dinheiro. Neste caso, nenhum ficheiro é encriptado, mas o utilizador é forçado a realizar o pagamento.
- Bloquear a execução de aplicações.

Utilizando a última tecnologia, a Proteção contra Ransomwares do Bitdefender assegura a integridade do sistema ao proteger áreas essenciais do sistema contra danos, sem prejudicar o desempenho do sistema. No entanto, pode desejar proteger os seus ficheiros pessoais, como documentos, fotos, filmes ou ficheiros que mantém armazenados na nuvem.

18.1. Ativar ou desativar a Proteção contra Ransomwares

Para desativar o módulo de Proteção contra Ransomwares, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. Clique em **Proteção contra Ransomware**.
4. Clique no botão para ativar ou desativar a **Proteção contra Ransomware**.

Sempre que uma aplicação tentar aceder a um ficheiro protegido, um pop-up do Bitdefender será exibido. Pode permitir ou negar o acesso.

18.2. Proteja os seus ficheiros pessoais contra ataques de ransomwares

Caso pretenda armazenar os ficheiros pessoais num alojamento num abrigo, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. Clique no módulo **Proteção contra Ransomware**, en seguida, clique no botão **Pastas protegidas**.
4. Clique em **Adicionar** e, em seguida, procure a pasta que pretenda proteger.
5. Clique em **OK** para adicionar a pasta selecionada ao ambiente de proteção.

As configurações de fábrica já protegem as pastas Documentos, Imagens, Documentos públicos e Imagens públicas contra ataques de malware. Dados pessoais armazenados em serviços online de armazenamento de ficheiros, como Box, Dropbox, Google Drive e OneDrive também são adicionados ao ambiente de proteção, desde que as suas aplicações estejam instaladas no sistema.

Nota
Pastas personalizadas apenas podem ser protegidas para os utilizadores atuais. Ficheiros de sistema e de aplicações não podem ser adicionados às exceções.

18.3. Configurar as aplicações fidedignas

A proteção contra ransomware pode ser desativada para algumas aplicações, mas apenas aquelas em que confia devem ser adicionadas à lista.

Para adicionar aplicações fidedignas às exceções, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. No módulo **Proteção contra Ransomware**, selecione **Aplicações fidedignas**.

4. Clique em **Adicionar** e procure as aplicações que pretenda proteger.
5. Clique em **OK** para adicionar a aplicação selecionada ao ambiente de proteção.

18.4. Configurar as aplicações bloqueadas

Entre as aplicações que instalou no seu computador, algumas podem solicitar aceder aos seus ficheiros pessoais.

Para restringir essas aplicações, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. No módulo **Proteção contra Ransomware**, selecione **Aplicações bloqueadas**.
4. Clique em **Adicionar** e procure as aplicações que pretenda restringir.
5. Clique em **OK** para adicionar a aplicação selecionada à lista de restrições.

18.5. Proteção no arranque

Sabe-se que muitas aplicações de malware são configuradas para serem executados no arranque do sistema, o que pode danificar gravemente a máquina. A Proteção no arranque do Bitdefender verifica todas as áreas essenciais do sistema antes que todos os ficheiros sejam carregados, sem impacto no desempenho do sistema. Simultaneamente, é fornecida proteção contra certos ataques que dependem da execução de códigos em stack ou heap, injeções de código ou ganchos em certas bibliotecas dinâmicas.

Para desativar a Proteção no arranque, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. Clique em **Proteção contra Ransomware**.
4. Clique no botão para ativar ou desativar a **Proteção no arranque**.

19. 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, por favor consulte o *"Proteção do Gestor de palavras-passe para as suas credenciais"* (p. 114).

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 inbuída para ser usada quando o seu computador 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™.

19.1. 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 computador 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 no botão de ação **Safepay** da interface do Bitdefender.
- 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.

> **Nota**
> Se o plug-in do Adobe Flash Player não estiver instalado ou estiver desatualizado, será apresentada um mensagem do Bitdefender. Clique no botão correspondente para continuar.
> Após o processo de instalação, terá que reabrir o navegador Bitdefender Safepay™ manualmente para continuar com o seu trabalho.

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 as informações importantes clicando em .

19.2. Configurar definições

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

Definições

Escolha o que deve de ser feito quando acede a um site online de compras ou de bancos no seu navegador habitual:

- Abrir sites Web automaticamente no Safepay.
- Recomendar-me a utilizar o Safepay.
- Não me recomendar a utilização do Safepay.

Lista de domínios

Escolha como o Bitdefender Safepay™ irá comportar-se quando visitar páginas com domínios específicos no seu navegador adicionando-os à lista de domínios e selecionando o comportamento para cada um deles:

- Abrir automaticamente no Bitdefender Safepay™.
- Que o Bitdefender o avise para a ação a tomar.
- Nunca utilizar o Bitdefender Safepay™ ao visitar uma página do domínio num navegador normal.

A bloquear 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 um site web desta lista, selecione-o na lista e clique na hiperligação **Remover** correspondente.

Permitir proteção de hotspot.

Pode permitir uma proteção extra quando estiver ligado a redes Wi-Fi inseguras ativando esta funcionalidade.

Aceda a *"Proteção Hotspot em redes não-seguras."* (p. 113) para mais informações.

19.3. 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 no ícone ao lado da barra de endereços 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. Inserir o URL e o título do bookmark e 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.

19.4. Proteção Hotspot em redes não-seguras.

Quando utilizar o Bitdefender Safepay™ em redes Wi-fi inseguras (por exemplo, um hotspot público), é oferecida uma proteção extra através da característica Proteção de Hotspot. Este serviço encripta as comunicações Internet em ligações não-seguras, ajudando assim a manter a sua privacidade sem importar a que rede esteja ligado.

A proteção de hotspot funciona apenas se o seu computador estiver ligado a uma rede insegura.

A ligação segura será iniciada e uma mensagem irá aparecer na janela do Bitdefender Safepay™ quando a ligação for estabelecida. O símbolo aparece à frente do URL na barra de endereços para o ajudar a identificar facilmente as ligações seguras.

Para melhorar a sua experiência de navegação, pode escolher ativar os plug-ins do **Adobe Flash** e do **Java** clicando em **Mostrar definições avançadas**.

Pode ser necessário confirmar a ação.

20. PROTEÇÃO DO GESTOR DE PALAVRAS-PASSE PARA AS SUAS CREDENCIAIS

Utilizamos os nossos computadores para efetuar compras online ou pagar as contas, para nos ligarmos a plataformas de comunicação social ou para iniciar sessão em 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 das aplicações
- Palavras-passe das redes Wi-Fi

20.1. Configurar o Gestor de palavras-passe

Após a conclusão da instalação e aquando da abertura do seu navegador, será notificado através de uma janela emergente que pode utilizar a Carteira para uma experiência de navegação mais simples.

A Carteira do Bitdefender é onde pode armazenar os seus dados pessoais.

Clique em **Explorar** para iniciar o assistente de configuração para a Carteira. Siga o assistente para concluir o processo de configuração.

Podem ser executadas duas tarefas adicionais durante este passo:

- Crie uma nova base de dados de Carteira para proteger as suas palavras-passe.

  Durante o processo de configuração, ser-lhe-á solicitada a proteção da sua Carteira com uma palavra-passe principal. A palavra-passe deve ser segura e conter pelo menos 6 carateres.

  Para criar uma palavra-passe segura utilize no mínimo um número ou símbolo e uma maiúscula. Após definir a palavra-passe, se alguém tentar aceder à Carteira terá de inserir primeiro a palavra-passe.

  Após definir a palavra-passe principal, tem a opção de sincronizar as informações na Carteira com a nuvem, para que possa utilizá-las em todos os seus dispositivos.

  No final do processo de configuração, são ativadas por predefinição as seguintes definições da Carteira:

  - **Guardar automaticamente as credenciais na Wallet**.
  - **Solicitar a minha palavra-passe principal quando iniciar sessão no meu computador**.
  - **Bloquear automaticamente a Wallet quando deixar o meu PC sem supervisão**.
- Importe uma base de dados existente caso já tenha utilizado anterior a Carteira no seu sistema.

Exportar a base de dados da Carteira

Para exportar a base de dados da Carteira, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Privacidade**.
3. Clique no módulo **Gestor de palavras-passe**, em seguida, selecione o separador **Carteiras**.
4. Selecione a base de dados da Carteira pretendida na secção **As Minhas Carteiras**, em seguida, clique no botão **Exportar**.
5. Siga os passos para exportar a base de dados da Carteira para uma localização no seu sistema.

Nota
A Carteira precisa de ser aberta para que o botão **Exportar** esteja disponível.

Criar uma nova base de dados Carteira

Para criar uma nova base de dados da Carteira, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Privacidade**.
3. Clique no módulo **Gestor de palavras-passe**, em seguida, selecione o separador **Carteiras**.
4. Clique no ícone + na janela que aparece.
5. Na área **Começar do zero**, clique em **Criar nova**.
6. Digite as informações solicitadas nos campos correspondentes.
   - Etiqueta 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.
   - Escrever novamente a Palavra-passe - volte a escrever a palavra-passe que definiu.
   - Sugestão - escreva uma sugestão para lembrar-se da palavra-passe.
7. Clique em **Continuar**.

8. Nesta etapa, pode escolher armazenar as suas informações na nuvem. Se selecionar Sim, as suas informações bancárias irão permanecer armazenadas localmente no seu dispositivo. Escolha a opção pretendida, em seguida, clique em **Continuar**.
9. Selecione o navegador da Internet de onde deseja importar as credenciais.
10. Clique em **Terminar**.

Sincronize as suas carteiras na nuvem

Para ativar ou desativar a sincronização das carteiras na nuvem, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Privacidade**.
3. Clique no módulo **Gestor de palavras-passe**, em seguida, selecione o separador **Carteiras**.
4. Selecione a base de dados da Carteira pretendida na secção **As Minhas Carteiras**, em seguida, clique no botão **Definições**.
5. Escolha a opção pretendida na janela que aparecer, em seguida, clique em **Guardar**.

Nota
A Carteira precisa de ser aberta para que o botão **Definições** esteja disponível.

Gerir as suas credenciais da Carteira

Para gerir as suas palavras-passe, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Privacidade**.
3. Clique no módulo **Gestor de palavras-passe**, em seguida, selecione o separador **Carteiras**.
4. Selecione a base de dados da Carteira pretendida na secção **As Minhas Carteiras**, em seguida, clique no botão **Abrir**.

Aparece uma nova janela. Selecione a categoria pretendida na parte superior da janela:

- Identidade
- Websites
- 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 da lista, selecione-a e clique no botão **Editar**.
- Para sair, clique em **Cancelar**.
- Para remover uma entrada, selecione-a, clique no botão **Editar** e escolha **Eliminar**.

20.2. Ativar ou desativar a proteção do Gestor de palavras-passe

Para ativar ou desativar a proteção do Gestor de palavras-passe, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Privacidade**.
3. Clique no módulo **Gestor de Palavras-passe**.
4. Clique no botão **Estado do módulo** para ativar ou desativar o Gestor de Palavras-passe.

20.3. Gerir as definições do Gestor de Palavras-passe

Para configurar a palavra-passe principal detalhadamente, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Privacidade**.

3. Clique no módulo **Gestor de palavras-passe**, em seguida, selecione o separador **Definições de segurança**.

Estão disponíveis as seguintes opções:

- **Solicitar a minha palavra-passe principal sempre que eu aceder ao meu PC** - 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.
- **Bloquear automaticamente a Carteira quando deixo o meu PC 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 as aplicações nos quais pretende integrar o Gestor de Palavras-passe, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Privacidade**.
3. Clique no módulo **Gestor de palavras-passe**, em seguida, selecione o separador **Plugins**.

   Marque uma aplicação para utilizar o Gestor de Palavras-passe e melhorar a sua experiência:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Safepay
   - Skype
   - Yahoo! Messenger

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 do **Preenchimento automático**, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Privacidade**.
3. Clique no módulo **Gestor de palavras-passe**, em seguida, selecione o separador **Definições de preenchimento automático**.
4. Configure as seguintes opções:
   - **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.
     - **Deixe-me decidir quando quero preencher automaticamente as minhas credenciais de início de sessão** - pode escolher quando preencher as credenciais automaticamente no navegador.
   - **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.
   - **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.
- Sites Web - abre um submenu com todos os inícios de sessão em sites Web armazenados na Carteira. Clique em **Adicionar sites 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.

21. BITDEFENDER USB IMMUNIZER

A funcionalidade Autorun inbuida no sistema operativo Windows é uma ferramenta bastante útil que permite aos computadores 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 usada pelo malware para iniciar automaticamente e infiltrar no seu computador a partir de dispositivos media graváveis, tais como drives USB flash e cartões de memória ligados através de leitores de cartões. Numerosos ataques Autorun foram criados nestes últimos anos.

Com o Imunizador USB pode evitar que qualquer drive flash formatada em NTFS, FAT32 ou FAT jamais possa automaticamente executar malware. Uma vez que um dispositivo USB esteja imunizado, o malware já não o pode configurar para correr uma certa aplicação quando o dispositivo esteja ligado ao computador em Windows.

Para imunizar um dispositivo USB, siga estes passos:

1. Ligue a drive flash ao seu computador.
2. Explore o seu computador 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 drive já foi imunizada, a mensagem **O dispositivo USB está protegido contra o malware baseado no autorun** aparecerá em vez da opção Imunizar.

Para prevenir que o seu computador execute malware de dispositivos USB não imunizados, desative a funcionalidade de media autorun. Para mais informação, por favor consulte o "*Usar monitorização de vulnerabilidade automática*" (p. 104).

OTIMIZAÇÃO DO SISTEMA

22. 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

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 um perfil é ativado:

- Todos os alertas e pop-ups do Bitdefender são desativados.
- A Atualização Automática é adiada.
- As análises agendadas são adiadas.
- O Consultor de Pesquisa é desativado.
- As ofertas especiais e as notificações do produto estão desativadas.

De acordo com a sua atividade, as seguintes definições do sistema são aplicadas quando um perfil é ativado:

- 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.

22.1. 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 serem tomadas durante o Perfil de Trabalho, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Ferramentas**.
3. Clique no módulo de **Perfis**.
4. Na janela de **Definições do Perfil**, clique no botão **Configurar** na área do Perfil de Trabalho.
5. 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
6. 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**.

Para adicionar aplicações manualmente à Lista de aplicações do Perfil de Trabalho:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Ferramentas**.
3. Clique no módulo **Perfis**, em seguida, clique no botão **Configurar** na área do perfil de Trabalho.
4. Na janela do **Perfil de Trabalho**, clique no link **Lista de aplicações**.
5. Clique em **Adicionar** para adicionar uma nova aplicação à **Lista de aplicações**.

   Aparece uma nova janela. Vá até ao ficheiro executável da aplicação, selecione-o e clique em **OK** para o adicionar à lista.

22.2. 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 no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Ferramentas**.
3. Clique no módulo de **Perfis**.
4. Na janela **Definições dos Perfis**, clique no botão **Configurar** na área do Perfil de Filme.
5. 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

6. 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 Filme ao iniciar uma determinada aplicação de reprodução de vídeo, pode adicionar manualmente a aplicação à **Lista de leitores**.

Para adicionar manualmente leitores de vídeo à Lista de leitores no Perfil de Filme:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Ferramentas**.
3. Clique no módulo **Perfis**, em seguida, clique no botão **Configurar** na área do perfil de Filme.
4. Na janela **Perfil de Filme**, clique no link **Lista de leitores**.
5. Clique em **Adicionar** para adicionar uma nova aplicação à **Lista de leitores**.

   Aparece uma nova janela. Vá até ao ficheiro executável da aplicação, selecione-o e clique em **OK** para o adicionar à lista.

22.3. Perfil de Jogo

Para desfrutar de uma experiência de jogo sem interrupções, é importante reduzir as interrupções 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 durante o Perfil de Jogo, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Ferramentas**.
3. Clique no módulo de **Perfis**.

4. Na janela **Definições dos Perfis**, clique no botão **Configurar** na área do Perfil de Jogo.
5. 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
6. 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 ao iniciar um determinado jogo ou aplicação, pode adicionar a aplicação manualmente à **Lista de jogos**.

Para adicionar jogos manualmente à Lista de jogos no Perfil de Jogo:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Ferramentas**.
3. Clique no módulo **Perfis**, em seguida, clique no botão **Configurar** na área do perfil de Jogos.
4. Na janela **Perfil de Jogo**, clique no link **Lista de jogos**.
5. Clique em **Adicionar** para adicionar um novo jogo à **Lista de jogos**.

   Aparece uma nova janela. Navegue até o ficheiro executável do jogo, selecione-o e clique em **OK** para adicioná-lo à lista.

22.4. Otimização em Tempo Real

A Otimização em Tempo Real do Bitdefender é um plug-in que melhora o desempenho do seu sistema de forma silenciosa, em segundo plano, garantindo que não é 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, siga estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Ferramentas**.
3. Clique no módulo **Perfis**, em seguida, selecione o separador **Definições de Perfis**.
4. Ative ou desative a Otimização em Tempo Real automática clicando no botão correspondente.

SOLUÇÃO DE PROBLEMAS

23. 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.

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. 155).

23.1. 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 todos os outros programas antivírus utilizados antes de instalar o Bitdefender. Para

mais informação, por favor consulte o "*Como posso remover outras soluções de segurança?*" (p. 69).

- **Não estão cumpridos os Requisitos Mínimos do Sistema para executar o Bitdefender.**

  Se o seu computador não cumprir os Requisitos Mínimos do Sistema, ficará lento, especialmente se estiver a executar muitas aplicações ao mesmo tempo. Para mais informação, por favor consulte o "*Requisitos mínimos do sistema*" (p. 3).

- **Instalou aplicações que não utiliza**.

  Algum computador possui 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 afectados pelo malware. Spyware, viruses, Trojans e adware prejudicam o desempenho do seu sistema. 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 malware que ameaçam a segurança do seu sistema.

  Para iniciar a Análise do Sistema, siga estes passos:

  1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
  2. Selecione o separador **Proteção**.
  3. No módulo **Antivírus**, selecione a **Análise do Sistema**.
  4. Siga os passos do assistente.

23.2. 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, siga os seguintes passos:

  1. Remover o Bitdefender totalmente do 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 Antivirus Plus 2016** e selecione **Desinstalar**.
       c. Clique em **Remover** na janela que aparece e, em seguida, selecione **Eu quero reinstalá-lo**.
       d. Clique em **Seguinte** para continuar.
       e. Aguarde que o processo de desinstalação termine, depois reinicie o seu 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 Antivirus Plus 2016** e selecione **Desinstalar**.
       d. Clique em **Remover** na janela que aparece e, em seguida, selecione **Eu quero reinstalá-lo**.
       e. Clique em **Seguinte** para continuar.
       f. Aguarde que o processo de desinstalação termine, depois reinicie o seu 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 Antivirus Plus 2016** e selecione **Desinstalar**.

d. Clique em **Desinstalar** novamente para confirmar a sua escolha.

e. Clique em **Remover** na janela que aparece e, em seguida, selecione **Eu quero reinstalá-lo**.

f. Clique em **Seguinte** para continuar.

g. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

2. Reinstale o seu produto Bitdefender

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

  Neste caso, siga os seguintes passos:

  1. Remover a outra solução de segurança. Para mais informação, por favor consulte o "*Como posso remover outras soluções de segurança?*" (p. 69).
  2. Remover o Bitdefender totalmente do 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 Antivirus Plus 2016** e selecione **Desinstalar**.

       c. Clique em **Remover** na janela que aparece e, em seguida, selecione **Eu quero reinstalá-lo**.

       d. Clique em **Seguinte** para continuar.

       e. Aguarde que o processo de desinstalação termine, depois reinicie o seu 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 Antivirus Plus 2016** e selecione **Desinstalar**.

d. Clique em **Remover** na janela que aparece e, em seguida, selecione **Eu quero reinstalá-lo**.

e. Clique em **Seguinte** para continuar.

f. Aguarde que o processo de desinstalação termine, depois reinicie o seu 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 Antivirus Plus 2016** e selecione **Desinstalar**.

d. Clique em **Desinstalar** novamente para confirmar a sua escolha.

e. Clique em **Remover** na janela que aparece e, em seguida, selecione **Eu quero reinstalá-lo**.

f. Clique em **Seguinte** para continuar.

g. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

3. Reinstale o seu produto Bitdefender

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 155).

23.3. Já não consigo usar 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 Controlo Ativo de Ameaças deteta erradamente algumas aplicações como maliciosas.

O Controlo Ativo de Ameaças é um módulo do Bitdefender que monitoriza constantemente as aplicações executadas no seu sistema e denuncia o comportamento potencialmente malicioso. Como este recurso é baseado num sistema heurístico, poderá haver casos em que as aplicações legítimas são denunciadas pelo Controlo Ativo de Ameaças.

Quando esta situação ocorrer, poderá excluir a respetiva aplicação da monitorização do Controlo Ativo de Ameaças.

Para adicionar o programa à lista de exceções, siga os seguintes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. Clique no módulo **Antivírus**, em seguida, selecione o separador **Exclusões**.
4. Clique na hiperligação **Processos Excluídos**. Na janela que aparece, pode gerir as exceções do processo de Controlo Ativo de Ameaças.
5. Adicionar exceções seguindo estes passos:
   a. Clique no botão **Adicionar** , localizado no cimo da tabela de exceções.
   b. Clique em **Explorar**, procure e selecione a aplicação que quer excluir e depois clique em **OK**.
   c. Manter a opção **Permitir** selecionada para evitar que o Controlo Ativo de Ameaças bloqueie a aplicação.
   d. Prima **Adicionar**.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 155).

23.4. O que fazer quando o Bitdefender bloqueia um site Web ou uma 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 Web ou uma aplicação online segura como insegura, o que fará com que a análise do tráfego de HTTP do Bitdefender bloqueie-os incorretamente.

Se a mesma página ou aplicação for bloqueada repetidamente, estes podem ser adicionados a uma lista branca para que não sejam analisados pelos

mecanismos do Bitdefender, o qeu assegura uma experiência de navegação Web normal.

Para adicionar um site Web na **Lista branca**, sigas estes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. Clique no módulo **Proteção da Internet**.
4. No separador **Definições**, clique na hiperligação **Lista branca**.
5. Forneça o endereço do site Web ou da aplicação online bloqueada no campo correspondente e clique em **Adicionar**.
6. Clique em **Guardar** para guardar as alterações e fechar a janela.

Apenas os sites Web e as aplicações em que confia totalmente devem ser adicionados a esta lista. Estes irão ser excluídos da análise pelos seguintes mecanismos: malware, phishing e fraude.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 155).

23.5. Como atualizar o Bitdefender numa ligação à Internet lenta

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

Para manter o seu sistema atualizado com as mais recentes assinaturas de malware Bitdefender, siga os seguintes passos:

1. Clique no ícone  na parte superior da interface do Bitdefender e selecione **Definições Gerais** no menu suspenso.
2. Na janela de **Definições Gerais**, selecione o separador **Atualizar**.
3. Ao lado do **Atualizar as regras de processamento**, selecione **Exibir antes de transferir** do menu suspenso.
4. Volte à janela principal e clique no botão de ação **Atualizar** na interface do Bitdefender.
5. Selecione apenas **Atualizações das assinaturas** e clique em **OK**.

6. O Bitdefender vai transferir e instalar apenas as atualizações das assinaturas de malware.

23.6. O Meu Computador não está ligado à Internet. Como posso actualizar o Bitdefender?

Se o seu computador não estiver ligado à Internet, tem de transferir manualmente as atualizações para um computador com acesso à Internet e, depois, transferi-las para o seu computador com um dispositivo amovível, por exemplo, um USB.

Siga os seguintes passos:

1. Num computador com acesso à Internet, abra o navegador da Internet e vá a:

   http://www.bitdefender.pt/site/view/Desktop-Products-Updates.html

2. Na coluna **Atualização Manual**, clique na hiperligação que corresponde ao seu produto e à arquitectura do sistema. Se não sabe se a versão do seu Windows é de 32 ou 64 bits, consulte "*Estou a utilizar uma versão de 32 ou 64 Bit do Windows?*" (p. 68).
3. Guarde o ficheiro com o nome weekly.exe no sistema.
4. Mova o ficheiro transferido para um dispositivo amovível, tal como uma unidade USB, e depois para o seu computador.
5. Faça duplo clique no ficheiro e siga os passos do assistente.

23.7. 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 computador, 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 computador e aguarde alguns momentos até o Bitdefender iniciar. Abra o Bitdefender e veja se o erro se mantém. Reiniciar o computador 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, por favor consulte o "*Como posso remover outras soluções de segurança?*" (p. 69).

Se o erro persistir, por favor contacte os nossos representantes do suporte conforme descrito na secção "*Pedir Ajuda*" (p. 155).

23.8. A funcionalidade Preenchimento automático na minha Carteira não funciona

Guardou as suas credenciais online na Carteira do Bitdefender e constatou que o preenchimento automático não está a funcionar. Normalmente, este problema surge quando a extensão do Gestor de Palavras-passe do Bitdefender não está instalada no seu navegador.

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. Selecione o **Bitdefender Gestor de Palavras-passe** e clique em Ativar.
- No **Mozilla Firefox:**
  1. Abra o Mozilla Firefox.

2. Clique em Ferramentas.
3. Clique em Suplementos.
4. Clique em Extensões.
5. Selecione o **Bitdefender Gestor de Palavras-passe** e clique em Ativar.

- No **Google Chrome:**
  1. Abra o Google Chrome.
  2. Aceda ao ícone Menu.
  3. Clique em Definições.
  4. Clique em Extensões.
  5. Selecione o **Bitdefender Gestor de Palavras-passe** e clique em Ativar.

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. 155).

23.9. 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 completamente Bitdefender do seu sistema, siga 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 Antivirus Plus 2016** e selecione **Desinstalar**.

3. Clique em **Remover** e, em seguida, selecione **Eu quero removê-lo permanentemente**.
4. Clique em **Seguinte** para continuar.
5. Aguarde que o processo de desinstalação termine, depois reinicie o seu 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 Antivirus Plus 2016** e selecione **Desinstalar**.
4. Clique em **Remover** e, em seguida, selecione **Eu quero removê-lo permanentemente**.
5. Clique em **Seguinte** para continuar.
6. Aguarde que o processo de desinstalação termine, depois reinicie o seu 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 Antivirus Plus 2016** e selecione **Desinstalar**.
4. Clique em **Desinstalar** novamente para confirmar a sua escolha.
5. Clique em **Remover** e, em seguida, selecione **Eu quero removê-lo permanentemente**.
6. Clique em **Seguinte** para continuar.
7. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

23.10. 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, siga estes passos:

  1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como fazer isto, consulte "*Como posso reiniciar no Modo de Segurança?*" (p. 71).
  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 Antivirus Plus 2016** e selecione **Desinstalar**.
       c. Clique em **Remover** na janela que aparece e, em seguida, selecione **Eu quero reinstalá-lo**.
       d. Clique em **Seguinte** para continuar.
       e. Aguarde até que o processo de desinstalação seja concluído.
       f. 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 Antivirus Plus 2016** e selecione **Desinstalar**.

d. Clique em **Remover** na janela que aparece e, em seguida, selecione **Eu quero reinstalá-lo**.

e. Clique em **Seguinte** para continuar.

f. Aguarde até que o processo de desinstalação seja concluído.

g. 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 Antivirus Plus 2016** e selecione **Desinstalar**.

d. Clique em **Desinstalar** novamente para confirmar a sua escolha.

e. Clique em **Remover** na janela que aparece e, em seguida, selecione **Eu quero reinstalá-lo**.

f. Clique em **Seguinte** para continuar.

g. Aguarde até que o processo de desinstalação seja concluído.

h. 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, siga estes passos:

1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como fazer isto, consulte "*Como posso reiniciar no Modo de Segurança?*" (p. 71).

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 que o processo de desinstalação termine, depois reinicie o seu 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 que o processo de desinstalação termine, depois reinicie o seu 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 que o processo de desinstalação termine, depois reinicie o seu 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, siga estes passos:

1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como fazer isto, consulte "*Como posso reiniciar no Modo de Segurança?*" (p. 71).
2. Usar a opção de Restauro do Sistema do Windows para restaurar o computador para uma data anterior antes de instalar o produto Bitdefender.
3. Reinicie o sistema no modo normal e contacte os nossos representantes do suporte conforme descrito na secção "*Pedir Ajuda*" (p. 155).

24. REMOVER MALWARE DO SEU SISTEMA

O malware pode afetar o seu sistema de várias formas e a atuação do Bitdefender depende do tipo de ataque por malware. Como os vírus alteram frequentemente o modo de ação, é difícil estabelecer um padrão com base no comportamento e nas ações.

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

- "*Modo de Recuperação Bitdefender*" (p. 145)
- "*O que fazer se o Bitdefender encontrar vírus no seu computador?*" (p. 147)
- "*Como posso limpar um vírus num ficheiro?*" (p. 149)
- "*Como posso limpar um vírus num ficheiro do email?*" (p. 150)
- "*O que fazer se suspeitar que um ficheiro é perigoso?*" (p. 151)
- "*O que são os ficheiros protegidos por palavra-passe no relatório de análise?*" (p. 152)
- "*O que são os itens ignorados no relatório de análise?*" (p. 152)
- "*O que são os ficheiros muito comprimidos no relatório de análise?*" (p. 152)
- "*Por que é que Bitdefender eliminou automaticamente um ficheiro infectado?*" (p. 153)

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. 155).

24.1. Modo de Recuperação Bitdefender

Modo do Recuperação é uma característica do Bitdefender que lhe permite analisar e desinfectar todas as partições do disco rígido existentes fora do seu sistema operativo.

Depois de instalar o Bitdefender Antivirus Plus 2016, o Modo de Recuperação pode ser usado mesmo que já não consiga arrancar no Windows.

Iniciar o seu sistema no Modo de Recuperação

Pode entrar no Modo de Recuperação de duas formas:

A partir da interface do Bitdefender

Para entrar no Modo de Recuperação diretamente a partir do Bitdefender, siga os seguintes passos:

1. Clique no ícone  no canto inferior direito da interface do Bitdefender.
2. Selecione o separador **Proteção**.
3. No módulo **Antivírus**, selecione **Modo de Recuperação**.

   Aparece uma janela de confirmação. Clique **Sim** para reiniciar o seu computador.
4. Depois do computador reiniciar, aparecerá um menu que o notifica para escolher um sistema operativo. Escolha **Modo de Recuperação do Bitdefender** e prima **Enter** para iniciar no ambiente do Bitdefender, de onde pode limpar a sua partição do Windows.
5. Se notificado, prima **Enter** e selecione a resolução do ecrã mais aproximada daquela que normalmente usa. Depois prima de novo **Enter**.

   O Modo de Recuperação do Bitdefender irá carregar dentro de momentos.

Arranque o seu computador diretamente no Modo de Recuperação

Se o Windows já não iniciar, pode arrancar o seu computador diretamente no Modo de Recuperação do Bitdefender, seguindo os passos abaixo:

1. Inicie / reinicie o seu computador e comece a premir a tecla **espaços** do seu teclado antes de aparecer o logo do Windows.
2. Um menu surge notificando-o para selecionar um sistema operativo para iniciar. Prima **TAB** para ir para a área das ferramentas. Escolha **Imagem de Recuperação Bitdefender** e prima a tecla **Enter** arrancar num ambiente do Bitdefender
3. Se notificado, prima **Enter** e selecione a resolução do ecrã mais aproximada daquela que normalmente usa. Depois prima de novo **Enter**.

O Modo de Recuperação do Bitdefender irá carregar dentro de momentos.

Analisar o seu sistema no Modo de Recuperação

Para analisar o seu sistema no Modo de Recuperação, siga os seguintes passos:

1. Entre no Modo de Recuperação, conforme descrito em "Iniciar o seu sistema no Modo de Recuperação" (p. 146).
2. O logo do Bitdefender surgirá e os motores antivírus começarão a ser copiados.
3. Uma janela de boas-vindas aparece. Clique em **Continuar**.
4. Iniciou-se uma atualização de assinaturas antivirus.
5. Quando a atualização estiver concluída, a janela da Análise-a-pedido do Bitdefender irá aparecer.
6. Clique em **Analisar Agora**, selecione o alvo da análise na janela que surge e clique em **Abrir** para iniciar a análise.

   Recomenda-se que analise toda a partição do Windows.

   > **Nota**
   > Ao trabalhar no Modo de Recuperação, lida com nomes de partições do tipo do Linux. As partições do disco surgirão como sda1 provavelmente correspondendo à (C:) partição do Windows, sda2 correspondendo a (D:) e assim sucessivamente.

7. Aguarde que a análise termine. Se for detectado algum malware, siga as instruções para remover a ameaça.
8. Para sair do Modo de Recuperação, clique com o botão direito do rato numa área vazia do ambiente de trabalho, selecione **Sair** no menu que aparece e depois escolha entre reiniciar ou encerrar o computador.

24.2. O que fazer se o Bitdefender encontrar vírus no seu computador?

Pode verificar se há um vírus no seu computador de uma das seguintes formas:

- O Bitdefender analisou o seu computador e encontrou itens infectados.
- Um alerta de vírus avisa que o Bitdefender bloqueou um ou vários vírus no seu computador.

Nestas situações, atualize o Bitdefender para se certificar que possui as assinaturas de malware mais recentes e realize uma Análise de Sistema.

Assim que a análise 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 no ícone  no canto inferior direito da interface do Bitdefender.
   b. Selecione o separador **Proteção**.
   c. Clique no módulo **Antivírus**, em seguida, selecione o separador **Escudo**.
   d. Clique no botão para desligar **Análise no-acesso**.
2. Mostrar objetos ocultos no Windows. Para saber como fazer isto, consulte "*Como posso mostrar objetos ocultos no Windows?*" (p. 68).
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.

No caso de o primeiro método falhar ao remover a infecção, siga os seguintes passos:

1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como fazer isto, consulte "*Como posso reiniciar no Modo de Segurança?*" (p. 71).

2. Mostrar objetos ocultos no Windows. Para saber como fazer isto, consulte "*Como posso mostrar objetos ocultos no Windows?*" (p. 68).
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. 155).

24.3. Como posso limpar um vírus 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 vírus no interior, mas não pode aplicar outras ações.

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

Pode limpar um vírus armazenado num arquivo da seguinte forma:

1. Identifique o ficheiro que contém o vírus realizando uma Análise Completa ao sistema.
2. Desative a proteção antivírus em tempo real do Bitdefender:
   a. Clique no ícone  no canto inferior direito da interface do Bitdefender.
   b. Selecione o separador **Proteção**.
   c. Clique no módulo **Antivírus**, em seguida, selecione o separador **Escudo**.
   d. Clique no botão para desligar **Análise no-acesso**.
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 completa ao sistema para se certificar que não há outras infecções no sistema.

Nota
É importante saber que um vírus armazenado num arquivo não é uma ameaça imediata ao seu sistema pois o vírus tem de ser descomprimido e executado de modo a infectar o seu sistema.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 155).

24.4. Como posso limpar um vírus num ficheiro do email?

O Bitdefender também pode identificar vírus 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.

Pode limpar um vírus armazenado num arquivo de correio eletrónico da seguinte forma:

1. Analisar a base de dados do correio eletrónico com o Bitdefender.
2. Desative a proteção antivírus em tempo real do Bitdefender:
   a. Clique no ícone  no canto inferior direito da interface do Bitdefender.
   b. Selecione o separador **Proteção**.
   c. Clique no módulo **Antivírus**, em seguida, selecione o separador **Escudo**.
   d. Clique no botão para desligar **Análise no-acesso**.
3. Abra o relatório da análise e utilize a informação de identificação (Assunto, De, Para) das mensagens infectadas para localizá-las no cliente de correio 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 Outlook Express: No menu Ficheiro, clique em Pasta e, depois em Compactar Todas as Pastas.
   - 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: 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. 155).

24.5. 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 se certificar de que o seu sistema está protegido, siga estes passos:

1. Execute uma **Análise de Sistema** com o Bitdefender. Para saber como fazer isto, consulte "*Como posso analisar o seu sistema?*" (p. 58).
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 fazer isto, consulte "*Pedir Ajuda*" (p. 155).

24.6. 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 estes conteúdos pudessem ser extraídos, o verificador em tempo real do Bitdefender analisaria-os automaticamente para manter o seu computador protegido. Se pretende analisar esses 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.

24.7. 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.

24.8. 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.

24.9. 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 malware, a desinfecção não é possível por o ficheiro detectado 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.

CONTACTE-NOS

25. 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. 131) 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:

- "Contacte-nos diretamente do seu produto Bitdefender" (p. 155)
- "Contacte-nos através do nosso Centro de Suporte Online" (p. 156)

Contacte-nos diretamente do seu produto Bitdefender

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 no ícone  na parte superior da interface do Bitdefender e selecione **Ajuda e Suporte** no menu suspenso.
2. Tem as seguintes opções:
   - **Documentação do Produto**

     Aceda à nossa base de dados e procure a informação necessária.
   - **Contato de Suporte**

     Utilize o botão **Contatar Suporte** para executar a Ferramenta de Suporte do Bitdefender e contatar o Departamento de Apoio ao Cliente. Pode navegar pelo assistente utilizando o botão **Seguinte**. Para sair do assistente, clique em **Cancelar**.

     a. Selecione a caixa de verificação para indicar aceitação e clique em **Seguinte**.

     b. Complete o formulário de envio com os dados necessários:

i. Insira o seu endereço de email.

ii. Digite o seu nome completo.

iii. Introduza a descrição do problema que encontrou.

iv. Marque a opção **Tentar reproduzir a incidência antes de enviar** caso esteja a encontrar uma incidência do produto. Continue com os passos necessários.

c. Por favor, aguarde alguns minutos enquanto o Bitdefender recolhe as informações relacionadas com o produto. Esta informação irá ajudar os nossos engenheiros a encontrar uma solução para o seu problema.

d. Clique em **Concluir** para enviar as informações ao Departamento de Apoio ao Cliente da Bitdefender. Será contactado assim que possível.

Contacte-nos através do nosso Centro de Suporte Online

Se não conseguir aceder às informações necessárias com o produto Bitdefender, por favor consulte o nosso Centro de Suporte online:

1. Vá para http://www.bitdefender.pt/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

   http://www.bitdefender.pt/support/contact-us.htmle contate os nossos representantes do suporte.

26. 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:

  http://www.bitdefender.pt/support/consumer.html

- Fórum de Suporte Bitdefender:

  http://forum.bitdefender.com

- o portal de segurança informática HOTforSecurity:

  http://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.

26.1. 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 d vírus, a gestao 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

http://www.bitdefender.pt/support/consumer.html.

26.2. 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 certos vírus do seu computador ou se tiver alguma questão sobre a forma como opera, coloque o seu problema ou a sua questão no fórum.

Os técnicos de 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, por favor pesquise o fórum por um tópico semelhante ou relacionado.

O Fórum de Suporte do Bitdefender está disponível em http://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.

26.3. 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 http://www.hotforsecurity.com.

27. INFORMAÇÕES DE CONTATO

Comunicação eficiente é a chave de um negócio bem-sucedido. Durante os últimos 10 anos a BITDEFENDER estabeleceu uma reputação indiscutível ao exceder as expectativas dos clientes e parceiros, ao procurar constantemente melhorar a comunicação. Por favor não hesite em contactar-nos acerca de qualquer questão ou assunto que nos queira colocar.

27.1. Endereços Web

Departamento Comercial: comercial@bitdefender.pt
Centro de Suporte:http://www.bitdefender.pt/support/consumer.html
Documentação: documentation@bitdefender.com
Distribuidores locais:http://www.bitdefender.pt/partners
Programa de parcerias: partners@bitdefender.com
Relações com os media: pr@bitdefender.com
Carreiras: jobs@bitdefender.com
Submeter Vírus: virus_submission@bitdefender.com
Submeter Spam: spam_submission@bitdefender.com
Relatórios de Abusos: abuse@bitdefender.com
Site Web:http://www.bitdefender.pt

27.2. 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 http://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. Por favor, escreva a sua mensagem em inglês para podermos responder imediatamente.

27.3. 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: http://www.bitdefender.com/support/consumer.html
Web: http://www.bitdefender.com

Alemanha

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Escritório: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Vendas: vertrieb@bitdefender.de
Suporte Técnico: http://www.bitdefender.de/support/consumer.html
Web: http://www.bitdefender.de

Espanha

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Tel: +34 902 19 07 65
Vendas: comercial@bitdefender.es
Suporte Técnico: http://www.bitdefender.es/support/consumer.html
Site: http://www.bitdefender.es

Roménia

BITDEFENDER SRL
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
Bucharest

Fax: +40 21 2641799
Telefone Comercial: +40 21 2063470
E-mail Vendas: sales@bitdefender.ro
Suporte Técnico: http://www.bitdefender.ro/support/consumer.html
Site: http://www.bitdefender.ro

United Arab Emirates

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Telefone Comercial: 00971-4-4588935 / 00971-4-4589186
E-mail Vendas: mena-sales@bitdefender.com
Suporte Técnico: http://www.bitdefender.com/support/consumer.html
Site: http://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 persistente avançada

A ameaça persistente avançada (APA) explora as vulnerabilidades dos sistemas para roubar informações importantes e fornecê-las à fonte. Grandes grupos como organizações, empresas ou governos são os alvos deste malware.

O objetivo de uma ameaça persistente avançada é permanecer não 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 o vírus 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.

Assinatura de Vírus

A patente binária de um vírus, usada pelo programa de anti-vírus para detetar e eliminar os vírus.

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 o seu próprio modulo de atualização que lhe permite verificar atualizações manualmente, ou permitir atualizar o produto automaticamente.

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.

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.

E-mail
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.

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 íncluem ".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 novos vírus. Este método de análise não se baseia em assinaturas específicas de vírus.

A vantagem da análise heurística, é que não se deixa enganar por uma nova variante de um vírus 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 que abra no ínicio, um ficheiro de som a ser tocado quando ligar inicialmente o computador, um lembrete, ou programas de aplicação podem ser itens que começam a funcionar ao iniciar o computador. 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 vírus 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.

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 análise depende da assinaturas de vírus especificas. A vantagem de uma análise não-heurística, é que ela não será induzido em erro pelo que possa parecer um vírus e não gera falsos alarmes.

Navegador

É um software de aplicação usado 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 a um utilizador como sendo falsamente uma empresa legítima e estabelecida numa tentativa de levar o utilizador a providenciar informação privada que será utilizada para roubo. O e-mail leva o utilizador a visitar um site na Internet onde lhe é solicitado que actualize informação pessoal, tal como palavras-passe e números de cartões de crédito, segurança social, e números de contas bancárias, que a legítima organização 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, desenhado para minimizar o impacto da proteção antivírus no desempenho. 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.

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.

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, eles são essencialmente utilizados para ocultar malware ou para esconder a presença de um intruso no sistema. Quando combinados com o malware, os rootkits são uma grande ameaça à integridade e segurança de um sistema. Eles podem monitorizar tráfego, criar backdoors no sistema, alterar ficheiros e relatórios e evitarem ser detetados.

Sector de arranque:

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.

Spam

Lixo de correio electrónico ou lixo de avisos de newsgroups. É normalmente conhecido como correio 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 reunir informação acerca de endereços de e-mail e até mesmo palavras-passe e números de cartões de crédito.

O spyware é similar a um 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 dos vírus, os cavalos de Tróia não se replicam, mas podem ser tão destrutivos como os vírus. Um dos cavalos de Tróia mais insidiosos é o programa que promete ver-se livre dos vírus do seu computador, mas em vez disso introduz vírus 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.

Utilização de 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.

Vírus

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 dos vírus podem-se replicar. Todos os vírus de computação são feitos pelo Homem. Um simples vírus que se possa reproduzir a si próprio vezes sem conta, é relativamente fácil de fabricar. Mesmo um simples vírus é perigoso, porque usará rapidamente toda a memória disponível e levará o sistema a uma quebra. Um tipo de vírus ainda mais perigoso é aquele que é capaz de se transmitir ao longo das redes e ultrapassar sistemas de segurança.

Vírus de saída

Um vírus que infecta o sector boot de um disco fixo ou de uma unidade de disquetes. A tentativa de arrancar por uma disquete infectada por um vírus de boot, irá causar a activação do vírus em memória. Sempre que iniciar o seu sistema a partir daquele ponto, terá o vírus activo em memória.

Vírus polimórfico

Um vírus que altera a sua forma a cada ficheiro que infecta. Dado que eles não têm uma padrão de patente binária consistente, tais vírus são difíceis de identificar.