ANTIVIRUS PLUS 2012

Guia de usuário

Bitdefender Antivirus Plus 2012
Guia de usuário

Data de Publicação 2011.10.06

Aviso Legal


Bitdefender

Índice

1. Instalação

1.1. Preparar a instalação

Antes de instalar o Bitdefender Antivírus 2010, complete estes preparativos para assegurar que a instalação irá ocorrer suavemente:

- Assegure-se que o computador onde deseja instalar o Bitdefender tenha os requisitos mínimos de sistema.Se o computador não encontrar todos os requisitos mínimos do sistema, o Bitdefender não será instalado ou se instalado, não irá trabalhar de forma apropriada e irá causar lentidão e instabilidade.Para uma lista completa de requisitos de sistema, por favor consulte em *"Requisitos de Sistema" (p. 1)*.
- Efetue logon no computador utilizando uma conta de Administrador.
- Remova qualquer outro software similar do seu computador.Rodar dois programas de segurança simultaneamente pode afetar o funcionamento deles e causar maiores problemas ao sistema.O Windows Defender será desativado durante a instalação.
- Recomenda-se que o seu computador esteja conectado à Internet durante a instalação, mesmo quando realizar a instalação a partir de um CD/DVD.Se estiverem disponíveis versões dos arquivos de aplicativos mais recentes do que as incluídas no pacote de instalação, o Bitdefender irá fazer o download e instalá-las.

1.2. Requisitos de Sistema

Você pode instalar o Bitdefender Antivirus Plus 2012 apenas nos computadores com os seguintes sistemas operacionais:

- Windows XP com o Service Pack 3 (32 bits)
- Windows Vista com o Service Pack 2
- Windows 7 com o Service Pack 1

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

Nota

Para saber qual é o sistema operacional que seu computador contém ea informação de hardware do mesmo, clique com o botão direito domouse no ícone **Meu Computador** no Ambiente de Trabalho e depois selecione **Propriedades** do menu.

1.2.1. Requisitos mínimos do sistema

- 1.8 GB de espaço disponível no disco rígido (pelo menos 800 MB na unidade do sistema)

- Processador de 800 MHz
- 1 GB de memória (RAM)

1.2.2. Requisitos de sistema recomendados

- 2.8 GB de espaço disponível no disco rígido (pelo menos 800 MB na unidade do sistema)
- Intel CORE Duo (1.66 GHz) ou processador equivalente
- Memória (RAM)
  - 1 GB para o Windows XP
  - 1.5 GB para o Windows Vista e Windows 7

1.2.3. Requisitos de Software

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

- Internet Explorer 7 ou superior
- Mozilla Firefox 3.6 ou superior
- Yahoo Messenger 8.1 ou superior
- .Net framework 3

1.3. Instalação do seu produto Bitdefender

Você pode instalar o Bitdefender de um CD de instalação Bitdefender ou usando um arquivo baixado do site do Bitdefender ou de sites autorizados. (Por exemplo, o site de um parceiro do Bitdefender ou uma loja online).Você pode fazer o download do arquivo de instalação do site da Bitdefender no endereço a seguir: http://www.bitdefender.com/site/Downloads/.

- Para instalar o Bitdefender a partir do disco de instalação, insira o disco na unidade ótica.A tela de boas-vindas será exibida em instantes. Siga as instruções para iniciar a instalação.

  Nota

  A tela de boas-vindas 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 você precisar instalar o Bitdefender em um computador que não possui uma unidade de disco (por exemplo, em um netbook).Insira o dispositivo no drive USB e então clique **Cópia para USB**.Depois, vá para o computador sem a unidade de disco, insira o dispositivo de armazenamento na unidade USB e clique duas vezes `runsetup.exe` na pasta onde você salvou o pacote de instalação.

  Se a tela de boas-vindas não aparecer, vá ao diretório raiz do CD e dê um duplo clique no arquivo `autorun.exe`.

- Para instalar o Bitdefender usando arquivo de instalação da rede baixado no seu computador, localize o arquivo e dê um duplo clique sobre ele.Isto irá iniciar o download dos arquivos de instalação, o que poderá demorar um pouco, dependendo da sua conexão à Internet.

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 antiga do Bitdefender, será avisado para removê-la do seu sistema.Por favor siga as instruções para remover o software do seu sistema, evitando assim que ocorram problemas mais tarde.

Nota
Pode ser preciso reiniciar o seu computador para concluir a remoção dos programas antivírus detectados.

Siga os passos do assistente de configuração para instalar o Bitdefender Antivirus Plus 2012.

Passo 1 - Boas-vindas

Por favor leia o Acordo de Licença e selecione **Aceitar & Continuar**.O Acordo de Licença contém os termos e condições sob os quais você pode usar o Bitdefender Antivirus Plus 2012.

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

Passo 2 - Registrar o seu produto

Para concluir o registro do seu produto insera a chave de licença e crie uma conta MyBitdefender.É necessária uma conexão ativa à Internet.

Proceda consoante a sua situação:

- **Eu adquiri o produto**

  Neste caso, registre o produto seguindo estas etapas:

  1. Selecione **Adquiri o produto e quero registrar-me agora**.
  2. Insira a chave de licença no campo correspondente.

     Nota
     A sua chave de licença pode ser encontrada:

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

3. Digite o seu endereço de e-mail no campo respetivo.

Importante

É necessário um endereço de e-mail válido.Uma mensagem de confirmação será enviada para o endereço indicado.

4. Clique **Registrar Agora**.

- **Desejo avaliar o Bitdefender**

  Neste caso, pode utilizar o produto durante 30 dias.Para iniciar o período de avaliação, selecione **Quero avaliar este produto**.

  Para usar os recursos online do produto, precisa de criar uma conta MyBitdefender.Para criar uma conta, digite o seu endereço de e-mail no campo respetivo.Uma mensagem de confirmação será enviada para o endereço indicado.Se já possui uma conta, insira o endereço de e-mail associado à mesma para registrar o produto nessa conta.

Configurações personalizadas

Opcionalmente, durante este passo você pode personalizar as configurações de instalação clicando em **Personalizar Configurações**.

Caminho da Instalação

Por padrão, o Bitdefender Antivirus Plus 2012 será instalado em `C:\Arquivos de Programa\Bitdefender\Bitdefender 2012`.Se deseja alterar o 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 2012 requer o acesso à Internet para registro do produto, baixar atualizações de segurança e de produtos, componentes de detecção na nuvem, etc.Se usar uma conexão por proxy em vez de uma conexão direta à Internet, deve selecionar esta opção e configurar as definições.

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

Ativar atualização P2P

Pode partilhar os arquivos e as assinaturas com outros utilizadores do Bitdefender.Desta forma, as atualizações do Bitdefender são mais rápidas.Se não quiser activar este recurso, seleccione a respectiva caixa.

Nota

Não será partilhada qualquer informação de identificação pessoal se este recurso estiver ativado.

Se quiser minimizar o impacto do tráfego de rede no desempenho do sistema durante as atualizações, utilize a opção de partilha de atualizações.Bitdefender usa as portas 8880 - 8889 para atualizações peer-to-peer.

Enviar Relatórios de Utilização Anônimos

Por predefinição, os Relatórios de Uso Anônimo estão ativados.Ao ativar esta opção, os relatórios que contêm informação sobre como você usa o produto são enviados para os servidores Bitdefender.Esta informação é essencial para melhorar o produto e pode ajudar-nos a oferecer-lhe uma experiência melhor no futuro.Note que estes relatórios não contêm dados confidenciais, tais como seu nome ou endereço de IP e que também não serão usados para fins comerciais.

Clique em **OK** para confirmar as suas preferências.

Clique em **Instalar** para iniciar a instalação.

Passo 3 - Evolução da instalação

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

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

Passo 4 - Terminar

É apresentado um resumo da instalação.Se tiver sido detectado malware ativo e removido durante a instalação, pode ser necessário reiniciar o sistema.

Clique em **Finalizar**.

1.3.1. Atualizar a partir de uma versão mais antiga

Se você estiver usando uma versão anterior do Bitdefender, existem duas formas de atualizar para Bitdefender Antivirus Plus 2012:

- Instalar o Bitdefender Antivirus Plus 2012 encima da antiga versão.O Bitdefender irá detectar a versão antiga e ajudará a removê-la antes de instalar a nova versão.Precisará de reiniciar o computador durante a atualização.
- Remova a versão anterior, reinicie o computador e instale a nova versão conforme descrito nas páginas anteriores.Use este método de upgrade se o outro falhar.

Nota

As definições do produto e o conteúdo da quarentena não serão importados da versão anterior.

2. Introdução

Assim que instalar o Bitdefender Antivirus Plus 2012, o seu computador ficará protegido contra todos os tipos de malware (tais como vírus, spyware e cavalos de tróia).

O Piloto Automático está ativado por predefinição não sendo necessario efetuar qualquer configuração.No entanto, poderá querer usufruir das definições do Bitdefender para optimizar e melhorar a sua protecção.

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 funcionamento do programa encontram-se disponíveis na janela Eventos.Para mais informações, por favor consulte em "*Eventos*" (p. 13).

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

Se você ainda não registrou o produto (incluindo a criação da conta MyBitdefender), lembre-se de fazê-lo antes do término do período de experiência.Crie uma conta para usar as características online do produto.Para mais informações sobre o processo de registro, por favor consulte o "*Registro do Produto*" (p. 8).

2.1. Abrindo o Bitdefender

Para acessar a interface principal do Bitdefender Antivirus Plus 2012, utilize o menu Iniciar do Windows, seguindo o caminho **Iniciar → Todos os Programas → Bitdefender 2012 → Bitdefender Antivirus Plus 2012** ou, mais rapidamente, faça duplo-clique no ícone do Bitdefender na bandeja do sistema.

Para mais informações sobre a janela e ícone do Bitdefender na bandeja do sistema, por favor consulte "*Interface Bitdefender*" (p. 19).

2.2. O que você precisa fazer após a instalação

Se quiser que o Bitdefender tome todas as decisões relacionadas com segurança por si, mantenha o Piloto Automático ativado.Para mais informações, por favor consulte em "*Automático*" (p. 14).

Aqui está uma lista de tarefas que você poderá executar após a instalação:

- Se o seu computador se conectar à Internet através de um servidor proxy, você deve configurar as definições do proxy conforme escrito em "*Como posso configurar Bitdefender para usar um proxy de conexão à Internet?*" (p. 33).
- Se instalou Bitdefender em diversos computadores na sua rede doméstica, pode gerenciar todos os produtos Bitdefender remotamente a partir de um único

computador.Para mais informações, por favor consulte em "*Mapa de Rede*" (p. 68).

- Criar regras de Proteção de Dados para evitar que os seus dados pessoais importantes sejam revelados sem a sua autorização.Para mais informações, por favor consulte em "*Proteção de Dados*" (p. 64).

2.3. Registro do Produto

Para ficar protegido com o Bitdefender, deve registrar o seu produto inserindo uma chave de licença e criando uma conta MyBitdefender.

A chave de licença especifica quanto tempo você tem direito a utilizar o produto.Logo que a chave da licença expirar, o Bitdefender para de executar as suas funções e proteger o seu computador.

Você deve comprar uma chave de licença ou renovar sua licença poucos dias antes do prazo que a chave de licença atual expira.Para mais informações, por favor consulte em "*Adquirir ou renovar chaves de licença*" (p. 11).Se estiver usando uma versão teste do Bitdefender, deve registrá-la com a chave de licença se quiser continuar a usá-lo depois que o período de teste terminar.

A conta MyBitdefender oferece o acesso a atualizações do produto e permite usar os serviços online oferecidos pelo Bitdefender Antivirus Plus 2012.Se você já possui uma conta, registre o seu produto Bitdefender nessa conta.

A conta MyBitdefender permite:

- Mantenha o seu produto atualizado.
- Recupere sua chave de licença, caso a tenha perdido.
- Contatar o Apoio ao Cliente Bitdefender.
- Obtenha proteção para a sua conta Facebook com Safego.

2.3.1. Inserir a sua chave de licença

Se, durante a instalação, selecionou a avaliação do produto, pode usá-lo durante um período de 30 dias.Para continuar a usar o Bitdefender quando o período de experiência expirar, você deve registrá-lo com uma chave de licença.

Se você quiser registrar o produto com uma chave de licença ou alterar a atual, clique no link **Informação de Licença**, localizado na parte inferior da janela do Bitdefender.A janela de registo irá aparecer.

Você pode ver o estado do registo do Bitdefender, a chave de licença atual e quantos dias faltam para a licença expirar.

Para registrar o Bitdefender Antivirus Plus 2012:

1. Insira a chave de licença no campo de edição.

Nota

A sua chave de licença pode ser encontrada:

- Na bolsa do CD.
- No cartão de registo do produto.
- no e-mail da sua compra on-line.

Se não tiver uma chave de licença do Bitdefender, clique no link fornecido na janela para abrir a página da rede onde poderá adquirir uma.

2. Clique **Registrar Agora**.

2.3.2. Efetuar login para MyBitdefender

Se você indicou um endereçço de e-mail durante a instalação, foi enviado um e-mail de confirmação para o endereço indicado.Clique no link do e-mail para concluir o registro.

Se não concluiu o registro, o Bitdefender irá notificá-lo de que precisa fazê-lo.

Importante

Você precisa criar uma conta dentro de 30 dias após a instalação do Bitdefender.Caso contrário, Bitdefender não mais efetuará atualizações de antivirus.

Para criar ou fazer login em uma conta MyBitdefender, clique no link **Concluir registro** / **MyBitdefender**, localizado na parte inferior da janela do Bitdefender.

A janela MyBitdefender abrirá.Proceda de acordo com sua situação.

Quero criar uma conta MyBitdefender

Para criar uma conta MyBitdefender com sucesso, siga estes passos:

1. Selecione **Criar uma nova conta**.

   Uma nova janela irá aparecer.

2. Digite as informações necessárias nos campos correspondentes.Os dados que nos fornecer serão mantidos confidenciais.

   - **Nome** - insira um nome de usuário para a sua conta. Este campo é opcional.
   - **E-mail** - insira o seu endereço de e-mail.
   - **Senha** - digite a senha da sua conta.A senha deve conter no mínimo 6 caracteres.
   - **Confirmar senha** - insira a senha novamente.
   - Opcionalmente, a Bitdefender poderá informá-lo a respeito de ofertas especiais e promoções usando o endereço de e-mail da sua conta.Para ativar esta opção, selecione **Autorizo que o Bitdefender me envie e-mails**.

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

3. Clique em **Submeter**.
4. Antes de poder usar a sua conta, deverá concluir o registro.Verifique o seu e-mail e siga as instruções do email de confirmação enviado pela Bitdefender.

Nota
Você também pode executar login usando sua conta Facebook ou Google.Para mais informações, por favor consulte"Quero executar o login usando minha conta do Facebook ou Google." (p. 10)

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

Para conectar-se com sua conta Facebook ou Google, siga estes passos:

1. Clique no ícone do serviço que deseja usar para executar o login.Você será redirecionado para a página de início de sessão daquele serviço.
2. Siga as instruções fornecidas pelo serviço selecionado para ligar a sua conta ao Bitdefender.

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

Já tenho uma conta MyBitdefender

Se tiver iniciado numa conta do seu produto anterior,o Bitdefender irá detectá-la e iniciará a sessão nessa conta.Pode visitar a sua conta em http://my.bitdefender.com clicando em **Ir paraMyBitdefender**.

Se quiser conectar-se em uma conta diferente, clique no link correspodente e siga as instruções das seções anteriores.

Se você já tiver uma conta ativa, mas o Bitdefender não a detectou, siga estes passos para conectar-se a essa conta:

1. Digite o endereço de email e senha da sua conta nos campos correspondentes.

Nota
Se não se lembra de sua senha, clique em **Esqueci a senha** e siga as instruções para recuperá-la.

2. Clique em **Iniciar Sessão**.

2.3.3. Adquirir ou renovar chaves de licença

Se o período experimental, vai acabar em breve, você deve comprar uma chave de licença e registrar o seu produto.De igual modo, se a sua atual chave de licença vai expirar brevemente, deve renová-la.

O Bitdefender avisa quando se aproxima o término da data de validade da sua licença atual. Siga as instruções no alerta para adquirir uma nova licença.

Você pode visitar uma página na rede onde uma chave de licença pode ser adquirida a qualquer momento, seguindo estes passos:

1. Abra a janela de Bitdefender.
2. Clique no link **Info da Licença**, localizado no fundo da janela do Bitdefender, para abrir a janela de registro do produto.
3. Clique no link fornecido na parte inferior da janela.

2.4. Corrigindo os problemas

O Bitdefender utiliza um sistema de rastreio de problemas para detectar e lhe informar sobre os problemas que podem afetar a segurança do seu computador e dados. Por padrão, ele irá monitorar apenas uma série de problemas que são considerados muito importantes. De qualquer forma você pode configurar ele conforme suas necessidades, escolhendo quais problemas em específico você deseja ser notificado.

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

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

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

Cor vermelha: Problemas críticos afetam a segurança de seu sistema. Eles requerem sua atenção imediata e devem ser corrigidos assim que possível.

Cor amarela: Problemas não críticos afetam a segurança de seu sistema. Você deve verificar e corrigí-los quando tiver tempo.

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

Quando você abre a janela do Bitdefender, a área do status de Segurança na barra de ferramentas superior irá indicar o número e a natureza dos problemas afetando o seu sistema.

2.4.1. Assistente de Correção de todos os Problemas

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

1. Para abrir o assistente, faça qualquer um dos seguintes:
   - Clique com o botão direito do mouse no ícone do Bitdefender na bandeja do sistema e selecione **Reparar todas as Incidências**.Dependendo das incidências detectadas, o ícone é vermelho (indica incidências críticas) ou amarelo (indica incidências não críticas).
   - Abra a janela Bitdefender e clique num local qualquer dentro da área de Segurança na barra de ferramentas superior (por exemplo, pode clicar no botão **Reparar Todas as Incidências**).
2. Você pode verificar as incidências que afetam a segurança do seu computador e dos dados.Todas ocorrências atuais estão selecionadas para serem corrigidas.

   Se não quiser resolver uma incidência específica de imediato, limpe a caixa correspondente.Será solicitado que você especifique por quanto tempo pretende adiar a correção do problema.Escolha a opção desejada no menu e clique em **OK**.Para deixar de monitorar a categoria de problema respectiva, escolha **Permanentemente**.

   O status da incidência mudará para **Adiar** e não será executada nenhuma ação para repará-la.
3. Para corrigir as ocorrências selecionadas, clique **Iniciar**. Algumas ocorrências são corrigidas imediatamente. Para outras, um assistente ajudará a corrigir

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

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

2.4.2. Configure o alerta de status

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

1. Abra a janela de Bitdefender.

2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Geral** localizado no lado esquerdo do menu e depois no separador **Configurações**.
4. Procure e clique no link **Configurar estado de alerta**.
5. Clique nos botões para ligar ou desligar os alertas de estado de acordo com as suas preferências.

2.5. Eventos

O Bitdefender mantém um registro detalhado dos eventos relacionados com a sua atividade no seu computador.Os eventos são uma ferramenta importante na monitoração e gestão da proteção do seu Bitdefender.Por exemplo, você pode facilmente verificar se a atualização foi executada com sucesso, se foi encontrado algum malware no seu computador.Adicionalmente, pode tomar outras ações se necessário ou alterar ações tomadas pelo Bitdefender.

Para abrir a Janela Eventos, abra a janela do Bitdefender e clique no botão **Eventos** na barra de ferramentas superior.

De forma a ajudá-lo a filtrar os eventos do Bitdefender, encontram-se disponíveis as seguintes categorias no menu do lado esquerdo:

- **Antivirus**
- **Controle Privacidade**
- **Mapa de Rede**
- **Atualizar**
- **Safego**

Encontra-se disponível uma lista de eventos para cada categoria.Para obter informações sobre um evento da lista em particular, clique nele. Os detalhes do evento são apresentados na parte inferior da janela.Cada evento surge com a seguinte informação: uma breve descrição, a ação do Bitdefender quando este ocorreu, e a data e hora em que ocorreu.Podem ser fornecidas opções para tomar outras medidas, caso seja necessário.

Pode filtrar os eventos pela sua importância.Há três tipos de eventos, sendo cada tipo indicado com um ícone específico:

Eventos de **Informação** indicam operações bem sucedidas.
O eventos de **Aviso** indicam incidências não críticas. Você deve verificar e resolvê-los quando puder.
Os eventos **Críticos** indicam problemas críticos. Verifique-os imediatamente.

Para o ajuda-lo a administrar facilmente os eventos registrados, cada seção da janela de Eventos oferece opções para eliminar ou marcar como lidos todos os eventos daquela seção.

2.6. Automático

Para todos os usuários que desejam nada mais da sua solução de segurança do que serem protegidos sem serem incomodados, a Bitdefender Antivirus Plus 2012 foi concebida com um modo Piloto Automático.

No Piloto Automático, o Bitdefender aplica uma configuração de segurança ótima e toma todas as decisões relacionadas com segurança por si.Isto significa que não verá pop-ups nem alertas e não terá de configurar quaisquer definições.

No modo Piloto Automático, o Bitdefender corrige automaticamente problemas críticos e silenciosamente gerencia:

- Proteção antivírus, proporcionada pela análise no acesso e análise contínua.
- Proteção de Firewall.
- A Proteção de privacidade, providenciada pela filtragem antiphishing e antimalware para o seu navegador.
- Atualizações Automáticas.

Por predefinição, o Piloto Automático estará ativado no momento em que a instalação do Bitdefender for concluída.Enquanto o Piloto Automático estiver ativado, o ícone Bitdefender na bandeja do sistema mudará para  .

Para ligar ou desligar o Piloto Automático, abra a janela Bitdefender e clique no botão **Piloto Automático** na barra de ferramentas superior.

Importante

Enquanto o Piloto Automático estiver ligado, se alguma de suas configurações for modificada, este será desligado.

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

2.7. Modo Jogo e Modo Laptop

Algumas atividades do computador, como jogos ou apresentações, requerem melhor resposta do sistema e performace e sem interrupções.Quando seu laptop esta operando funcionando com a bateria, o melhor é que operações desnecessárias, que consomem energia, sejam adiadas até que o laptop esteja ligado a uma rede de energia.

Para se adaptar a estas situações particulares, o Antivirus Bitdefender 2010 inclui dois modos especiais de operação:

- Modo de Jogo
- Modo Laptop

2.7.1. Modo de Jogo

O Modo de Jogo modifica temporariamente as definições da proteção de forma a minimizar o seu impacto no desempenho do sistema.As seguintes definições são aplicadas quando o Modo de Jogo está ligado:

- Todos os alertas e pop-ups do Bitdefender estão desativados.
- A Análise no acesso está configurada para o nível de proteção **Permissivo**.
- A Análise Automática está desligada.A Análise Automática encontra e usa fatias de tempo quando o uso dos recursos do sistema fica abaixo de um determinado limite, para realizar análises periódicas a todo o sistema.
- A Atualização Automática está desligada.
- A barra de ferramentas Bitdefender do seu navegador está desativada quando joga online jogos baseados no navegador.

Enquanto no Modo de Jogo, pode ver a letraG sobre o  icone do Bitdefender.

Usar o Modo de Jogo

Por padrão, o Bitdefender entra automaticamente em Modo Jogo quando inicia um jogo da lista dos jogos conhecidos do Bitdefender, ou quando uma aplicativo vai para tela cheia.O Bitdefender retornará automaticamente ao modo de operação normal quando você fechar o jogo ou quando o aplicativo detectado sair da tela cheia.

Se você quiser ativar o Modo Jogo manualmente, use um dos métodos a seguir:

- Clique com o botão-direito do mouse no ícone do Bitdefender que está na área de notificação e selecione **Ligar Modo de Jogo**.
- Aperte `Ctrl+Shift+Alt+G` (A tecla atalho por padrão).

Importante
Não se esqueça de desligar o Modo de Jogo quando terminar. Para fazer isto, use os mesmos processos que usou para o ligar.

Mudar a Hotkey do Modo de Jogo

Pode entrar manualmente em Modo Jogo usando uma tecla de atalho como padrão `Ctrl+Alt+Shift+G`.Se deseja mudar a hotkey, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Geral** localizado no lado esquerdo do menu e depois no separador **Definições**.

4. Na opção **Ativar teclado de atalho do Modo Jogo**, defina a tecla de atalho desejada:

   a. Escolha as teclas que deseja usar ao seleccionar uma das seguintes: Tecla Control (`Ctrl`), Tecla Shift (`Shift`) ou tecla Alternate (`Alt`).

   b. No campo de edição, insira a letra correspondente à tecla que deseja usar.

   Por exemplo, de deseja usar a hotkey `Ctrl+Alt+D` , deve seleccionar `Ctrl` e `Alt` e inserir D.

Nota
Para desativar a tecla de atalho, desligue a opção **Ativar atalho do teclado do Modo de Jogo**.

Ligar ou desligar automaticamente o modo jogo

Para ligar ou desligar o modo de jogo automático, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Geral** localizado no lado esquerdo do menu e depois no separador **Definições**.
4. Ligue ou desligue o modo de jogo automático clicando no botão correspondente.

2.7.2. Modo Laptop

O Modo Portátil foi especialmente desenhado para os usuários de laptops. O seu propósito é minimizar o impacto do Bitdefender no consumo de energia enquanto o laptop estiver a funcionar a bateria.Quando Bitdefender opera no Modo Laptop, a Análise Automática e Atualização Automática estão desligadas, já que requerem mais recursos do sistema e, consequentemente, aumento do consumo de energia.

O Bitdefender detecta quando o seu laptop está funcionando com bateria e automaticamente entra em Modo Laptop.Desta forma, O Bitdefender sai automaticamente do Modo Laptop quando detecta que o seu laptop não está mais funcionando com bateria.

Para ligar ou desligar o modo automático do laptop, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Geral** localizado no lado esquerdo do menu e depois no separador **Definições**.
4. Ligue ou desligue o modo laptop clicando no botão correspondente.

Se o Bitdefender não estiver instalado em um laptop, desligue o modo automático do laptop.

2.8. Configurações de proteção da senha do Bitdefender

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

Para configurar a proteção de senha para as definições do Bitdefender, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Geral** localizado no lado esquerdo do menu e depois no separador **Definições**.
4. Na seção **Definições da proteção por senha**, ative a proteção por senha, clicando no botão.
5. Clique no link **Alterar senha**.
6. Insira a senha nos dois campos e depois clique em **OK**.A senha deve conter no mínimo 8 caracteres.

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

Importante

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

Para remover a proteção da senha, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Geral** localizado no lado esquerdo do menu e depois no separador **Definições**.
4. Na seção **Definições da proteção por senha**, desative a proteção por senha, clicando no botão.
5. Digite a nova senha e depois clique em **OK**.

2.9. Relatórios de utilização anônimos

Por predefinição, o Bitdefender envia relatórios que contêm informação sobre como usá-lo nos servidores Bitdefender.Esta informação é essencial para melhorar o produto e pode ajudar-nos a oferecer-lhe uma experiência melhor no futuro.Note

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

Caso queira parar de enviar Relatórios Anônimos de utilização, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Geral** localizado no lado esquerdo do menu e depois no separador **Configurações**.
4. Desligue os relatório de uso Anônimo clicando no botão respectivo.

2.10. Reparar ou remover o Bitdefender

Se pretende reparar ou remover o Bitdefender Antivirus Plus 2012, faça o seguinte a partir do menu Iniciar do Windows: **Iniciar → Todos os Programas → Bitdefender 2012 → Reparar ou Desinstalar**.

Seleccione a ação que quer efectuar:

- **Reparar** - para reinstalar todos os componentes do programa.
- **Remover** - para remover todos os componentes instalados.

Nota
Recomendamos que escolha **Desinstalar** para uma reinstalação limpa.

Aguarde que o Bitdefender conclua a ação que seleccionou.Isto irá demorar vários minutos.

Precisará de reiniciar o computador para concluir o processo

3. Interface Bitdefender

O Bitdefender Antivírus 2010 vai de encontro às necessidades tanto de iniciantes como de pessoas mais técnicas. Sua interface gráfica do usuário foi desenhada para facilitar o uso de ambos.

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

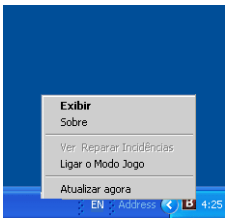
A janela principal concede acesso rápido aos módulos do produto e informações importantes sobre o mesmo, e permite-lhe executar tarefas comuns.

Para configurar o seu produto Bitdefender em detalhe e realizar tarefas administrativas avançadas, poderá encontrar todas as ferramentas de que precisa na janela configurações.

3.1. Ícone da bandeja do sistema

Para gerenciar todo o produto mais rapidamente, você pode usar o ícone do Bitdefender na área de notificação.Se fizer um duplo-clique neste ícone, o Bitdefender irá abrir. Clicando com o botão direito do mouse sobre ele aparecerá um menu contextual que lhe permitirá uma administração rápida do Bitdefender.

- **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.
- **Reparar Incidências** - ajuda-o a remover as vulnerabilidades de segurança.Se a opção não está disponível, não há problemas a serem corrigidos.Para informação detalhada, por favor consulte em "*Corrigindo os problemas*" (p. 11).
- **Alternar o Modo Jogo ligado/desligado** - ativa/desativa o Modo Jogo.
- **Atualizar agora** - realiza uma atualização imediata.Pode seguir o estado da atualização no painel Atualizar da janela principal do Bitdefender.



Ícone da área de notificação

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

Problemas críticos afetam a segurança de seu sistema. Eles requerem sua atenção imediata e devem ser corrigidos assim que possível.

Não há incidências críticas a afetar a segurança do seu sistema.Deve verificá-las e repará-las quando tiver oportunidade.

O produto opera em Modo Jogo.

O Piloto Automático Bitdefender está ativado.

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

3.2. Janela Principal

A janela principal do Bitdefender permite-lhe realizar tarefas comuns, reparar rapidamente problemas de segurança, visualizar informação sobre eventos na operação de produtos e personalizar 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 você poderá verificar o status de segurança de seu computador e acessar tarefas importantes.

Área de painéis

É aqui que você poderá gerenciar os módulos principais do Bitdefender.

Adicionalmente, pode encontrar diversos lins úteis na parte inferior da janela:

Link	Descrição
Comente	Abre uma página da rede no seu navegador onde você pode responder uma pesquisa breve sobre sua experiência de uso do produto.Contamos com o seu feedback em nossa busca constante para melhorar os Bitdefender produtos.
Concluir registro / MyBitdefender	Abre a janela da conta MyBitdefender, onde você pode criar ou entrar em uma conta.A conta MyBitdefender é necessária para receber atualizações e se beneficiar dos recursos online do seu produto.Para saber mais sobre como criar uma conta e as vantagens oferecidas, por favor consulte *"Efetuar login para MyBitdefender"* (p. 9).
Informações da Licença	Abre uma janela onde pode ver a informação da chave de licença atual e registar o seu produto com a nova chave de licença.
Ajuda e Suporte	Clique nesta hiperligação se precisar de ajuda com o Bitdefender.

Link	Descrição
	Adiciona pontos de interrogação em diferentes áreas da janela Bitdefender para ajudá-lo a encontrar facilmente informação sobre os diferentes elementos da interface. Mova o cursor do mouse sobre uma marca para ver informações rápidas sobre o elemento próximo a ele.

3.2.1. 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 status da segurança muda dependendo das incidências detectadas e são apresentadas diferentes mensagens:

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

  Ao clicar no botão **Visualizar Incidências**  no centro da barra de ferramentas ou em qualquer ponto da área de estado da segurança à esquerda, você pode acessar o assistente que o ajudará a remover facilmente quaisquer ameaças do seu computador.Para informação detalhada, por favor consulte em "*Corrigindo os problemas*" (p. 11).

- **Eventos** permite acessar a um histórico detalhado dos eventos relevantes que ocorreram na atividade do produto.Para informação detalhada, por favor consulte em "*Eventos*" (p. 13).
- **Definições** permite acessar as definições da janela onde poderá configurar as definições do produto.Para informação detalhada, por favor consulte em "*Janela de configurações*" (p. 24).
- O **Piloto Automático** permite ativar o Piloto Automático e desfrutar de uma segurança silenciosa.Para informação detalhada, por favor consulte em "*Automático*" (p. 14).

3.2.2. Área de painéis

A área dos painéis é onde pode gerir diretamente os módulos do Bitdefender.

Pode organizar os painéis conforme desejar.Para reorganizar a área de acordo com as suas necessidades, arraste os painéis individuais e solte-os em outros espaços.

Para navegar pelos painéis, use o cursor abaixo dos painéis ou as setas localizadas no lado direito e no lado esquerdo.

De cima para baixo, cada painel de módulo contém os seguintes elementos:

- O nome do módulo.
- Uma mensagem de status.
- O ícone do módulo.Clique no ícone de um módulo para configurar as suas definições na janela definições.
- Um botão que lhe permite relizar tarefas importantes relacionadas com o módulo.
- Encontra-se disponível um botão em determinados painéis que lhe permite ligar ou desligar características importantes do módulo.

Os painéis disponíveis nesta área são:

Antivirus

A proteção 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.

Você pode facilmente acessar tarefas de análise importantes a partir do painel Antivírus.Clique em **Analisar agora** e selecione uma tarefa no menu pendente:

- Análise Rápida
- Análise Completa
- Análise Pessoal
- Analisar Vulnerabilidade
- Modo de recuperação

O botão **Análise Automática** permite ligar ou desligar o recurso da Análise Automática.

Para mais informações sobre tarefas de análise e como configurar a proteção antivírus, por favor consulte "*Proteção Antivírus*" (p. 35).

Atualizar

Num mundo em que os cibercriminosos tentam constantemente arranjar novas formas de causar danos, é essencial manter a sua solução de segurança atualizada se quiser estar um passo à frente deles.

Por padrão, o Bitdefender procura automaticamente atualizações de hora em hora. Se quiser desligar as atualizações automáticas, use o botão **Atualização Automática** no painel Atualizar.

Atenção

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

Clique no botão **Atualizar Agora** no painel para iniciar de imediato uma atualização.

Para mais informações sobre as atualizações de configuração, consulte "*Atualizar*" (p. 72).

Privacidade

O módulo de controle de privacidade ajuda a manter dados pessoais importantes privados.Protege você quando estiver conectado à Internet contra ataques de phishing, tentativas de fraude, vazamento de dados privados, e muito mais.

Clique no botão **Gerenciar Regras** no painel Controle de Privacidade para ir para a seção Proteção de Dados onde você pode configurar as regras de privacidade.

O botão Antiphishing permite-lhe ligar ou desligar a proteção antiphishing.

Para mais informações sobre como configurar o Bitdefender para proteger a sua privacidade, por favor consulte "*Controle Privacidade*" (p. 61).

Mapa de Rede

Com o Mapa de Rede você pode facilmente administrar a segurança de computadores em sua casa a partir de um único computador.

Para começar, clique em **Gerenciar** no painel de Mapa de Rede e selecione **Ativar Rede**.

Quando a rede estiver ativada, se clicar em **Gerenciar** no painel de Mapa de Rede terá acesso às seguintes opções:

- **Desativar conexão** - desativar a rede.
- **Analisar todos** - iniciar a análise rápida ou análise completa ao sistema nos computadores administrados.
- **Atualizar todos os computadores** - atualizar os produtosBitdefender nos computadores gerenciados.

Para mais informações, por favor consulte em "*Mapa de Rede*" (p. 68).

Safego

Para ajudar a mantê-lo seguro no Facebook, você pode acessar ao Safego, a solução de segurança do Bitdefender para redes sociais, diretamente a partir do seu produto.

Clique **Ativar** para ativar e gerenciar a Safego da sua conta Facebook.

Se já ativou Safego, poderá acessar as estatísticas sobre suas atividades clicando no botão **Ver Relatórios**.

Para mais informações, por favor consulte em "*Proteção Safego para redes sociais*" (p. 76).

3.3. Janela de configurações

A janela de definições oferece-lhe o acesso a cada componente do produto e à personalização.Aqui você poderá configurar o Bitdefender detalhadamente.

Do lado esquerdo da janela existe um menu que contém todos os módulos de segurança.Cada módulo possui uma ou mais abas onde você pode configurar as definições de segurança correspondentes ou executar tarefas administrativas ou de segurança.A lista seguinte descreve resumidamente cada módulo.

Geral
: Permite configurar as definições gerais do produto, tais como definições de senha, Modo de Jogo, Modo Laptop, definições de proxy e alertas de estado.

Antivirus
: Permite-lhe configurar a sua proteção contra malware, detectar e reparar vulnerabilidades do seu sistema, configurar exceções de análise e gerenciar arquivos da quarentena.

Controle Privacidade
: Permite-lhe evitar que sejam roubados dados do seu computador e protege a sua privacidade enquanto se encontra on-line.Configurar proteção para o seu navegador da rede, software de mensagens instantâneas, gerernciar proteção de dados e mais.

Mapa de Rede
: Permite-lhe configurar e gerenciar os produtos Bitdefender instalados nos seus computadores em casa a partir de um só computador.

Atualizar
: Permite-lhe configurar o processo de atualização em detalhe.

Adicionalmente, pode encontrar diversos lins úteis na parte inferior da janela:

Link	Descrição
Comente	Abre uma página da rede no seu navegador onde você pode responder uma pesquisa breve sobre sua experiência de uso do produto.Contamos com o seu feedback em nossa busca constante para melhorar os Bitdefender produtos.
Concluir registro / MyBitdefender	Abre a janela da conta MyBitdefender, onde você pode criar ou entrar em uma conta.A conta MyBitdefender é necessária para receber atualizações e se beneficiar dos recursos online

Link	Descrição
	do seu produto.Para saber mais sobre como criar uma conta e as vantagens oferecidas, por favor consulte "*Efetuar login para MyBitdefender*" (p. 9).
Informações da Licença	Abre uma janela onde pode ver a informação da chave de licença atual e registar o seu produto com a nova chave de licença.
Ajuda e Suporte	Clique nesta hiperligação se precisar de ajuda com o Bitdefender.
	Adiciona pontos de interrogação em diferentes áreas da janela Bitdefender para ajudá-lo a encontrar facilmente informação sobre os diferentes elementos da interface. Mova o cursor do mouse sobre uma marca para ver informações rápidas sobre o elemento próximo a ele.

Para voltar à janela principal, clique no botão **Início** que se encontra no canto superior direito da janela.

4. Como

Este capítulo fornece instruções passo-a-passo para definir configurações habitualmente usadas ou para realiar tarefas comuns com o Bitdefender.Alguns dos tópicos fazem referência a outros tópicos onde você pode encontrar informações detalhadas.

4.1. Como posso registrar uma versão experimental?

Se você instalou uma versão teste, só poderá usá-la durante um período de tempo limitado.Para continuar a usar o Bitdefender depois que o período de testes expirar, você deve registrar o seu produto com uma chave de licença e criar uma conta MyBitdefender.

- Para registrar o Bitdefender, siga estes passos:

  1. Abra a janela de Bitdefender.
  2. Clique no link **Informação de Licença** na parte inferior da janela.A janela de registo irá aparecer.
  3. Introduza a chave de registo e clique em **Registar Agora**.

     Se não tiver uma chave de licença, clique no link fornecido na janela para visitar a página na rede onde poderá adquirir uma.

4. Aguarde até que o processo de registro esteja concluído e feche a janela.

- Para criar uma conta MyBitdefender, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Clique no link **Concluir registro** na parte inferior da janela.A janela da conta irá aparecer.
3. Selecione o link respectivo para criar uma nova conta.
4. Digite as informações necessárias nos campos correspondentes.Os dados que nos fornecer serão mantidos confidenciais.

   Clique em **Submeter**.
5. Consulte o seu e-mail e siga as instruções recebidas para concluir o registro.

Nota
Use o endereço de e-mail e a senha que nos forneceu para fazer log in na sua conta em http://my.bitdefender.com.

4.2. Como posso registrar o Bitdefender sem uma conexão com a Internet?

Se acabou de adquirir o Bitdefender e não possui uma conexão com a Internet, pode registrar o Bitdefender offline.

Para registar Bitdefender com a sua chave de licença, siga os seguintes passos:

1. Ir para um PC conectado à Internet.Por exemplo, pode usar o computador de um amigo ou um PC público.
2. Ir para https://my.bitdefender.com para criar a conta MyBitdefender.
3. Efetue login na sua conta e selecione**Obter registro offline**.
4. Insira a chave de licença que adquiriu.
5. Clique em **Enviar** para obter o código de confirmação.

Importante
Anote o código de confirmação.

6. Ir para o seu PC com o código de confirmação.
7. Abra a janela de Bitdefender.
8. Clique no link **Informação de Licença** na parte inferior da janela.A janela de registo irá aparecer.
9. Selecione a opção para registrar o produto com um código de confirmação.

10. Insira o código de confirmação no campo correspondente e clique em **Enviar**.
11. Aguarde até que o processo de registro esteja concluído e clique em **Concluir**.

4.3. Como posso fazer o upgrade para outro produto Bitdefender 2012?

Você pode fazer facilmente o upgrade de um produto Bitdefender 2012 para outro.

Imaginemos a seguinte situação: você tem utilizado o Bitdefender Antivirus Plus 2012 há já algum tempo e decidiu recentemente mudar para o Bitdefender Total Security 2012, com todos os recursos adicionais que este oferece.

Tudo que você precisa fazer é adquirir uma chave de licença para o produto 2012 Bitdefender que você deseja atualizar e inseri-lo na janela de registro do produto Bitdefender 2012 que você está usando atualmente.

Siga esses passos:

1. Abra a janela de Bitdefender.
2. Clique no link **Informação de Licença** na parte inferior da janela.A janela de registo irá aparecer.
3. Introduza a chave de registo e clique em **Registar Agora**.
4. O Bitdefender irá informar que a chave de licença destina-se a um produto diferente e dará a opção de instalá-lo.Clique no link correspondente e siga o procedimento para efetuar a atualiação.

4.4. Quando devo reinstalar o Bitdefender?

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

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

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

Para reinstalar o Bitdefender use o disco de instalação que adquiriu ou baixe uma nova versão do site web Bitdefender.

Durante a instalação, será solicitado que você regisrte o produto com a sua chave de licença.

Se não consegue encontrar sua chave de licença, você pode efetuar login em https://my.bitdefender.com para recuperá-la.Digite o endereço de email e senha da sua conta nos campos correspondentes.

4.5. Quando é que a proteção do Bitdefender expira?

Para saber quantos dias restam para a sua chave de licença expirar, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no link **Informação de Licença** na parte inferior da janela.
3. Na janela **Registrar o seu produto** poderá verificar o número de dias restantes.

4.6. Como posso renovar a proteção do meu Bitdefender?

Quando a proteção do seu Bitdefender estiver quase a expirar, deve renovar a sua chave de licença.

- Siga os seguintes passos para visitar um site onde você pode renovar a sua chave de licença do Bitdefender:
  1. Abra a janela de Bitdefender.
  2. Clique no link **Informação de Licença** na parte inferior da janela.
  3. Clique **Não tem uma chave de licença? Compre uma agora!**
  4. Abre-se uma página da rede no seu navegador onde poderá adquirir a chave de licença do Bitdefender.

  Nota
  Como alternativa, pode contatar o revendedor onde adquiriu o produto Bitdefender.

- Siga estes passos para registrar o seu Bitdefender com a nova chave de licença:
  1. Abra a janela de Bitdefender.
  2. Clique no link **Informação de Licença** na parte inferior da janela.A janela de registo irá aparecer.
  3. Introduza a chave de registo e clique em **Registar Agora**.
  4. Aguarde até que o processo de registro esteja concluído e feche a janela.

Para mais informações, poderá contatar a Bitdefender para suporte, como descrito na seção "*Suporte*" (p. 93).

4.7. Que produto Bitdefender estou usando?

Para saber que programa Bitdefender instalou, siga estes passos:

1. Abra a janela de Bitdefender.
2. Na parte superior da janela você verá o seguinte:

- Bitdefender Antivirus Plus 2012
- Bitdefender Internet Security 2012
- Bitdefender Total Security 2012

4.8. Como posso analisar um arquivo ou uma pasta?

A forma mais fácil e recomendada para analisar um arquivo ou pasta é clicando com o botão direito no objeto que deseja analisar e selecionando **Analisar com o Bitdefender** no menu.Para concluir a análise, siga o assistente de Análise Antivírus.O Bitdefender executará automaticamente as ações recomendadas nos arquivos detectados.Se ainda houver ameaças não resolvidas, será solicitado que você escolha as ações a serem tomadas com relação às mesmas.Para mais informações, por favor consulte em "*Assistente do analisador Antivírus*" (p. 46).

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

- Você suspeita que um arquivo específico ou diretório esteja infectado.
- Sempre que você faz download de arquivos da Internet e suspeita que podem ser perigosos.
- Analisar um compartilhamento de rede antes de copiar os arquivos para o computador.

4.9. Como posso analisar o meu sistema?

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

1. Abra a janela de Bitdefender.
2. Ir para o painel **Antivírus**.
3. Clique em **Analisar Agora** e selecione **Análise Completa ao Sistema** no menu pendente.
4. Siga o assistente de análise Antivírus para concluir a análise.O Bitdefender executará automaticamente as ações recomendadas nos arquivos detectados.Se ainda houver ameaças não resolvidas, será solicitado que você escolha as ações a serem tomadas com relação às mesmas.Para mais informações, por favor consulte em "*Assistente do analisador Antivírus*" (p. 46).

4.10. Como posso criar uma tarefa de análise personalizada?

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

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

1. Abra a janela de Bitdefender.
2. Ir para o painel **Antivírus**.

3. Clique em **Analisar Agora** e selecione **Análise Personalizada** no menu pendente.
4. Clique em **Adicionar Alvo** para seleccionar os arquivos ou as pastas a analisar.
5. Se desejar configurar detalhadamente as opções de análise, clique em **Opções de Análise**.

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

   Também pode optar por desligar o computador sempre que a análise termina, se não forem encontradas ameaças.Lembre-se de que esta será a ação padrão sempre que executar esta tarefa.
6. Clique em **Iniciar Análise** e siga o assistente de Análise Antivírus para completar a análise.Ao final da análise, será solicitado que você escolha as ações a serem tomadas nos arquivos detectados, caso haja algum.
7. Se quiser guardar a tarefa de análise para uso futuro, abra a janela de personalização da configuração da análise novamente.
8. Localize uma análise que acabou de executar na lista **Análises recentes**.
9. Passe com o cursor do mouse sobre o nome da análise e clique no ícone ★ para adicionar a análise à lista de análises favoritas.
10. Introduza um nome sugestivo para a análise.

4.11. Como posso excluir uma pasta da análise?

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

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

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

Para adicionar a pasta à lista de Exceções, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Exceções**.
4. Clique no link **Arquivos e pastas excluídos**.

5. Clique no botão **Adicionar**, localizado na parte superior da tabela de exceções.
6. Clique em **Explorar**, selecione a pasta que deseja excluir da análise e depois clique **OK**.
7. Clique em **Adicionar** e depois clique em **OK** para salvar as alterações e fechar a janela.

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

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

1. Desative a proteção antivírus em tempo real do Bitdefender:
   a. Abra a janela de Bitdefender.
   b. Clique no botão **Definições** na parte superior da barra de ferramentas.
   c. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Proteção**.
   d. Clique no botão para desligar **análise no acesso**.
2. Mostrar objectos ocultos no Windows.Para saber como fazer isto, consulte "*Como posso mostrar objetos ocultos no Windows?*" (p. 101).
3. Restaurar o arquivo da área de Quarentena:
   a. Abra a janela de Bitdefender.
   b. Clique no botão **Definições** na parte superior da barra de ferramentas.
   c. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Quarentena**.
   d. Selecione um arquivo e clique em **Restaurar**.
4. Adicionar o arquivo à lista de Exceções.Para saber como fazer isto, consulte "*Como posso excluir uma pasta da análise?*" (p. 31).
5. Active a protecção antivírus em tempo real do Bitdefender.
6. Contate os nossos representantes do suporte para que possamos remover a assinatura de detecção.Para saber como fazer isto, consulte "*Solicite Ajuda*" (p. 94).

4.13. Como proteger meus dados pessoais?

O Controle de Privacidade monitora os dados que saem do seu computador através de formulários da Rede, mensagens de e-mail ou mensagens instantâneas.

Para garantir que nenhum dado privado sai do seu computador sem o seu consentimento, você deve criar regras apropriadas de proteção de dados.As regras de de proteção de dados especificam as informações a serem bloqueados.

Para criar uma regra de Proteção de Dados, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Controle de Privacidade** no menu do lado esquerdo e depois no separador **Proteção de Dados**.
4. Se a **Proteção de Dados** estiver desligada, ative-a usando o botão adequado.
5. Selecione a opção **Adicionar regra** para iniciar o assistente Proteção de Dados.
6. Siga os passos do assistente.

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

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

Importante

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

Para gerenciar as configurações de proxy, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Geral** localizado no lado esquerdo do menu e depois no separador **Configurações**.
4. Na seção **Definições de Proxy**, ative o uso de proxy clicando no botão.
5. Clique no link **Gerenciar proxies**.
6. Existem duas opções para definir as configurações de proxy:
   - **Importar configurações de proxy do navegador padrão** - configurações de proxy do usuário atual, extraídas do navegador padrão. Se o servidor proxy requer um nome de usuário e uma senha, você deve especificá-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 usuário** - digite um nome de usuário reconhecido pelo proxy.
  - **Senha do proxy** - digite a senha válida para o usuário especificado anteriormente.

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

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

5. Proteção Antivírus

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

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

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

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

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

  Com Análise Automática ligada, não há praticamente nenhuma necessidade de executar manualmente análises em busca de malware.A Análise Automática irá analisar o seu computador várias vezes, executando as ações adequadas quando o malware é detectado.A Análise Automática é executada apenas quando estão disponíveis recursos do sistema suficientes, para não tornar lento o seu computador.

O Bitdefender analisa automaticamente qualquer mídia removível que esteja conectada ao computador para garantir um acesso seguro.Para mais informações, por favor consulte em "*Análise automática de mídia removível*" (p. 49).

Os utilizadores avançados podem configurar as exclusões da análise se não quiserem que certos arquivos ou tipos de arquivos sejam analisados.Para mais informações, por favor consulte em "*Configurar exceções da análise*" (p. 51).

Quando detecta um vírus ou outro malware, o Bitdefender irá tentar remover automaticamente o código de malware do arquivo e reconstruir o arquivo original.Esta operação é designada por desinfecção.Os arquivos que não podem ser desinfectados são movidos para a quarentena de modo a conter a infecção.Para mais informações, por favor consulte em "*Gerenciar arquivos em quarentena*" (p. 53).

Se o seu computador estiver infectado com malware, por favor consulte "*Remover malware do seu sistema*" (p. 84).Para ajudá-lo a remover o malware do computador que não pode ser removido no sistema operacional Windows, o Bitdefender lhe

fornece o Modo de Recuperação.Este é um ambiente confiável especialmente concebido para a remoção de malware, o que lhe permite inicializar o computador independentemente do Windows.Quando o computador estiver sendo executado no Modo de Recuperação, o malware do Windows fica inativo, tornando-se mais fácil a sua remoção.

Para protegê-lo contra aplicativos maliciosos desconhecidos, o Bitdefender utiliza o Controle Ativo de Vírus, uma tecnologia heurística avançada, a qual monitora continuamente os aplicativos em execução no seu sistema.O Controle Ativo de Vírus bloqueia automaticamente aplicativos que exibem comportamento semelhante a malware para impedi-los de danificar o seu computador.Ocasionalmente, aplicativos legítimos podem ser bloqueados. Em tais situações, você pode configurar o Controle Ativo de Vírus para não bloquear os aplicativos novamente, criando regras de exclusão.Para saber mais, favor consultar "*Controle de Vírus Ativo*" (p. 54).

Muitas formas de malware são projetados para infectar sistemas, explorando as suas vulnerabilidades, tais como ausência de atualizações do sistema operacional ou aplicativos desatualizados.O Bitdefender ajuda a identificar facilmente e a resolver vulnerabilidades do sistema para tornar o seu computador mais seguro contra malware e hackers.Para mais informações, por favor consulte em "*Reparar vulnerabilidades do sistema*" (p. 57).

5.1. Análise no acesso (proteção em tempo real)

O Bitdefender providencia uma proteção contínua e em tempo-real, contra todo tipo de ameaças de malware ao analisar os arquivos acessados, e as comunicações feitas através de aplicaticos de software de Mensagens Instantâneas (ICQ, NetMeeting, Yahoo! Messenger, MSN Messenger).

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

5.1.1. Verificação de malware detetado pela análise no acesso

Para verificar o malware detectado por análise no acesso, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Eventos** na parte superior da barra de ferramentas.
3. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Análises de Vírus**.Aqui poderá encontrar todos os eventos de análise malware, incluindo ameaças detectadas na análise no acesso, análises iniciadas pelo usuário e alterações de status para as análises automáticas.

4. Clique no evento para visualizar detalhes sobre o mesmo.

5.1.2. Ajustar o nível de proteção em tempo real

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

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

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Proteção**.
4. Arraste o cursor pela escala para definir o nível de protecção pretendido.Utilize a descrição do lado direito da escala para escolher o nível de protecção que melhor se adequa às suas necessidades de segurança.

5.1.3. Criar um nível de proteção personalizado

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

Para criar um nível de proteção personalizado, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Proteção**.
4. Clique em **Personalizar**.
5. Configure as definições de análise como necessário.
6. Clique em **OK** para guardar as alterações e fechar a janela.

Poderá achar esta informação útil:

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

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

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

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

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

- **Opções de análise para tráfego de correio eletrônico, Internet e mensagens instantâneas.** Para impedir que seja transferido malware para o seu computador, o Bitdefender analisa automaticamente os seguintes pontos de entrada de malware:
  - e-mails recebidos e enviados
  - tráfego da Internet
  - arquivos recebidos através de Yahoo! Messenger

  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 desactivar a análise ao correio eletrônico, Internet ou mensagens instantâneas para aumentar o desempenho do sistema.Se desactivar as respectivas opções de análise, as mensagens electrónicas e os arquivos recebidos e transferidos da Internet não serão analisados, permitindo

que arquivos infectados sejam guardados no seu computador.Esta é uma ameaça grave pois a protecção em tempo real vai bloquear o malware quando os arquivos infectados forem acedidos (abertos, movidos, copiados ou executados).

- **Verificar setor de boot.** Pode definir o Bitdefenderpara analisar os setores de saída do seu disco rígido.Este setor do disco rígido contém o código do computador necessário para iniciar o processo de reinício.Quando um vírus infecta o setor de saída, o drive pode tornar-se inacessível e você poderá não conseguir iniciar o sistema e acessar seus dados.
- **Analisar apenas arquivos novos e alterados.** Ao analisar apenas arquivos novos e modificados, pode melhorar significativamente o desempenho do seu sistema sem comprometer a sua segurança.

5.1.4. Restaurar configurações padrão

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

Para restaurar as configurações padrão de proteção em tempo real, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Proteção**.
4. Clique em **Padrão**.

5.1.5. 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. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Proteção**.
4. Clique no botão para ativar ou desativar a análise no acesso.
5. Se deseja desativar a Proteção em Tempo-real, uma janela de aviso irá aparecer.Deverá confirmar a sua escolha ao selecionar no menu durante quanto tempo deseja que a sua proteção em tempo-real fique desativada. Pode desativar a sua proteção em tempo-real durante 5, 15 ou 30 minutos, por uma hora, permanentemente ou até que o sistema reinicie.

Atenção

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

5.1.6. Ações efetuadas em malware detetado

Os arquivos detectados pela protecção em tempo real são agrupados em duas categorias:

- **Arquivos infectados.** Os arquivos detectados como infectados correspondem a uma assinatura de malware na Base de Dados de Assinaturas de Malware do Bitdefender.Por norma, o Bitdefender consegue remover o código de malware de um arquivo infectado e reconstruir o arquivo original. Esta operação é conhecida por desinfecção.

Nota

As assinaturas de malware são fragmentos de código extraídos de amostras de malware. São utilizados por programas antivírus para efectuar correspondência entre padrões e detectar malware.

A Base de Dados de Assinatura de Malware Bitdefender é uma colecção de assinaturas de malware atualizada a toda hora pelos investigadores de malware da Bitdefender.

- **Arquivos suspeitos.** Os arquivos são detectados como suspeitos pela análise heurística.Como B-HAVE é uma tecnologia de análise heurística, o Bitdefender não consegue saber se o arquivo está realmente infectado com malware.Não foi possível desinfectar os arquivos suspeitos por não estar disponível uma rotina de desinfecção.

Consoante o tipo do arquivo detectado, são tomadas automaticamente as seguintes acções:

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

Importante

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

- Se for detectado um arquivo suspeito, este será removido para a quarentena para evitar uma potencial infecção.

  Por padrão, os arquivos da quarentena são automaticamente enviados para os Laboratórios Bitdefender para serem analisados pelos pesquisadores de malware

da Bitdefender.Se a presença de malware for confirmada, é emitida uma assinatura para possibilitar a remoção do malware.

5.2. Verificação solicitada

O objetivo principal para o Bitdefender é manter seu computador livre de vírus. Isso é feito primordialmente mantendo novos vírus fora de seu computador e verificando seus e-mails e novos arquivos copiados para seu sistema.

Há o risco que um vírus já esteja alojado em seu sistema, antes mesmo de você instalar o Bitdefender. É por isso que é uma ótima idéia verificar seu computador contra vírus residentes após instalar o Bitdefender. E é definitivamente uma boa idéia verificar seu computador freqüentemente contra 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.Você pode analisar o computador sempre que desejar, executando as tarefas de análise padrão, ou as suas próprias tarefas de análise (tarefas definidas pelo usuário).Se você deseja analisar locais específicos no seu computador ou configurar as opções de análise, configure e execute uma análise personalizada.

5.2.1. Autoanálise

A Análise Automática é uma análise breve a pedido que verifica silenciosamente em todos os seus dados se existe malware e toma as ações adequadas para quaisquer infecções encontradas.A Análise Automática encontra e usa fatias de tempo quando o uso dos recursos do sistema fica abaixo de um determinado limite, para realizar análises periódicas a todo o sistema.

Vantagens do uso da Análise Automática:

- Tem quase um impacto zero no seu sistema.
- Ao pré-analisar todo o disco rígido, as futuras tarefas a pedido serão realizadas muito mais depressa.
- A análise no acesso também demorará menos tempo.

Para ativar ou desativar a Análise Automática, siga estes passos:

1. Abra a janela de Bitdefender.
2. Ir para o painel **Antivírus**.
3. Clique nos botões para ativar ou desativar a Análise Automática.

5.2.2. Procurar malware em um arquivo ou pasta

Deve analisar os arquivos e as pastas sempre que suspeitar de uma infecção.Clique com o botão direito do mouse sobre o arquivo ou pasta que você deseja analisar e selecione **Análisar com Bitdefender**.O Assistente do analisador Antivírus aparecerá e irá lhe guiar através do processo de análise.Ao final da análise, será solicitado

que você escolha as ações a serem tomadas nos arquivos detectados, caso haja algum.

5.2.3. Executar uma Análise Rápida

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

Para executar uma Análise Rápida, siga estes passos:

1. Abra a janela de Bitdefender.
2. Ir para o painel **Antivírus**.
3. Clique em **Analisar agora** e selecione **Análise Rápida** no menu pendente.
4. Siga o assistente de Análise Antivírus para completar a análise.O Bitdefender executará automaticamente as ações recomendadas nos arquivos detectados.Se ainda houver ameaças não resolvidas, será solicitado que você escolha as ações a serem tomadas com relação às mesmas.

5.2.4. Executar uma Análise Completa do Sistema

A tarefa de Análise Completa do Sistema procura em todo o computador todos os tipos de malware que ameaçam a sua segurança, tais como vírus, spyware, adware, rookits e outros.Se tiver a Análise Automática desligada, recomenda-se que execute uma Análise Completa do Sistema pelo menos uma vez por semana.

Nota

Como a **Análise completa ao sistema** realiza uma análise profunda em todo o sistema, esta pode demorar um pouco. Portanto, recomenda-se executar esta tarefa quando não estiver usando o seu computador.

Antes de executar uma análise completa ao sistema, siga as seguintes recomendações:

- Certifique-se de que o Bitdefender apresenta as assinaturas de malware atualizadas. A análise do computador com assinaturas desatualizadas pode impedir que o Bitdefender detecte novo malware encontrado desde a última atualização.Para mais informações, por favor consulte em *"Atualizar"* (p. 72).
- Encerre todos os programas abertos.

Se você deseja analisar locais específicos no seu computador ou configurar as opções de análise, configure e execute uma análise personalizada.Para mais informações, por favor consulte em *"Configuração e execução de uma análise personalizada"* (p. 43).

Para excutar uma Análise Completa ao Sistema, siga estes passos:

1. Abra a janela de Bitdefender.
2. Ir para o painel **Antivírus**.
3. Clique em **Analisar Agora** e selecione **Análise Completa ao Sistema** no menu pendente.
4. Siga o assistente de Análise Antivírus para completar a análise.O Bitdefender executará automaticamente as ações recomendadas nos arquivos detectados.Se ainda houver ameaças não resolvidas, será solicitado que você escolha as ações a serem tomadas com relação às mesmas.

5.2.5. Configuração e execução de uma análise personalizada

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

1. Abra a janela de Bitdefender.
2. Ir para o painel **Antivírus**.
3. Clique em **Analisar agora** e selecione **Análise Personalizada** no menu pendente.
4. Se quiser, pode voltar a executar uma análise personalizada anterior ao clicar na entrada correspondente na lista **Análises recentes** ou **Análises favoritas**.
5. Clique em **Adicionar Alvo**, selecione as caixas que correspondem às localizações onde deseja que se verifique a existência de malware e depois clique em **OK**.
6. Clique em **Opções de Análise** se quiser configurar as opções de análise.Uma nova janela irá aparecer.Siga esses passos:
   a. Pode facilmente configurar as opções de análise ajustando o nível de análise. Arraste o cursor ao longo da escala para definir o nível de análise pretendido.Utilize a descrição do lado direito da escala para escolher o nível de análise que melhor se adequa às suas necessidades.

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

   b. Também pode configurar as seguintes opções gerais:

      - **Executar a tarefa com prioridade Baixa.** Diminui a prioridade do processo de verificação. Você permitirá outros programas a executarem mais rapidamente e aumentar o tempo de verificação.
      - **Minimizar o Assistente de Análise para a área de notificação.** Minimiza a janela de verificação para a Área de notificação. Clique duplamente no ícone Bitdefender para abrir.

- Especifique a ação a aplicar se não forem encontradas ameaças.

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

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

Guardar uma análise personalizada nos favoritos

Quando configura e executa uma análise personalizada, esta é adicionada automaticamente a uma lista limitada de análises recentes.Se planejar voltar a usar uma análise personalizada no futuro, pode optar por guardá-la na lista de análises favoritas com um nome sugestivo.

Para guardar uma análise personalizada recentemente executada na lista de análises favoritas, siga os seguintes passos:

1. Abre a janela de configuração personalizada da análise.
   a. Abra a janela de Bitdefender.
   b. Ir para o painel **Antivírus**.
   c. Clique em **Analisar agora** e selecione **Análise Personalizada** no menu pendente.
2. Localize a análise desejada na lista **Análises recentes**.
3. Passe com o cursor do mouse sobre o nome da análise e clique no ícone para adicionar a análise à lista de análises favoritas.
4. Introduza um nome sugestivo para a análise.

As análises guardadas nos favoritos são marcadas com o ícone .Se clicar neste ícone, a análise será removida da lista de análises favoritas.

Informação sobre as opções de análise

Poderá achar esta informação útil:

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

  As aplicações (ou arquivos de programa) são muito mais vulneráveis a ataques de malware do que qualquer outro tipo de arquivos.Esta categoria inclui as seguintes extensões de arquivo: `386; a6p; ac; accda; accdb; accdc;`

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

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

  Nota

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

- **Verificar setor de boot.** Pode definir o Bitdefenderpara analisar os setores de saída do seu disco rígido.Este setor do disco rígido contém o código do computador necessário para iniciar o processo de reinício.Quando um vírus infecta o setor de saída, o drive pode tornar-se inacessível e você poderá não conseguir iniciar o sistema e acessar seus dados.
- **Analisar a Memória.** Selecione esta opção para analisar programas executados na memória do seu sistema.
- **Analisar registro.** Selecione esta opção para analisar as chaves de registro.O Registo do Windows é uma base de dados que armazena as definições de configuração e as opções para os componentes do sistema operacional Windows, bem como para os aplicativos instalados.
- **Analisar cookies.** Selecione esta opção para analisar os cookies armazenados pelos navegadores no seu computador.

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

5.2.6. Assistente do analisador Antivírus

A qualquer momento que você iniciar uma análise por demanda (por exemplo, clique com o botão direito do mouse numa pasta e selecione **Analisar com o Bitdefender**), O assistente de Análise do Bitdefender Antivirus aparecerá.Siga o assistente para concluir o processo de análise.

Nota

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

Passo 1 - Realizar Análise

Bitdefender iniciará a análise dos objectos seleccionados.Você pode ver informação em tempo real sobre o status da análise e as estatísticas (incluindo o tempo decorrido, uma estimativa do tempo restante e o número de ameaças detectadas).Para ver mais detalhes, clique no link **Mostrar mais**.

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

Parando ou suspendendo a análise. Pode parar o processo de análise a qualquer altura que desejar, fazendo clique em **Parar&**. Irá diretamente 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 comprimidos protegidos por senha. Quando é detectado um arquivo protegido por senha, dependendo das definições da análise, poderá ter de indicar a senha.Os arquivos protegidos por senha não podem ser analisados a não ser que forneça a senha.As seguintes opções estão disponíveis:

- **Senha.** Se você deseja que o Bitdefender analise o arquivo, selecione essa opção e digite a senha.Se você não sabe a senha, escolha uma das outras opções.

- **Não solicite uma senha e não analise este objeto.** Selecione essa opção para pular a análise desse arquivo.
- **Pular todos os itens protegidos por senha.** Selecione essa opção caso não deseje ser questionado sobre arquivos protegidos por senha.O Bitdefender não será capaz de os analisar, porém um registro será mantido no relatório da análise.

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

Passo 2 - Escolher ações

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

Nota

Quando você executa uma análise rápida ou uma análise completa ao sistema, o Bitdefenderirá automaticamente executar as ações recomendadas nos arquivos detectados durante a análise.Se ainda houver ameaças não resolvidas, será solicitado que você escolha as ações a serem tomadas com relação às mesmas.

Os objectos 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 objectos infectados.

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

Tomar medidas adequadas

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

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

  Os arquivos que não podem ser desinfectados são movidos para a quarentena de modo a conter a infecção.O arquivos em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.Para mais informações, por favor consulte em "*Gerenciar arquivos em quarentena*" (p. 53).

Importante

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

- **Arquivos suspeitos.** Os arquivos são detectados como suspeitos pela análise heurística.Os arquivos suspeitos não podem ser desinfectados, porque não se encontra disponível uma rotina de desinfecção. Serão removidos para a quarentena para evitar uma potencial infecção.

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

- **Arquivos que contêm arquivos infectados.**

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

Excluir

Remove os arquivos detectados do disco.

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

Não tome medida alguma

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

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

Passo 3 - Resumo

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

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

Importante

Na maioria dos casos o Bitdefender desinfecta com sucesso o arquivo infectado ou isola a infecção.No entanto, há incidências que não puderam ser automaticamente resolvidas.Se necessário, ser-lhe-á solicitado que reinicie o seu computador, para que o processo de limpeza seja completado.Para mais informações e instruções sobre

como remover manualmente o malware, por favor consulte "*Remover malware do seu sistema*" (p. 84).

5.2.7. Ver os relatórios da análise

Sempre que efectuar uma análise, é criado um relatório de análise.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 ver os registos de análise posteriormente, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Eventos** na parte superior da barra de ferramentas.
3. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Análises de Vírus**.Aqui poderá encontrar todos os eventos de análise malware, incluindo ameaças detectadas na análise no acesso, análises iniciadas pelo usuário e alterações de status para as análises automáticas.
4. Na lista de eventos, pode ver as análises que foram recentemente efetuadas.Clique no evento para visualizar detalhes sobre o mesmo.
5. Para abrir o registro de análise, clique em **Exibir registro** .O relatório da análise será aberto no seu explorador da internet.

5.3. Análise automática de mídia removível

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

Os dispositivos detectados se enquadram em uma destas categorias:

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

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

5.3.1. Como funciona?

Quando detecta dispositivos de armazenamento removíveis, o Bitdefender começa a verificar se existe malware em segundo plano (desde que a análise automática

esteja ativada para aquele tipo de dispositivo).Um ícone da análise do Bitdefender surgirá na bandeja do sistema.Você pode clicar nesse ícone para abrir a janela de análise e para visualizar o progresso da mesma.

Se o Piloto Automático estiver ativado, não será incomodado com a análise.A análise será apenas registrada 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 detectado ou isola os arquivos infectados na quarentena.Se houver ameaças não resolvidas depois da análise, será solicitado que você escolha as ações a serem tomadas com relação às mesmas.

   Nota
   Leve em conta que nenhuma ação pode ser efetuada nos arquivos que estiverem infectados ou suspeitos detectados em CDs / DVDs. Do mesmo modo, nenhuma ação pode ser tomada em arquivos infectados ou suspeitos detectados em unidades de rede mapeada se você não tiver os privilégios adequados.

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

Esta informação pode ser útil para você:

- Tenha cuidado ao usar um CD/DVD infectado com malware, porque o malware não pode ser removido do disco (é apenas para leitura).Certifique-se que a proteção em tempo real está ativada para evitar que o malware se propague no seu sistema.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 arquivos específicos devido a restrições legais ou técnicas. Exemplo disso são os arquivos guardados usando uma tecnologia patenteada (isto acontece porque o arquivo não pode ser corretamente recriado).

  Para saber como lidar com malware, por favor consulte *"Remover malware do seu sistema"* (p. 84).

5.3.2. Gerenciamento da análise de mídia removível

Para gerenciar a análise automática de mídia removível, siga estes passos:

1. Abra a janela de Bitdefender.

2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Exceções**.
4. Na seção **Analisar dispositivos detetados**, escolha que tipo de dispositivos de armazenamento deseja que sejam analisados automaticamente.Clique nos botões para ativar ou desativar a análise automática.

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

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

5.4. Configurar exceções da análise

Bitdefender permite excluir arquivos específicos, pastas ou extensões de arquivos 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 usuários com conhecimentos avançados de informática ou sob as recomendações de um representante da Bitdefender.

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

Nota

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

5.4.1. Excluir arquivos ou pastas da análise

Para excluir arquivos ou pastas específicas da análise, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Exceções**.
4. Ative as exceções de análise para os arquivos que utilizem o respetivo botão.
5. Clique no link **Arquivos e pastas excluídos**.Na janela que surge, pode gerenciar os arquivos e pastas excluídos da análise.

6. Adicionar exceções seguindo estes passos:
   a. Clique no botão **Adicionar**, localizado na parte superior da tabela de exceções.
   b. Clique em **Explorar**, selecione a pasta que deseja excluir da análise e depois clique **OK**.Alternativamente, pode digitar (ou copiar e colar) o caminho para o arquivo ou pasta no campo editar.
   c. Por predefinição, o arquivo ou pasta selecionado é excluído tanto da análise no acesso quanto na análise a pedido. Para alterar quando a exclusão deve ser aplicada, selecione uma das outras opções.
   d. Clicando **Adicionar**.
7. Clique em **OK** para guardar as alterações e fechar a janela.

5.4.2. Excluir extensões de arquivos da análise

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

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

Para excluir extensões de arquivo da análise, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Exceções**.
4. Ative as exceções de análise para os arquivos que utilizem o respetivo botão.
5. Clique no link **Extensões excluídas**.Na janela que surge, pode gerenciar o arquivo e extensões excluídos da análise.
6. Adicionar exceções seguindo estes passos:
   a. Clique no botão **Adicionar**, localizado na parte superior 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 predefinição, todos os arquivos com as extensões especificadas são excluídos da análise no acesso e a pedido. Para alterar o aplicativo da exclusão, selecione uma das outras opções.

d. Clicando **Adicionar**.

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

5.4.3. Gerenciar exclusões de análise

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

Para gerenciar as exceções da análise, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Exceções**.Use as opções na seção **Arquivos e pastas** para gerenciar as exceções de análise.
4. Para remover ou editar exceções da análise, clique em um dos links disponíveis.Proceder da seguinte forma:
   - Para eliminar um item da lista, selecione-o e clique no botão **Remover**.
   - Para editar uma entrada da lista, dê um duplo clique na mesma (ou selecione-a e clique no botão **Editar**.Aparecerá uma nova janela onde poderá alterar a extensão ou o caminho a ser excluído e o tipo de análise da qual quer que eles sejam excluídos. Faça as alterações necessárias e clique em **Modificar**.
5. Para desativar exceções da análise, utilize o respectivo botão.

5.5. Gerenciar arquivos em quarentena

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

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

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

Para verificar e gerenciar arquivos da quarentena, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.

3. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Quarentena**.
4. Os arquivos da quarentena são gerenciados automaticamente pelo Bitdefender de acordo com as predefinições da quarentena.Embora não seja recomendado, pode ajustar as definições da quarentena de acordo com as suas preferências.

   Reanalisar quarentena após a atualização de definições de vírus
   Mantenha esta opção ativada para analisar automaticamente os arquivos da quarentena após cada atualização das definições de vírus.Os arquivos limpados são movidos automaticamente de volta ao seu local original.

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

   Apagar conteúdo com mais de {30} dias
   Por definição, arquivos de quarentena mais antigos que 90 dias são automaticamente apagados.Se quiser alterar este intervalo, digite um novo valor no campo correspondente.Para desabilitar a exclusão automática dos antigos arquivos em quarentena, digite 0.
5. Para eliminar um arquivo da quarentena, seleccione-o e clique no botão **Eliminar**.Se pretende restaurar um arquivo da quarentena para a respectiva localização original, seleccione-o e clique em **Restaurar**.

5.6. Controle de Vírus Ativo

O Controle Ativo de Vírus da Bitdefender é uma tecnologia de detecção proativa inovadora que usa métodos heurísticos avançados para detectar novas e potenciais ameaças em tempo real.

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

Se o Piloto Automático estiver desativado, você será notificado através de uma janela pop-up sobre o aplicativo bloqueado.Caso contrário, o aplicativo será bloqueado sem qualquer notificação.Pode verificar quais aplicativos foram detectadas pelo Controle Ativo de Vírus na janela Eventos.

5.6.1. Verificar aplicativos detectados

Para verificar os aplicativos detectadas pelo Controlo Ativo de Vírus, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Eventos** na parte superior da barra de ferramentas.
3. Clique em **Antivirus** no menu do lado esquerdo e depois no separador **Controle de Vírus Ativo**.
4. Clique no evento para visualizar detalhes sobre o mesmo.
5. Se confiar no aplicativo, pode configurar o Controle Ativo de Vírus para não bloquea-lo mais, clicando em **Permitir e monitorar**.O Controlo Ativo de Vírus continuará a monitorar os aplicativos excluídos. Se um aplicativo excluído for detetado realizando atividades suspeitas, o evento será simplesmente registrado e comunicado à Nuvem do Bitdefender como uma detecção de erro.

5.6.2. Ligar ou desligar o Controle Ativo de Vírus

Para ativar ou desativar o Controle Ativo de Vírus, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Proteção**.
4. Clique no botão para ativar ou desativar o Controle Ativo de Vírus.

5.6.3. Ajustar proteção de Controle de Vírus Ativo

Se verificar que o Controle Ativo de Vírus detecta frequentemente aplicativos legítimos, defina um nível de proteção inferior.

Para ajustar a proteção do Controle Ativo de Vírus, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Proteção**.
4. Certifique-se de que o Controlo Ativo de Vírus esteja ligado.
5. Arraste o cursor pela escala para definir o nível de protecção pretendido.Utilize a descrição do lado direito da escala para escolher o nível de protecção que melhor se adequa às suas necessidades de segurança.

Nota

Quando define um nível de proteção superior, o Controle Ativo de Vírus irá requerer menos sinais de comportamento malware para comunicar um processo. Isto provocará um aumento do número de aplicativos que são comunicados e, ao mesmo tempo, um aumento da probabilidade de falsos positivos (aplicativos limpos detectadas como maliciosos).

5.6.4. Gerenciar processos excluídos

Pode configurar regras de exclusão para aplicativos confiáveis para que o Controle Ativo de Vírus não as bloqueie, se ações como as de malware se realizarem.O Controlo Ativo de Vírus continuará a monitorar os aplicativos excluídos. Se um aplicativo excluído for detetado realizando atividades suspeitas, o evento será simplesmente registrado e comunicado à Nuvem do Bitdefender como uma detecção de erro.

Para gerenciar o processo de exceções do Controle Ativo de Vírus, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Exceções**.
4. Clique no link **Processos excluídos**.Na janela que aparece, você pode gerir as exceções do processo de Controle Ativo de Vírus.
5. Adicionar exceções seguindo estes passos:
   a. Clique no botão **Adicionar**, localizado na parte superior da tabela de exceções.
   b. Clique em **Explorar**, procure e selecione o aplicativo que quer excluir e depois clique em **OK**.
   c. Manter a opção **Permitir** selecionada para evitar que o Controle Ativo de Vírus bloqueie o aplicativo.
   d. Clicando **Adicionar**.
6. Para remover ou editar exceções, proceda da seguinte forma:
   - Para eliminar um item da lista, selecione-o e clique no botão **Remover**.
   - Para editar uma entrada da lista, dê um duplo clique na mesma (ou selecione-a e clique no botão **Editar**.Faça as alterações necessárias, depois clique em **Modificar**.
7. Clique em **OK** para guardar as alterações e fechar a janela.

5.7. Reparar vulnerabilidades do sistema

Um passo importante na proteção do seu computador contra as pessoas e aplicações maliciosas é manter atualizado o seu sistema operacional 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, senhas fortes (senhasque não são fáceis de adivinhar) devem de ser criadas para cada conta de usuário do Windows.

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

- Poderá analisar as vulnerabilidades do sistema e corrigi-las, passo a passo, com o assistente de **Análise de Vulnerabilidade**.
- Se usar a monitorização da vulnerabilidade automática, pode verificar e resolver vulnerabilidades detectadas na janela Eventos.

Você deve verificar e corrigir vulnerabilidades do sistema a cada uma ou duas semanas.

5.7.1. Procurar vulnerabilidades no seu sistema

Para resolver vulnerabilidades do sistema usando o assistente de Análise de Vulnerabilidade, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Ir para o painel **Antivírus**.
3. Clique em **Analisar agora** e depois selecione **Análise de Vulnerabilidade**.
4. Siga o procedimento de seis passos para remover as vulnerabilidades do seu sistema.Pode navegar pelo assistente utilizando o botão **Seguinte**. Para sair do assistente, clique em **Cancelar**.

   a. **Protege seu PC**

      Seleccione as vulnerabilidades a verificar.

   b. **Verificar problemas**

      Aguarde que o Bitdefender termine a análise de vulnerabilidades ao sistema.

   c. **Atualizações do Windows**

      Pode ver a lista das atualizações criticas e não-criticas do Windows que não se encontram atualmente instaladas no seu computador.Seleccione as atualizações que pretende instalar.

      Para iniciar a instalação das atualizações selecionadas, clique em **Seguinte**.Note que a instalação das atualizações poderá demorar um pouco

e algumas delas podem exigir a reinicialização do sistema para concluir a instalação.Se necessário, reinicie o sistema quando lhe convier.

d. **Atualizações do aplicativo**

Se o aplicativo não estiver atualizado, clique no link fornecido para baiar a versão mais recente.

e. **Senhas inadequadas**

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

Clique em **Reparar** para modificar as senhas fracas.Você pode escolher entre pedir para o usuário alterar a senha no próximo login ou você mesmo alterar a senha imediatamente.Para obter uma senha forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).

f. **Sumário**

Aqui pode ver o resultado da operação.

5.7.2. Usando o monitoramento automático de vulnerabilidade

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

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

1. Abra a janela de Bitdefender.
2. Clique no botão **Eventos** na parte superior da barra de ferramentas.
3. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Vulnerabilidade**.
4. Pode ver a informação detalhada sobre as vulnerabilidades detectadas do sistema.Dependendo da incidência, para consertar uma vulnerabilidade específica, proceda da seguinte forma:
   - Se estiverem disponíveis as atualizações do Windows, clique em **Atualizar Agora** para abrir o assistente de Análise de Vulnerabilidade e instale-as.
   - Se um aplicativo estiver desatualizado, clique em **Atualizar agora** para obter a conexão com a página da Internet do fornecedor, onde poderá instalar a versão mais recente desse aplicativo.
   - Se uma conta de usuário do Windows tiver uma senha fraca, clique **Corrigir senha** para forçar o usuário a trocar a senha no próximo logon ou mude a senha você mesmo.Para obter uma senha forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).

- Se o recurso Windows Autorun estiver ativado, clique em **Desativar** para o desativar.

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

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Vulnerabilidade**.
4. Clique no botão para ativar ou desativar a Análise de Vulnerabilidade Automática.

Importante
Para ser automaticamente notificado sobre as vulnerabilidades do seu sistema e aplicativos, mantenha a **Análise Automática de Vulnerabilidades** 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 operacional Windows possui as mais recentes e importantes atualizações de segurança da Microsoft.

Atualizações Regulares do Windows
Verifique se o seu sistema operativo Windows possui as mais recentes atualizações de segurança regulares da Microsoft.

Atualizações do aplicativo
Verifique se os aplicativos cruciais relacionados com a rede e instalados no seu sistema estão atualizados.As aplicações desatualizadas podem ser exploradas por software malicioso, tornando o PC vulnerável a ataques externos.

Senhas inadequadas
Verifique se as senhas das contas Windows configuradas no sistema são fáceis de descobrir ou não.A configuração de senhas difíceis de descobrir (senhas altamente seguras) torna muito difícil a invasão do seu sistema pelos hackers.Uma senha segura inclui letras maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).

Execução automática de conteúdos multimídia
Verifique o status do recurso Windows Autorun.Esta característica permite que os aplicativos se iniciem automaticamente a partir dos CDs, DVDs, drives USB ou outros dispositivos externos.

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

Nota

Se desativar a monitoração de uma vulnerabilidade específica, as incidências relacionadas deixarão de ser registradas na janela de Eventos.

6. Controle Privacidade

A sua informação privada é um alvo constante dos ciber-criminosos.Como as ameaças se propagaram a quase todas as atividades online, o e-mail inadequadamente protegido, as mensagens instantâneas e a navegação na Rede podem conduzir a fugas de informação que comprometem a sua privacidade.

O Controle de Privacidade Bitdefender resolve todas estas ameaças com uma diversidade de componentes.

- Proteção Antiphishing - oferece um conjunto de recursos abrangente que protege toda a sua experiência de navegação na rede, protegendo-o inclusive de divulgar informação pessoal a sites fraudulentos disfarçados de legítimos.
- Proteção de Dados - ajuda a garantir que a sua informação pessoal não seja enviada do seu computador sem o seu consentimento.Analisa e-mail e mensagens instantâneas enviadas do seu computador, bem como quaisquer dados enviados via páginas da rede e bloqueia qualquer informação protegida por regras de Proteção de Dados que você tenha criado.
- Criptografia de Chat - criptografa as suas conversas de MI para garantir que os seus conteúdos permanecem entre você e a outra pessoa.
- ID theft protection - for users in the United States, Bitdefender integrates one of the most comprehensive identity theft protection solutions on the market - **ID Watchdog**.

6.1. Proteção Antiphishing

O Bitdefender Antiphishing impede que seja revelada informação pessoal enquanto explora a internet ao alertá-lo acerca das páginas web potencialmente phishing.

O Bitdefender oferece uma proteção Antiphishing em tempo-real para:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera
- Yahoo! Messenger

Para definir as configurações Antiphishing, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Controle de Privacidade** no menu do lado esquerdo e depois no separador **Antiphishing**.

As configurações estão organizadas por duas categorias.

Funções da Barra de Ferramentas

Clique nos botões para ligar ou desligar:

- Mostrar a barra de ferramentas Bitdefender no navegador da rede.
- O Consultor de procura, é um componente de classifica os resultados das pesquisas Google, Bing e Yahoo!, bem como os links do Facebook e Twitter, colocando um ícone em frente de cada resultado:

  Você não deve visitar esta página da rede.

  Esta página da rede pode ter conteúdo perigoso. Tenha cautela caso decida visitá-la.

  Esta página é segura.
- 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 para navegadores web

Clique nos botões para ligar ou desligar:

- Proteção contra fraudes.
- Proteção contra phishing.
- Proteção para mensagens instantâneas.

Você pode criar uma lista de sites que não serão analisados pelos mecanismos Antiphishing doBitdefender.A lista deve conter apenas os websites em que você confia plenamente.Por exemplo, adicione os websites onde costuma frequentemente fazer compras on-line.

Para configurar e administrar a lista branca antiphishing, clique no link **Lista Branca**.Uma nova janela irá aparecer.

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

Para remover um site desta lista, selecione-o na lista e clique no link **Remover** correspondente.

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

6.1.1. Proteção do Bitdefender no navegador da web

Bitdefender integra-se diretamente através de uma barra de tarefas intuitiva e fácil de usar nos seguintes exploradores da Internet:

- Internet Explorer
- Mozilla Firefox
- Google Chrome

- Safari
- Opera

A barra de ferramentas do Bitdefender não é a barra habitual do seu navegador.A única coisa que adiciona ao seu navegador é um pequeno arrastador no topo de cada página Web.Clique para ver a barra de ferramentas.

A barra de ferramentas Bitdefender contém os seguintes elementos:

Avaliação da Página

Dependendo de como Bitdefender classifica a página da rede que você está atualmente visualizando, uma das seguintes classificações é exibida do lado esquerdo da barra de ferramentas:

- A mensagem "Esta página não é segura" aparece com um fundo vermelho - você deve deixar a página da rede imediatamente.
- A mensagem "Recomenda-se cautela" aparece em um fundo laranja - esta página da rede pode conter conteúdo perigoso.Tenha cautela caso decida visitá-la.
- A mensagem "Esta página é segura" surge com um fundo verde - esta é uma página segura para visitar.

Sandbox

Clique para lançar o navegador em um ambiente fornecido por Bitdefender, isolando-o do sistema operacional.Isto impede que as ameaças com base no navegador explorem as vulnerabilidades do navegador para obterem o controlo do seu sistema.Use a Sandbox ao visitar as páginas da Rede sob suspeita de conterem malware.

Nota
A Sandbox não se encontra disponível em computadores com Windows XP.

Configuração

Clique em para selecionar características individuais a ativar ou desativar:

- Filtro Antiphishing
- Filtro Antimalware
- Consultor de Buscas

Interruptor

Para ativar/desativar totalmente as características da barra de ferramentas, clique em no lado direito da barra de ferramentas.

6.1.2. Alertas de Bitdefender no navegador

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

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

Você precisa decidir o que fará a seguir. Estão disponíveis as seguintes opções:

- Navegue fora da página da rede.
- Prosseguir para a página web, apesar do aviso, clicando em **eu compreendo os riscos, avançar assim mesmo** .
- Adicione a página à lista branca Antiphishing, clicando em **Adicionar à Lista Branca**.Esta página já não será analisada pelos motores Antiphishing do Bitdefender.

6.2. Proteção de Dados

A proteção de dados evita as fugas de dados sensíveis quando se encontra online.

Imagine a seguinte situação: você criou uma regra de proteção de dados para proteger o número do seu cartão de crédito.Se, de alguma forma, um software espião conseguir instalar-se no seu computador, não conseguirá enviar o número do seu cartão de crédito em e-mail, mensagens instantâneas ou páginas da Internet.Além disso, os seus filhos não poderão utilizá-lo para fazer compras pnline ou revelá-lo a pessoas que conheceram na Internet.

6.2.1. Proteção de dados

Qualquer que seja o seu e-mail o seu número de cartão de crédito, quando eles caem em mãos erradas, essa informação poderá causar-lhe danos: poderá encontrar-se afogado em mensagens spam ou poderá ser surpreendido ao acessar à sua conta e verificar que está vazia.

Baseado nas regras que criar, a Proteção de Dados analisa o tráfego da rede, de e-mail e de mensagens instantâneas que sai do seu computador em busca de sequência de caracteres específicos (por exemplo, o seu número de cartão de crédito). Se houver uma correspondência, a respectiva página da rede, e-mail ou mensagem instantânea é bloqueada.

Pode criar regras para proteger cada peça de informação que possa considerar pessoal ou confidencial, desde o seu número de telefone ou endereço de e-mail até à sua informação bancária.Suporte multi-usuário é fornecido de forma que os usuários de diferentes contas do Windows possam configurar e usar as suas próprias regras.Se a sua conta do Windows é uma conta de administrador, as regras que você criou podem sendo configuradas também para ser aplicadas quando outros usuários do computador estiverem conectados às suas contas de usuários.

6.2.2. Configurar proteção de dados

Se deseja usar a proteção de dados, siga os seguintes passos:

1. Abra a janela de Bitdefender.

2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Controle de Privacidade** no menu do lado esquerdo e depois no separador **Proteção de Dados**.
4. Certifique-se de que a proteção de dados está ativada.
5. Criar regras para proteger a sua informação sensível.Para mais informações, por favor consulte em "*Criar regras de proteção de dados*" (p. 65).

Criar regras de proteção de dados

Para criar uma regra, clique no botão **Adicionar regra** e siga o assistente de configuração.Pode navegar pelo assistente utilizando os botões **Seguinte** e **Retroceder**.Para sair do assistente, clique em **Cancelar**.

1. **Definir Tipo de Regra e Dados**

   Deve definir os seguintes parâmetros:

   - **Nome Regra** - insira o nome da regra no campo editável.
   - **Tipo de Regra** - escolha o tipo de regra (morada, nome, cartão de crédito, PIN, NSS, etc.
   - **Dados Regra** - insira os dados que quer proteger com a regra no campo editável.Por exemplo, se deseja proteger o seu número de cartão de crédito, insira o mesmo ou parte dele aqui.

     Importante
     Se inserir menos do que três caracteres, será notificado a validar os dados. Recomendamos que insira pelo menos três caracteres de forma a evitar o bloqueio por engano de mensagens e páginas web.

   Todos os dados que inserir são encriptados. Para uma segurança adicional, não insira a totalidade dos dados que deseja proteger.

2. **Selecionar Tipo de Tráfego e Usuários**

   a. Selecione o tráfego que você deseja que o Bitdefender analise.

   - **Analisar Internet (tráfego de HTTP)** - analisa o tráfego HTTP (web) e bloqueia os dados de saída que correspondem aos dados da regra.
   - **Analisar e-mail (tráfego de SMTP)** - analisa todo o tráfego SMTP (mail) e bloqueia as mensagens de e-mail de saída que contém os dados da regra.
   - **Analisar tráfego de Mensagens Instantâneas** - analisa todo o tráfego de Mensagens Instantâneas e bloqueia as mensagens de chat de saída que contenham os dados da regra.

Pode escolher aplicar a regra apenas se a mesma corresponder em todas as palavras ou se os dados da regra e os caracteres detectados correspondem em termos de letra (Maiúsculas, minúsculas).

b. Especificar os usuários os quais as regras se aplicam.

- **Somente para mim (usuário atual)** - a regra se aplicará somente à sua conta de usuário.
- **Contas limitadas de usuários** - A regra se aplicará a você e a todas as contas limitadas do Windows.
- **Todos os usuários** - a regra se aplicará a todas as contas do Windows.

3. **Descrever Regra**

Insira uma breve descrição da regra no campo de edição.Uma vez que os dados bloqueados (string de caracteres) não são mostrados em pleno texto quando se acede à regra, a descripção deverá ajudá-lo a identificá-la facilmente.

Clique em **Finalizar**.A regra aparecerá na tabela.

A partir de agora, qualquer tentativa de enviar os dados especificados (através de e-mail, mensagens instantâneas ou de uma página da Internet) falhará.Será apresentada uma entrada na janela Eventos indicando que o Bitdefender bloqueou o envio de conteúdo específico de uma identidade.

6.2.3. Gerir Regras

Para gerenciar as regras de proteção de dados:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Controle de Privacidade** no menu do lado esquerdo e depois no separador **Proteção de Dados**.

Pode ver as regras criadas até agora listadas na tabela.

Para apagar uma regra, seleccione-a e clique no botão **Remover regra**.

Para editar uma regra, selecione-a e clique no botão **Editar regra**. Uma nova janela aparecerá.Aqui pode mudar o nome, descripção e parâmetros da regra (tipo, dados e tráfego). Clique em **OK** para guardar as alterações.

6.3. Encriptação de Chat

O conteúdo das suas mensagens instantâneas deve permanecer entre si e a pessoa com quem conversa.Ao encriptar as suas conversas, tem a garantia que, se alguém tentar interceptá-las não conseguirá ler o conteúdo.

De forma padrão, Bitdefender cifra todas as suas sessões de chat desde que:

- Seu parceiro de conversa possui um produtoBitdefender instalado que suporta a Encriptação de Conversas e a mesma está habilitada para o programa de mensagens usado para conversação.
- Você e o seu parceiro de mensagens instantâneas usam Yahoo! Messenger.

Importante
Bitdefender não criptografa uma conversa se um dos parceiros usar um aplicativo de chat na Rede como o Meebo.

Para configurar a encriptação de mensagens instantâneas:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Controle de Privacidade** no menu do lado esquerdo e depois no separador **Criptografia**.

Como padrão, a criptografia de Chat é ativada.Poderá desativar a Criptografia de Chat, se clicar no botão respectivo.

6.4. ID theft protection

To protect you against identity theft, Bitdefender integrates the services of **ID Watchdog**.

Nota
This feature is available only for users in the United States.

ID Watchdog monitors and identifies changes in both public and private records such as national security watch lists, Social Security records, national phone records, criminal records, DMV and driving records, medical collections and much more.

To turn on ID Watchdog, follow these steps:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Click **Privacy Control** on the left-side menu and then the **ID theft protection** tab.
4. Turn on ID theft protection by clicking the corresponding switch.

Identity theft protection can be configured through your MyBitdefender account.Click the provided link to log in to http://my.bitdefender.com, where you can learn more about ID Watchdog and set up identity protection.

7. Mapa de Rede

O módulo de rede permite-lhe gerir os produtos Bitdefender instalados nos seus computadores em casa a partir de um só computador.

Para poder gerir os produtos Bitdefender instalados nos computadores de casa, siga os seguintes passos:

1. Ativa a rede do Bitdefender no seu computador.Defina o seu computador como **Computador Servidor**.
2. Vá a cada computador que deseja gerir e adira-o à rede (defina a senha).Defina cada computador como **Computador Normal**.
3. Volte para o seu computador e adicione os computadores que deseja gerir.

7.1. Ativar a rede do Bitdefender

Para ativar a rede doméstica do Bitdefender, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Mapa de Rede** no menu do lado esquerdo.
4. Clique em **Ativar Rede**.Será solicitado que configure a senha de gerenciamento para o mapa de rede.
5. Insira a mesma senha em cada um dos campos editáveis.
6. Defina a função do computador no mapa de rede do Bitdefender:
   - **Computador Servidor** - selecione esta opção no computador que será utilizado para gerenciar todos os outros computadores.
   - **Computador Normal** - selecione esta opção nos computadores que serão gerenciados pelo Computador Servidor.
7. Clique em **OK**.

   Pode ver o nome do computador a aparecer no mapa de rede.

   Aparece o botão **Desativar conexão**.

Nota

Também pode ativar o mapa de rede a partir da janela principal do Bitdefender:

1. Abra a janela de Bitdefender.
2. Ir para o painel **Mapa de Rede**.
3. Clique em **Gerir** e selecione **Ativar Rede** no menu pendente.

7.2. Adicionar Computadores à rede Bitdefender

Todos os computadores serão automaticamente adicionados à rede se cumprir os seguintes requisitos:

- o mapa de rede Bitdefender foi ativado nele.
- a função foi definida como Computador Normal.
- a senha definida na activação da rede é a igual à definida no Computador Servidor.

Nota

Você pode analisar o mapa de rede para encontrar os computadores que cumprem os requisitos, a qualquer momento, clicando no botão **Auto descobrir** .

Para adicionar manualmente um computador ao mapa de rede do Bitdefender a partir do Computador Servidor, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Mapa de Rede** no menu do lado esquerdo.
4. Clique em **Adicionar Computador**.
5. Insira a senha de gestão rede pessoal e clique em **OK**.Uma nova janela irá aparecer.

   Pode ver a lista dos computadores na rede.O significado do ícone é o seguinte:

    Indica um computador on-line sem produtos Bitdefender instalados.

    Indica um computador on-line com o Bitdefender instalado.

    Indica um computador offline com o Bitdefender instalado.
6. Faça uma das coisas seguintes:
   - Selecione da lista o nome do computador a adicionar.
   - Insira o endereço IP ou o nome do computador a adicionar no campo correspondente.
7. Clicando **Adicionar**.
8. Insira a senha de gerenciamento configurada no respectivo computador.
9. Clique em **OK**.Se forneceu a senha correta, a nome do computador selecionado aparecerá no mapa de rede.

7.3. Gestão da Rede Bitdefender

Depois de criar com sucesso o seu mapa de rede do Bitdefender, pode gerenciar todos os produtos Bitdefender a partir de um único Computador Servidor.

Para executar várias tarefas em todos os computadores gerenciados, siga estes passos:

1. Abra a janela de Bitdefender.
2. Ir para o painel **Mapa de Rede**.
3. Clique em **Gerenciar** e selecione os botões correspondentes no menu pendente:
   - **Desativar conexão** - permite-lhe desativar a rede.
   - **Analisar Todos** - permite-lhe analisar ao mesmo tempo todos os computadores gerenciados.
   - **Atualizar todos os computadores** - permite que você atualize todos os computadores gerenciados, ao mesmo tempo.

Antes de executar uma tarefa num computador específico, você será notificado para inserir a senha de gerenciamento local.Insira a senha de gestão rede pessoal e clique em **OK**.

Para ver todo o Mapa de Rede e acessar todas as tarefas de gerenciamento, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Mapa de Rede** no menu do lado esquerdo.

Se mover o cursor do seu mouse sobre um computador do mapa de rede, pode visualizar alguma informação sobre ele (endereço IP, número de incidências que estão afetando a segurança do sistema, o estado de registro do Bitdefender).

Se você clicar em um nome de computador no mapa da rede, você poderá ver todas tarefas administrativas que você pode executar no computador remoto.

Registrar o produto
Permite que você registre o Bitdefender neste computador digitando uma licença.

Configurar senha para as definições do produto
Permite você criar uma senha para restringir o acesso às configurações do Bitdefender neste PC.

Execute uma rotina de análise por demanda
Permite você executar uma análise por demanda num computador remoto. Você pode executar qualquer das seguintes tarefas de análise: Análise Rápida ou Análise Completa do Sistema.

Reparar tudo
Permite que você corriga ocorrências que estão afetando a segurança deste computador seguindo o assistente Corrigir Todas Ocorrências.

Atualizar agora

Inicia o processo de atualização do produto Bitdefender instalado neste computador.

Definir como Servidor de Atualizações desta rede

Permite que você defina este computador como um servidor de atualização para todos produtos Bitdefender instalados nesta rede.Usando esta opção irá reduzir o tráfego de internet, porque apenas um computador na rede irá se conectar e fazer o download das atualizações.

Remover PC do mapa de rede

Permite que você remova o PC da rede doméstica.

Nota

Se você planeja executar várias tarefas, selecione **Não me mostrem mais esta mensagem durante esta sessão**.Ao selecionar esta opção, não será notificado novamente pela senha durante esta sessão.

8. Atualizar

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

Se você se conectar a Internet através de banda-larga ou DSL, o Bitdefender se encarrega da atualização. Ele verifica novas assinaturas de vírus quando você liga o seu computador e toda **hora** depois.Se alguma atualização for detectada, esta será automaticamente baixada e instalada em seu computador.

O processo de atualização é executado "on the fly", o que significa que os arquivos são substituidos progressivamente. Desta forma, o processo de atualização não afetará o funcionamento do produto e, ao mesmo tempo, exclui qualquer possibilidade de vulnerabilidade.

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

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

- Se o seu computador se conectar à Internet através de um servidor proxy, você deve configurar as definições do proxy conforme escrito em *"Como posso configurar Bitdefender para usar um proxy de conexão à Internet?"* (p. 33).
- Se não possui uma conexão à Internet, pode atualizar Bitdefender manualmente conforme descrito em *"O meu computador não está conectado à Internet. Como posso atualizar o Bitdefender?"* (p. 80).O arquivo de atualização manual é liberado uma vez por semana.
- Podem ocorrer erros ao baixar atualizações com uma conexão lenta à Internet.Para saber como superar tais erros, consulte *"Como atualizar o Bitdefender numa ligação à Internet lenta"* (p. 79).
- Se você estiver conectado a Internet através de uma conexão discada, é uma boa idéia gerar o hábito de atualizar o Bitdefender a pedido do usuário.Para mais informações, por favor consulte em *"Efetuar uma atualização"* (p. 73).

8.1. Verifique se o Bitdefender está atualizado

Para verificar se a proteção de Bitdefender está atualizada, siga estes passos:

1. Abra a janela de Bitdefender.
2. Ir para o painel **Atualizar**.
3. O momento da última atualização é exibido abaixo do nome do painel.

Para informações mais detalhadas acerca das mais recentes atualizações, verifique os eventos de atualização:

1. Na janela principal, clique em **Eventos** na barra de ferramentas superior.
2. Clique em **Atualizar** do lado esquerdo do menu.

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.

8.2. Efetuar uma atualização

Para realizar atualizações, é necessária uma conexão à Internet.

Para iniciar uma atualização, faça o seguinte:

- Abra a janela Bitdefender, vá para o painel **Atualização** e clique em **Atualizar agora**.
- CLique com o botão direito do mouse no ícone do Bitdefender na bandeja do sistema e selecione **Atualizar Agora**.

O módulo Atualização irá conectar-se ao servidor de atualização de Bitdefender e verificará se existem atualizações.Se uma atualização é detectada, poderá ser notificado para confirmar a atualização ou a mesma é realizada automaticamente, dependendo das configurações de atualização.

Importante

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

8.3. Ligar ou desligar a atualização automática

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

1. Abra a janela de Bitdefender.
2. Ir para o painel **Atualizar**.
3. Clique no botão para ativar ou desativar a Atualização Automática.
4. Se você desativar a atualização automática, uma janela de alerta aparecerá.Você tem que confirmar a sua escolha ao selecionar no menu durante quanto tempo deseja que a atualização automática fique desativada. Você pode desativar a atualização automática durante 5, 15 ou 30 minutos, por uma hora, permanentemente ou até que o sistema reinicie.

Atenção

Esta é uma incidência de segurança critica. Recomendamos que desative a actualização automática pelo menor tempo possível. Se o Bitdefender não for

atualizado regularmente, não será capaz de proteger você contra as ameaças mais recentes.

8.4. Ajuste das configurações de atualização

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

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

Para ajustar as definições de atualização, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Atualizar** do lado esquerdo do menu.
4. Ajuste as definições de acordo com as suas preferências.

Local de atualização

Bitdefender está configurado para ser atualizado a partir dos servidores de atualização de Bitdefender na Internet.A localização de atualização é `http://upgrade.bitdefender.com`, um endereço genérico da Internet que é automaticamente redirecionado para o servidor de atualização da Bitdefender mais próximo da sua região.

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

Se instalou Bitdefender em diversos computadores na sua casa, pode configurar uma rede doméstica do Bitdefender e depois designar um dos seus computadores como servidor de atualização.É fornecida informação detalhada em *"Mapa de Rede"* (p. 68).O programa Bitdefender instalado no servidor de atualização designado fará a atualização a partir da Internet. Os programas Bitdefender em outros computadores obterão as atualizações a partir do servidor de atualiação local (o seu local de atualização é automaticamente alterado, em conformidade).Esta configuração visa minimizar o tráfego da Internet e otimizar as atualizações.

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

Regras de processamento da atualização

Pode escolher entre três formas para baixar e instalar atualizações:

- **Atualização Silenciosa** - O Bitdefender faz download automaticamente e implementa a atualização.
- **Consultar antes do download** - sempre que uma atualiação estiver disponível, você será consultado antes do download ser efetuado.
- **Avisar antes de instalar** - cada vez que uma atualização for baixada, você será consultado antes da instalação ser feita.

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

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

Atualizações P2P

Além do mecanismo de atualização normal, o Bitdefender também usa um sistema de partilha inteligente de atualização baseado no protocolo peer-to-peer (P2P) para distribuir atualizações de assinaturas de malware entre os usuários do Bitdefender.

Pode ligar ou desligar as opções de atualização P2P usando os botões correspondentes.

Usar sistema de atualização P2P

Ative essa opção para baixar as atualizações de assinaturas de malware de outros Bitdefender usuários usando o sistema de atualização P2P.Bitdefender usa as portas 8880 - 8889 para atualizações peer-to-peer.

Distribuir arquivos Bitdefender

Ative esta opção para partilhar as assinaturas de malware mais recentes disponíveis no seu computador com outros usuários do Bitdefender.

9. Proteção Safego para redes sociais

Você confia nos seus amigos online.Mas confia nos seus computadores?Use a proteção Safego nas redes sociais para proteger a sua conta e os seus amigos de ameaças online.

Safego é um aplicativo do Facebook desenvolvido pelo Bitdefender para manter a sua conta da rede social segura.O seu papel é analisar os links que recebe dos seus amigos do Facebook e monitorar as configurações de privacidade de sua conta.

Nota
A conta MyBitdefender é necessária para usar este recurso.
Para mais informações, por favor consulte em "*Registro do Produto*" (p. 8).

Estas são as características principais:

- procura automaticamente nas publicações no seu Alimentador de Notícias por links maliciosos.
- protege a sua conta contra ameaças online.

  Quando detecta uma publicação ou um comentário que seja spam, pshishing ou malware, você receberá um aviso.
- adverte seus amigos sobre links suspeitos postados no Alimentador de Notícias.
- ajuda a construir uma rede segura de amigos que usam o recurso **Avaliação de amigos**.
- obtenha uma análise do estado da segurança do sistema pela Análise Rápida do Bitdefender.

Para acessar a Safego a partir do seu produto Bitdefender, siga estes passos:

1. Abra a janela de Bitdefender.
2. Ir para o painel **Safego**.
3. Clique em **Ativar**.Será direcionado para a sua conta.

   Se já ativou Safego, poderá acessar as estatísticas sobre suas atividades clicando no botão **Ver Relatórios**.
4. Use a sua informação de acesso ao Facebook para acessar o aplicativo Safego.
5. Permitir que a Safego acesse a sua conta Facebook.

10. Resolução de Problemas

Este capítulo apresenta alguns dos problemas que poderá encontrar ao utilizar o Bitdefender e as possíveis soluções.A maioria destes problemas pode ser resolvida com a configuração correcta das definições do produto.

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 "*Suporte*" (p. 93).

10.1. 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 informações, por favor consulte em "*Como posso remover outras soluções de segurança?*" (p. 99).

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

  Se o seu computador não cumprir os Requisitos Mínimos do Sistema, ficará lento, especialmente se estiver executando multiplos aplicativos ao mesmo tempo.Para mais informações, por favor consulte em "*Requisitos mínimos do sistema*" (p. 1).

- **As unidades do seu disco rígido estão muito fragmentadas.**

A fragmentação dos arquivoos abranda o acesso aos arquivos e diminui o desempenho do sistema.

Para desfragmentar o seu disco com o sistema operativo do Windows, siga o caminho a partir do menu Iniciar: **Iniciar → Todos os Programas → Acessórios → Ferramentas do Sistema → Desfragmentador de Disco**.

10.2. 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 passos seguintes:

  1. Remover o Bitdefender totalmente do sistema:
     a. Vá para http://www.bitdefender.com/uninstall e baixe a ferramenta de desinstalação no seu computador.
     b. Execute a ferramenta de desinstalação usando privilégios de administrador.
     c. Reinicie seu computador.
  2. Reinstalar o Bitdefender no sistema.

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

  Neste caso, siga os passos seguintes:

  1. Remover a outra solução de segurança.Para mais informações, por favor consulte em "*Como posso remover outras soluções de segurança?*" (p. 99).
  2. Remover o Bitdefender totalmente do sistema:
     a. Vá para http://www.bitdefender.com/uninstall e baixe a ferramenta de desinstalação no seu computador.
     b. Execute a ferramenta de desinstalação usando privilégios de administrador.
     c. Reinicie seu computador.
  3. Reinstalar o Bitdefender no sistema.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção "*Solicite Ajuda*" (p. 94).

10.3. Já não consigo utilizar um aplicativo

Este problema ocorre quando está a tentar utilizar um programa que estava a funcionar normalmente antes de instalar o Bitdefender.

Poderá encontrar 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 módulo de Controle Activo de Vírus classifica erradamente algumas aplicações como maliciosas.

O Controle de Vírus Activo 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 Controle Activo de Vírus.

Quando isto acontece, pode excluir a respectiva aplicação da monitorização do Controle Activo de Vírus.

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

1. Abra a janela de Bitdefender.
2. Clique no botão **Definições** na parte superior da barra de ferramentas..
3. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Exceções**.
4. Clique no link **Processos Excluídos**.Na janela que aparece, você pode gerir as exceções do processo de Controle Ativo de Vírus.
5. Adicionar exceções seguindo estes passos:
   a. Clique no botão **Adicionar**, localizado na parte superior da tabela de exceções.
   b. Clique em **Explorar**, procure e selecione o aplicativo que quer excluir e depois clique em **OK**.
   c. Manter a opção **Permitir** selecionada para evitar que o Controle Ativo de Vírus bloqueie o aplicativo.
   d. Clicando **Adicionar**.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção “*Solicite Ajuda*” (p. 94).

10.4. 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. Abra a janela de Bitdefender.

2. Clique no botão **Definições** na parte superior da barra de ferramentas.
3. Clique em **Atualizar** localizado no lado esquerdo do menu e em seguida no separador **Atualizar**.
4. Sob **Atualizar regras de processamento**, selecione **Avisar antes de baixar**.
5. Clique no botão **Início** na parte superior da barra de ferramentas.
6. Ir para o painel **Atualização** e clicar em **Atualizar agora**.
7. Seleccione apenas **Atualizações das assinaturas** e clique em **Ok**.
8. O Bitdefender vai transferir e instalar apenas as atualizações das assinaturas de malware.

10.5. O meu computador não está conectado à Internet. Como posso atualizar 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 esses passos:

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

   http://www.bitdefender.com/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 usando uma versão de 32 ou 64 Bit do Windows?"* (p. 100).
3. Guarde o arquivo com o nome `weekly.exe` no sistema.
4. Mova o arquivo transferido para um dispositivo amovível, tal como uma unidade USB, e depois para o seu computador.
5. Faça duplo clique no arquivo e siga os passos do assistente.

10.6. Os Serviços do Bitdefender não estão respondendo

Este artigo ajuda você a solucionar o erro **Os Serviços do Bitdefender não estão respondendo**.Você pode encontrar esse erro da seguinte forma:

- O ícone do Bitdefender na bandeja do sistema está cinza e você recebe a informação de que os serviços do Bitdefender não estão respondendo.
- A janela do Bitdefender mostra que os serviços do Bitdefender não estão respondendo.

O erro pode ser causado por uma das seguintes condições:

- Uma importante atualização está sendo instalada.
- Erro temporário de comunicação entre os serviços do Bitdefender.
- Alguns dos serviços do Bitdefender estão parados.
- outras soluções de segurança sendo executadas em seu computador ao mesmo tempo com o Bitdefender.

Para solucionar este erro, tente estas soluções:

1. Espere um pouco e veja se alguma coisa muda.O erro pode ser temporário.
2. Reinicie o computador e aguarde alguns momentos até que o Bitdefender seja carregado. Abra o Bitdefender para ver se o erro persiste.Reiniciar o computador normalmente resolve o problema.
3. Verifique se você tem alguma outra solução de segurança instalada, pois ela poderão afetar o funcionamento do Bitdefender. Se este for o caso, recomendamos que você remova todas as outras soluções de segurança e então reinstale o Bitdefender.

   Para mais informações, por favor consulte em "*Como posso remover outras soluções de segurança?*" (p. 99).

Se o erro persistir, entre em contato com nossos representantes de suporte conforme descrito na seção "*Solicite Ajuda*" (p. 94).

10.7. A Remoção do Bitdefender falhou

Este artigo ajuda a solucionar erros que poderão ocorrer ao remover o Bitdefender.Há duas situações possíveis:

- Durante a remoção, uma tela de erros aparece.Uma tela fornece um botão para executar uma ferramenta de desinstalação que limpará o sistema.
- A remoção trava e, possivelmente, seu sistema congela.Clique **Cancelar** para abortar a remoção. Se não funcionar, reinicie o sistema.

Se a remoção falhar, algumas chaves do registro e arquivos do Bitdefender poderão permanecer em seu sistema. Estes arquivos remanescentes poderão evitar uma nova instalação do Bitdefender. Elas também podem afetar o desempenho do sistema e sua estabilidade.

Para remover completamente Bitdefender do seu sistema, siga estes passos:

1. Vá para http://www.bitdefender.com/uninstall e baixe a ferramenta de desinstalação no seu computador.
2. Execute a ferramenta de desinstalação usando privilégios de administrador.
3. Reinicie seu computador.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção "*Solicite Ajuda*" (p. 94).

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

Se instalou o Bitdefender e não consegue reiniciar o seu sistema no modo normal, são vários os motivos para este tipo de problema.

Isto é muito provavelmente causado por uma instalação anterior de Bitdefender que não foi removida adequadamente ou por outra solução de segurança que ainda se encontra no sistema.

Eis como pode resolver cada situação:

- **Você tinha o Bitdefender anteriormente e não o removeu corretamente.**

  Para resolver isto, 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. 100).
  2. Remove Bitdefender do seu sistema:
     a. Vá para http://www.bitdefender.com/uninstall e baixe a ferramenta de desinstalação no seu computador.
     b. Execute a ferramenta de desinstalação usando privilégios de administrador.
     c. Reinicie seu computador.
  3. Reinicie o seu sistema no modo normal e reinstale o 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. 100).
  2. Remove Bitdefender do seu sistema:
     a. Vá para http://www.bitdefender.com/uninstall e baixe a ferramenta de desinstalação no seu computador.
     b. Execute a ferramenta de desinstalação usando privilégios de administrador.
     c. Reinicie seu computador.
  3. Para desinstalar corretamente outro software, acesse o site do fornecedor e execute a ferramenta de desinstalação ou contate-o diretamente, para que lhe indiquem os procedimentos de desinstalação.
  4. 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. 100).
2. Usar a opção de Restauro do Sistema do Windows para restaurar o computador para uma data anterior antes de instalar o produto Bitdefender.Para saber como fazer isto, consulte "*Como posso usar o Restauro do Sistema no Windows?*" (p. 101).
3. Reinicie o sistema no modo normal e contate os nossos representantes do suporte conforme descrito na seção "*Solicite Ajuda*" (p. 94).

11. Remover malware do seu sistema

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

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

- "*Modo de Recuperação Bitdefender*" (p. 84)
- "*O que fazer se o Bitdefender encontrar vírus no seu computador?*" (p. 86)
- "*Como posso limpar um vírus num arquivo?*" (p. 87)
- "*Como posso limpar um vírus de um arquivo de correio eletrônico?*" (p. 88)
- "*O que fazer se eu suspeitar que um arquivo seja perigoso?*" (p. 89)
- "*Como limpar os arquivos infectados da Informação de Volume do Sistema*" (p. 89)
- "*O que são arquivos protegidos por senha no registro de análise?*" (p. 91)
- "*Quais são os itens ignorados no relatório de análise?*" (p. 91)
- "*O que são arquivos muito comprimidos no registro de análise?*" (p. 91)
- "*Por que é que o Bitdefender eliminou automaticamente um arquivo infectado?*" (p. 92)

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 "*Suporte*" (p. 93).

11.1. 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 operacional.

Depois de instalar o Bitdefender Antivirus Plus 2012, o Modo de Recuperação pode ser usado mesmo que você não consiga inicializar no Windows.

Iniciar o seu sistema no Modo de Recuperação

Você pode entrar no Modo de Recuperação de duas formas:

Na janela de Bitdefender.

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

1. Ir para o painel **Antivírus**.
2. Clique em **Analisar Agora** e selecione **Modo de Recuperação** no menu pendente.

   Aparecerá uma janela de confirmação. Clique em **Sim** para inicializar o seu computador.
3. Após a reinicialização do computador, aparecerá um menu solicitando que você selecione um sistema operacional.Escolha **Imagem de Recuperação Bitdefender** e prima a tecla **Enter** inicializar num ambiente do Bitdefender onde poderá limpar a sua partição Windows.
4. Se notificado, pressione **Enter** e selecione a resolução de tela mais próxima da que você normalmente usa.Depois pressione novamente **Enter**.

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

Inicialize o seu computador diretamente no Modo de Recuperação

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

Nota

Este método não se encontra disponível em computadores com Windows XP.

1. Inicie / reinicie o seu computador e comece a pressionar a tecla **espaços** do seu teclado antes de aparecer o logo do Windows.
2. Um menu aparecerá solicitando que você selecione um sistema operacional para iniciar.Pressione **TAB** para ir para a área de ferramentas.Escolha **Imagem de Recuperação Bitdefender** e prima a tecla **Enter** inicializar num ambiente do Bitdefender onde poderá limpar a sua partição Windows.
3. Se notificado, pressione **Enter** e selecione a resolução de tela mais próxima da que você normalmente usa.Depois pressione novamente **Enter**.

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

Analisar o seu sistema no Modo de Recuperação

Para 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. 84).
2. O logo do Bitdefender surgirá e os motores antivírus começarão a ser copiados.
3. Uma janela de boas-vindas aparecerá.Clique em **Continuar**.
4. Iniciou-se uma atualização de assinaturas antivirus.

5. Quando a atualização estiver concluída, a janela da Análise-a-pedido do Bitdefender surgirá.
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, você lida com nomes de partições do tipo do Linux.As partições do disco surgirão como `sda1` provavelmente correspondendo à `(C:)` partição do Windows, `sda2` correspondendo a `(D:)` e assim sucessivamente.

7. Aguarde 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 mouse numa área vazia do Ambiente de Trabalho, selecione **Sair** no menu que aparece e depois escolha entre reiniciar ou encerrar o computador.

11.2. 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 Minuciosa ao Sistema.

Assim que a análise completa terminar, selecione a ação pretendida para os itens infectados (Desinfectar, Eliminar, Mover para a Quarentena).

Atenção

Se suspeitar que o arquivo faz parte do sistema operativo do Windows ou que não é um arquivo infectado, não siga estes passos e contacte e Apoio ao Cliente do Bitdefender assim que possível.

Se não for possível efectuar a ação seleccionada e o relatório da análise indicar uma infecção que não foi possível eliminar, tem de remover o(s) arquivo(s) manualmente:

O primeiro método pode ser utilizado no modo normal:

1. Desative a proteção antivírus em tempo real do Bitdefender:

a. Abra a janela de Bitdefender.

b. Clique no botão **Definições** na parte superior da barra de ferramentas.

c. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Proteção**.

d. Clique no botão para desligar **análise no acesso**.

2. Mostrar objectos ocultos no Windows.Para saber como fazer isto, consulte "*Como posso mostrar objetos ocultos no Windows?*" (p. 101).
3. Procure a localização do arquivo infectado (veja no relatório da análise) e elimine-o.
4. Active a protecção 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. 100).
2. Mostrar objectos ocultos no Windows.
3. Procure a localização do arquivo infectado (veja no relatório da análise) e elimine-o.
4. Reinicie o seu sistema e inicie sessão no modo normal.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção "*Solicite Ajuda*" (p. 94).

11.3. Como posso limpar um vírus num arquivo?

Um arquivo é um arquivo ou um conjunto de arquivos comprimidos num formato especial para reduzir o espaço no disco necessário para armazenar os arquivos.

Alguns destes formatos são formatos livres, possibilitando ao Bitdefender a opção de analisar o conteúdo e aplicar as acções adequadas para os remover.

Outros formatos de arquivo estão parcial ou totalmente fechados, mas o Bitdefender só pode detectar a presença de vírus no interior, mas não pode aplicar outras acções.

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

Pode limpar um vírus armazenado num arquivo da seguinte forma:

1. Identifique o arquivo que contém o vírus realizando uma Análise Minuciosa ao Sistema.
2. Desative a proteção antivírus em tempo real do Bitdefender:

a. Abra a janela de Bitdefender.

b. Clique no botão **Definições** na parte superior da barra de ferramentas.

c. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Proteção**.

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 arquivo infectado.
5. Elimine o arquivo original de modo a garantir que a infecção é totalmente removida.
6. Comprima novamente os arquivos num novo arquivo com uma aplicação de arquivo, como o WinZip.
7. Ative a proteção antivírus em tempo real do Bitdefender e execute uma 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 foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção "*Solicite Ajuda*" (p. 94).

11.4. Como posso limpar um vírus de um arquivo de correio eletrônico?

O Bitdefender também pode identificar vírus em bases de dados de correio eletrônico e arquivos de correio eletrônico armazenados no disco.

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

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

1. Analisar a base de dados do correio eletrônico com o Bitdefender.
2. Desative a proteção antivírus em tempo real do Bitdefender:

a. Abra a janela de Bitdefender.

b. Clique no botão **Definições** na parte superior da barra de ferramentas.

c. Clique em **Antivírus** localizado no lado esquerdo do menu e depois clique no separador **Proteção**.

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 eletrônico.
4. Elimine as mensagens infectadas.A maioria dos clientes de correio eletrônico move a mensagem eliminada para uma pasta de recuperação, a partir da qual pode ser recuperada.Deve certificar-se que a mensagem também é eliminada desta pasta de recuperação.
5. Compactar a pasta com a mensagem infectada.
   - No Outlook Express:No menu Arquivo, clique em Pasta e, depois em Compactar Todas as Pastas.
   - No Microsoft Outlook:No menu Arquivo, clique em Gestão de Arquivos de Dados.Seleccione os arquivos das pastas (.pst) que pretende compactar e clique em Definições.Clique em Compactar.
6. Active a protecção antivírus em tempo real do Bitdefender.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção "*Solicite Ajuda*" (p. 94).

11.5. O que fazer se eu suspeitar que um arquivo seja perigoso?

Você pode suspeitar que um arquivo do seu sistema é perigoso, embora o seu produto Bitdefender não o tenha detectado.

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

1. Execute uma **Análise Completa ao Sistema** com o Bitdefender.Para saber como fazer isto, consulte "*Como posso analisar o meu sistema?*" (p. 30).
2. Se o resultado da análise parece estar limpo, mas você ainda tem dúvidas e quer verificar o arquivo, entre em contato com os representantes do suporte para que possamos ajudá-lo.

   Para saber como fazer isto, consulte "*Solicite Ajuda*" (p. 94).

11.6. Como limpar os arquivos infectados da Informação de Volume do Sistema

A pasta de Informação de Volume do Sistema é uma zona no seu disco rígido criada pelo Sistema Operativo e utilizada pelo Windows para armazenar informações essenciais relacionadas com a configuração do sistema.

Os motores do Bitdefender podem detectar qualquer arquivo infectado armazenado na Informação de Volume de Sistema mas, sendo esta uma área protegida, poderá não conseguir removê-lo.

Os arquivos infectados detectados nas pastas do Restauro do Sistema aparecerão no relatório da análise da seguinte forma:

`?:\Informação de Volume de Sistema\_restore{B36120B2-BA0A-4E5D-…`

Para remover total e imediatamente o(s) arquivo(s) infectado(s) do armazém de dados, desactive e reactive o recurso do Restauro do Sistema.

Se o Restauro do Sistema estiver desativado, todos os pontos de restauro são removidos.

Quando o Restauro do Sistema é novamente ativado, são criados novos pontos de restauro consoante as necessidades do agendamento e de eventos.

Para desactivar o Restauro do Sistema, siga os seguintes passos:

- **Para o Windows XP:**
  1. Siga este caminho: **Iniciar** → **Todos os Programas** → **Acessórios** → **Ferramentas do Sistema** → **Restauro do Sistema**
  2. Clique em **Definições do Restauro do Sistema**, na lado esquerdo da janela.
  3. Seleccione a caixa **Desactivar o Restauro do Sistema** em todas as unidades e clique em **Aplicar**.
  4. Quando receber a notificação que todos os Pontos de Restauro serão eliminados, clique em **Sim** para continuar.
  5. Para activar o Restauro do Sistema, desmarque a caixa **Desactivar o Restauro do Sistema** em todas as unidades e clique em **Aplicar**.
- **Para Windows Vista:**
  1. Siga o seguinte caminho: **Iniciar** → **Painel de Controle** → **Sistema e Manutenção** → **Sistema**
  2. No painel da esquerda, clique em **Protecção do Sistema**.

     Se lhe for pedida a senha de administrador ou a confirmação, escreva a senha ou dê a confirmação.
  3. Para desactivar a Restauração do Sistema, desmarque as caixas de seleção de cada unidade e clique em **Ok**.
  4. Para activar o Restauro do Sistema, desmarque as caixas de seleção de cada unidade e clique em **Ok**.
- **Para o Windows 7:**
  1. Clique em **Iniciar**, clique com o botão direito em **Computador** e clique em **Propriedades**.
  2. Clique na hiperligação da **Protecção do sistema** no painel da esquerda.

3. Nas opções da **Protecção do Sistema**, seleccione a letra de cada unidade e clique em **Configurar**.
4. Seleccione **Desactivar protecção do sistema** e clique em **Aplicar**.
5. Clique em **Eliminar**, clique em **Continuar** quando pedido e, depois, clique em **Ok**.

Se esta informação não foi útil, você pode contatar a Bitdefender para suporte, como descrito na seção "*Solicite Ajuda*" (p. 94).

11.7. O que são arquivos protegidos por senha no registro de análise?

Isto é apenas uma notificação que indica que o Bitdefender detectou que estes arquivos estão protegidos por senha ou por outra forma de encriptação.

Normalmente, os itens protegidos por senha são:

- Arquivos que pertencem a outras solução de segurança.
- Arquivos que pertencem ao sistema operativo.

Para analisar verdadeiramente os conteúdos, estes arquivos têm de ser extraídos ou de outra forma descodificados.

Se estes conteúdos pudessem ser extraídos, o verificador em tempo real do Bitdefender analisaria-os automaticamente para manter o seu computador protegido.Se pretende analisar esses arquivos com Bitdefender, terá de contactar o fabricante do produto para receber mais informações sobre esses arquivos.

Recomendamos que ignore estes arquivos pois não constituem uma ameaça ao seu sistema.

11.8. Quais são os itens ignorados no relatório de análise?

Todos os arquivos que aparecem como Ignorados no relatório de análise estão limpos.

Para um melhor desempenho, o Bitdefender não analisa arquivos que não tenham sido alterados desde a última análise.

11.9. O que são arquivos muito comprimidos no registro de análise?

Os itens sobre-comprimidos são elementos que não puderam ser extraídos pelo motor de análise ou elementos para os quais a desencriptação levaria muito tempo, tornando o sistema instável.

Sobre-comprimido significa que o Bitdefender não realizou a análise a esse arquivo pois a descompactação iria consumir muitos recursos do sistema. O conteúdo será analisado aquando o acesso em tempo real, se necessário.

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

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

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

Este é, normalmente, o caso de arquivos de instalação que são transferidos de sítios de Internet suspeitos.Se se encontrar numa situação assim, transfira o arquivo de instalação do sítio de Internet do fabricante ou de outro sítio fiável.

12. Ajuda

12.1. Suporte

A Bitdefender esforça-se por fornecer aos seus clientes um nível de suporte rápido e eficaz.Se encontrar algum problema ou se tiver alguma questão sobre o nosso produto Bitdefender, pode utilizar vários recursos em linha para encontrar rapidamente uma solução ou resposta.Ou, se preferir, pode contactar a equipa de Apoio ao Cliente da Bitdefender. Os nossos técnicos de apoio responderão atempadamente às suas questões e dar-lhe-ão a ajuda que precisar.

12.1.1. Recursos online

Estão disponíveis vários recursos em linha para o ajudar a resolver problemas e a responder a questões relacionados com o Bitdefender.

- Centro de Suporte Bitdefender:http://www.bitdefender.com/help
- Fórum de Suporte Bitdefender:http://forum.bitdefender.com
- o portal de segurança informática Malware City:http://www.malwarecity.com

Também pode utilizar o seu motor de busca favorito para saber mais sobre a segurança de computadores, os produtos Bitdefender e a empresa.

Centro de Suporte Bitdefender

O Centro de Suporte do Bitdefender é um repositóio de informação online sobre os produtos Bitdefender.Armazena, num formato facilmente acessível, relatórios sobre os resultados do suporte técnico em curso e atividades de correção de falhas do suporte e equipas de desenvolvimento do Bitdefender, além de artigos mais gerais sobre prevenção de vírus, gestão de soluções do Bitdefender com explicações detalhadas e muitos outros artigos.

O Centro de Suporte da Bitdefender está aberto ao público e é acessado com freqüência.A informção extensiva que ele contêm é mais um meio de proporcionar aos clientes do Bitdefender as informações técnicas e o conhecimento de que necessitam.Todos os pedidos de informação válidos ou relatórios de falhas oriundos de clientes do Bitdefender são eventualmente direcionados para o Centro de Apoio do Bitdefender, como relatórios de correção de falhas, fichas de resolução de problemas ou artigos informativos como suplemento dos arquivos de ajuda.

O Centro de Suporte da Bitdefender encontra-se disponível a qualquer hora http://www.bitdefender.com/help.

Fórum de Suporte Bitdefender

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

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

Os técnicos de 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 **Protecção Casa & Casa/Escritório** para acessar à secção dedicada aos produtos de consumidor.

Portal Malware City

O portal Malware City é uma excelente fonte de informações relacionadas com segurança informática. Aqui, pode ficar a conhecer as várias ameaças a que o seu computador fica exposto quando ligado à Internet (malware, phishing, spam, cibercriminosos).Um dicionário útil que ajuda a compreender os termos de segurança informática que não conhece.

Os novos artigos são publicados regularmente para o manter atualizado sobre as últimas ameaças descobertas, as actuais tendências de segurança e outras informações sobre a indústria de segurança informática.

A página de Internet do Malware City é http://www.malwarecity.com.

12.1.2. Solicite Ajuda

A seção **Resolução de Problemas** providencia a informação necessária com relação às incidências mais frequentes que poderá encontrar ao utilizar este produto.

Se não encontrar a solução para o seu problema nos recursos disponibilizados, pode contactar-nos directamente:

- “Contacte-nos diretamente do seu produto Bitdefender” (p. 95)
- “Contate-nos através do nosso Centro de Suporte Online” (p. 95)

Importante

Para contactar o Apoio ao Cliente da Bitdefender é necessário registrar o seu produto Bitdefender.Para mais informações, por favor consulte em “*Registro do Produto*” (p. 8).

Contacte-nos diretamente do seu produto Bitdefender

Se possuir uma conexão ativa com a Internet, você pode entrar em contato com o suporte do Bitdefender diretamente da interface do produto.

Siga esses passos:

1. Abra a janela de Bitdefender.
2. Clique no link **Ajuda e Suporte**, localizado no canto inferior direito da janela.
3. Você tem as seguintes opções:
   - Leia os artigos ou os documentos e experimente as soluções propostas.
   - Inicie uma procura na nossa base de dados para encontrar a informação que precisa.
   - Use o botão **Contatar suporte** para ativar a Ferramenta de Suporte e contatar o Departamento de Atendimento 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 e-mail.
        ii. Digite o seu nome completo.
        iii. Escolha o seu país a partir do menu correspondente.
        iv. Introduza a descrição do problema que encontrou.
     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.

Contate-nos através do nosso Centro de Suporte Online

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

1. Vá para http://www.bitdefender.com/help.O Centro de Suporte doBitdefender armazena inúmeros artigos que contém soluções para as questões relacionadas ao Bitdefender.
2. Selecione o seu produto na coluna do lado esquerdo e pesquise no Centro de Suporte Bitdefender artigos que poderão fornecer a solução para o seu problema.
3. Leia os artigos ou os documentos e experimente as soluções propostas.

4. Se a solução não resolver o problema, utilize a hiperligação no artigo para contactar o Apoio Técnico Bitdefender.
5. Entre em contato com os representantes do suporte do Bitdefender por e-mail.

12.2. Informação sobre contato

Comunicação eficiente é a chave para um negócio de sucesso. Nos últimos 10 anos a BITDEFENDER estabeleceu uma reputação indiscutível excedendo as expectativas dos clientes e parceiros, sempre buscando uma melhor comunicação. Por favor, não hesite em nos contactar sobre quaisquer assuntos ou dúvidas que você possa ter.

12.2.1. Endereços da Rede

Departamento de Vendas: vendas@bitdefender.com.br
Centro de Suporte:http://www.bitdefender.com/help
Documentação: documentation@bitdefender.com
Distribuidores locais:http://www.bitdefender.com/partners
Programa de parcerias: partners@bitdefender.com
Relações com a mídia: pr@bitdefender.com
Carreiras: jobs@bitdefender.com
Apresentação de Vírus: virus_submission@bitdefender.com
Envio de spam: spam_submission@bitdefender.com
Relato de abuso: abuse@bitdefender.com
Site Web:http://www.bitdefender.com

12.2.2. 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/site/Partnership/list/.
2. As informações de contatos com os distribuidores locais do Bitdefender devem ser apresentados automaticamente. Se isto não acontecer, selecione o país em que reside para visualizar a informação.
3. Se não encontrar um distribuidor Bitdefender no seu país, não hesite em contactar-nos por correio eletrônico através do endereço sales@bitdefender.com.Por favor, escreva a sua mensagem em inglês para podermos responder imediatamente.

12.2.3. Escritórios Bitdefender

Os escritórios Bitdefender estão prontos a responder quaisquer dúvidas na respectiva área de operação, comercialmente e assuntos gerais. Seus endereços respectivos estão listados abaixo.

E.U.A

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
Telefone (escritório&vendas): 1-954-776-6262
Vendas: sales@bitdefender.com
Suporte Técnico: http://www.bitdefender.com/help
Página da Web http://www.bitdefender.com

UK e Irlanda

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
E-mail: info@bitdefender.co.uk
Fone: +44 (0) 8451-305096
Vendas: sales@bitdefender.co.uk
Suporte Técnico: http://www.bitdefender.com/help
Página da Web http://www.bitdefender.co.uk

Alemanha

Bitdefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Escritório: +49 2301 91 84 0
Vendas: vertrieb@bitdefender.de
Suporte Técnico: http://kb.bitdefender.de
Página da Web http://www.bitdefender.de

Espanha

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
Fax: +34 93 217 91 28
Fone: +34 902 19 07 65
Vendas: comercial@bitdefender.es

Suporte Técnico: http://www.bitdefender.es/ayuda
Website: http://www.bitdefender.es

Romênia

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
Fax: +40 21 2641799
Telefone de Vendas: +40 21 2063470
E-mail de vendas: sales@bitdefender.ro
Suporte Técnico: http://www.bitdefender.ro/suport
Website: http://www.bitdefender.ro

13. Informações Úteis

Este capítulo apresenta alguns procedimentos importantes que tem de considerar antes de começar a fazer o diagnóstico de um problema técnico.

Resolver um problema técnico do Bitdefender requer alguns conhecimentos do Windows, por isso os passos seguintes estão quase totalmente relacionados com o sistema operativo do Windows.

13.1. Como posso remover outras soluções de segurança?

A principal razão para utilizar uma solução de segurança é proporcionar protecção 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 2012 detecta 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:

- Para o **Windows XP**:
  1. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Adicionar/Remover Programas**.
  2. Aguarde alguns momentos até que a lista do software instalado seja apresentada.
  3. Encontre o nome do programa que pretende remover e seleccione **Remover**.
  4. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.
- Para o **Windows Vista** e o **Windows 7**:
  1. Clique em **Iniciar**, vá ao **Painel de Controle** e faça duplo clique sobre **Programas e Recursos**.
  2. Aguarde alguns momentos até que a lista do software instalado seja apresentada.
  3. Encontre o nome do programa que pretende remover e seleccione **Desinstalar**.

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

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

13.2. Como posso reiniciar no Modo de Segurança?

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

Para iniciar o Windows no Modo de Segurança:

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

13.3. Estou usando 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:

- Para o **Windows XP**:
  1. Clique em **Iniciar**.
  2. Localize o **Meu Computador** no menu **Iniciar**.
  3. Clique com o botão direito em **Meu Computador** e seleccione **Propriedades**.
  4. Se estiver indicada a **Edição x64** na secção **Sistema**, está a executar a versão de 64 bit do Windows XP.

     Se não estiver indicada a **Edição x64** você está executando a versão de 32 bit do Windows XP.

- Para o **Windows Vista** e o **Windows 7**:
  1. Clique em **Iniciar**.
  2. Localize o **Computador** no menu **Iniciar**.
  3. Clique com o botão direito em **Computador** e seleccione **Propriedades**.
  4. Procure na secção **Sistema** a informação sobre o seu sistema.

13.4. Como posso usar o Restauro do Sistema no Windows?

Se não conseguir iniciar o computador no modo normal, pode inicializa-lo no Modo de Segurança e usar o Restauro do Sistema para restaura-lo em um momento em que consiga inicializar o computador sem erros.

Para executar o Restauro do Sistema, você deve estar conectado no Windows como um administrador.

Para usar o Restauro do Sistema, siga os seguintes passos:

- No Windows XP:
  1. Inicie o Windows no Modo de Segurança.
  2. Siga este caminho a partir do menu iniciar do Windows: **Iniciar** → **Todos os Programas** → **Ferramentas do Sistema** → **Restauro do Sistema**.
  3. Na página **Benvindo ao Restauro do Sistema**, clique para selecionar a opção **Restaurar o meu computador para um momento anterior** e depois clique em Seguinte.
  4. Siga os passos do assistente e você poderá inicializar o sistema no modo normal.
- No Windows Vista e Windows 7:
  1. Inicie o Windows no Modo de Segurança.
  2. Siga este caminho a partir do menu iniciar do Windows: **Todos os Programs** → **Acessórios** → **Ferramentas do Sistema** → **Restauro do Sistema**.
  3. Siga os passos do assistente e você poderá inicializar o sistema no modo normal.

13.5. Como posso mostrar objetos ocultos no Windows?

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

Siga os seguintes passos para mostrar objectos ocultos no Windows:

1. Clique em **Iniciar**, vá ao **Painel de Controle** e seleccione **Opções de Pastas**.
2. Abra o separador **Ver**.

3. Seleccione **Mostrar conteúdo das pastas de sistema** (apenas para o Windows XP).
4. Seleccione **Mostrar arquivos e pastas ocultos**.
5. Desmarque **Ocultar extensões de arquivos nos tipos de arquivo conhecidos**.
6. Desmarque **Ocultar arquivos protegidos do sistema operativo**.
7. Clique em **Aplicar** e depois em **Ok**.

Glossário

ActiveX

ActiveX é um modelo para escrever programas para que outros programas e seus sistemas operacionais possam buscá-los. A tecnologia ActiveX é usada com o Microsoft Internet Explorer para fazer páginas da Web interativas que se parecem e se comportam como programas de computador, melhor que páginas estáticas. Com o ActiveX, usuários podem perguntar ou responder questões, apertar botões e interagir de outras formas com a página. Controles ActiveX são também escritos usando Visual Basic.

O ActiveX é notável para uma completa falta de controles de segurança; especialistas em segurança de computador desencorajam seu uso pela Internet.

Adware

O Adware é sempre combinado com um programa host sem custo enquanto o usuário concordar em aceitar o adware. Não existem implicações neste tipo de instalação, pois o usuário concordou com o propósito do aplicativo.

No entanto, propagandas do tipo “pop-up” podem se tornar uma inconveniência, e em alguns casos afetar a performance do seu sistema. Além disto, a informação que alguns destes programas coleta pode causar problemas de privacidade para usuários que não estão totalmente cientes do funcionamento do programa.

Área de Notificação

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 acessar aos detalhes e controles.

Arquivo

Um disco, fita ou diretório que contém arquivos que podem ter sido gravados como backup.

Um arquivo que contém um ou mais arquivos em formato comprimido.

Arquivo de relatório

Um arquivo que lista as ações que ocorreram. Por exemplo Bitdefender mantém um arquivo de relatório com uma lista dos caminhos verificados, as pastas, o número de arquivos e arquivos comprimidos verificados, quantos arquivos infectados e suspeitos foram encontrados.

Assinatura de vírus

É um padrão binário de vírus, utilizado pelo programa antivírus para detectar e eliminar os vírus.

Atualizar

Uma nova versão do programa ou driver do produto projetado para substituir uma versão antiga do mesmo produto. Além disso, as rotinas de instalação verificam se uma versão mais antiga está instalada no seu computador, caso contrário, você não poderá instalar a atualização.

O Bitdefender possui um módulo de atualização que permita a você verificar manualmente por atualizações ou deixa que ele automaticamente atualize o produto.

Backdoor

Um furo na segurança do sistema deixado deliberadamente pelos desenvolvedores os mantenedores. A motivação para tais furos não pe sempre sinistra, alguns sistemas operacionais, por exemplo, saem com contas privilegiadas para uso em campo para serviço dos técnicos ou programa de manutenção dos programadores do fabricante.

Caminho

As direções exatas de um arquivo em um computador. Estas direções são descritos geralmente por mídia do sistema de arquivamento hierárquico de cima para baixo.

A rota entre dois pontos quaisquer, com os canais de comunicação entre dois computadores.

Cliente de e-mail

É um aplicativo que lhe permite enviar e receber e-mails.

Cookie

Dentro da indústria da Internet, os cookies são descritos como pequenos arquivos de texto que contém informações sobre computadores individuais que podem sendo analisados e usados pelos anunciantes para rastrear gostos e interesses on-line. Nesse reino, a tecnologia de cookies está sendo desenvolvida ainda e a intenção é direcionar os anúncios diretamente aos seus interesses. É uma espada de dois gumes para muitos porque por um lado é eficiente e pertinente porque só vê anúncios que interessam a você. E por outro lado, envolve “rastrear” e “seguir” a onde você vai e onde está clicando. Compreensível assim, existe um debate sobre a privacidade e muitas pessoas que se sentem ofendidas pelo fato de serem observados com um número SKU (você sabe, o código de barras na parte traseira dos pacotes que são lidos na saída do supermercado). Embora esse ponto de vista possa ser extremo, em alguns casos é exato.

Download

Copiar dados (geralmente um arquivo inteiro) de uma fonte principal para um periférico. O termo é muitas vezes usado para descrever o processo de copiar um arquivo de um serviço on-line para seu próprio computador. Download também pode se referir a copiar um arquivo de um servidor de rede para um computador na rede.

E-mail

Correio eletrônico. Um serviço que envia mensagens para computadores em redes locais ou mundiais.

Eventos

Uma ação ou ocorrência detectada por um programa. Eventos podem ser ações de usuários, tais como clicar com botão do mouse ou pressionar uma tecla, ou ocorrências do sistema, como sem memória.

Extensão do arquivo

É a parte do arquivo, após o ponto final, indica o tipo de dados que estão armazenados no arquivo.

Muitos sistemas operacionais usam extensões de arquivos, ex. Unix, VMS, MS-DOS. Eles são usualmente de uma a três letras e / ou números (alguns sistemas operacionais antigos não suportam mais que três). Exemplos: "c" para códigos em C, "ps" para PostScript, "txt" para texto.

Falso positivo

Ocorre quando a verificação identifica um arquivo infectado quando de fato não está.

Heurística

Um método baseado em regras para identificar novos vírus. Esse método de verificação não se baseia em definições de vírus específicas. A vantagem da verificação heurística é que ela não é enganada por uma nova variante do vírus. Entretanto. Entretanto ela pode relatar um código suspeito em um programa normal, gerando assim um chamado "falso positivo".

IP

Um protocolo roteável no conjunto do protocolo TCP/IP que é responsável pelo endereçamento IP, roteamento, e fragmentação e montagem dos pacotes IP.

Itens para inicializar

Qualquer arquivo colocado nessa pasta será executado quando o computador iniciar. Por exemplo uma tela de boas-vindas, um arquivo de som, um aviso de calendário ou um aplicativo pode sendo um item para inicializar.

Java applet

Um programa em Java que é projetado para sendo executado somente em uma página web. Para usar um aplicativo em uma página web, você deve especificar o nome do aplicativo e o tamanho (comprimento e largura em pixels) que o aplicativo pode utilizar. Quando a página da web é acessada, o navegador descarrega-a de um servidor e executa na máquina do usuário (o cliente). Os aplicativos diferem dos programas em que eles são comandados por um protocolo estrito de segurança.

Por exemplo, mesmo um aplicativo funcione em um cliente, eles não podem ler ou escrever dados na máquina do cliente. Adicionalmente, os aplicativos são mais restringidos de modo que só podem ler e escrever dados nos domínios aos quais servem.

Keylogger

Um keylogger é um aplicativo que registra tudo o que é digitado.

Os keyloggers não são por natureza maliciosos. Podem ser usados com objetivos legítimos, tais como monitorar a atividade de funcionários ou das crianças. No entanto, são cada vez mais usados por cibercriminosos com objetivos maliciosos (por exemplo, para recolher dados privados, tais como credenciais de acesso e números da segurança social).

Linha de comando

Na interface de linha de comando, os usuários digitam os comando em um espaço fornecido diretamente na tela usando comandos da linguagem.

Memória

São áreas internas de armazenamento do computador. O termo memória identifica o armazenamento de dados que vem em forma de chips. Todo computador vem com uma certa quantidade de memória física, geralmente referida com memória RAM.

Não heurística

Esse método de verificação confia em definições de vírus específicas. A vantagem da verificação não heurística é que ela não pode ser enganada por algo pode parecer um vírus, e não gera falsos alarmes.

Navegador

Termo simplificado para navegador da web, um programa utilizado para localizar e exibir páginas da Internet. Os dois mais populares são Netscape Navigator e Microsoft Internet Explorer. Ambos são navegadores gráficos o que significa que podem exibir tanto gráficos como texto. Em adição, os navegadores mais modernos podem apresentar informações multimídia, como som e vídeo, através de plugins para alguns formatos.

Phishing

O ato de enviar e-mail a um usuário declarando falsamente ser uma empresa legítima em uma tentativa de enganar o usuário a entregar informações que serão usadas para roubo de identidade. O e-mail direciona o usuário a uma página web onde é perguntado a fornecer informação pessoal, tais como senhas, cartão de crédito, cadastros e contas em bancos, que a empresa legítima em questão já possui. A página web, no entanto, é falsa e existe apenas para roubar informação do usuário.

Porta

Uma interface no computador na qual você pode conectar um dispositivo. Computadores pessoais possuem vários tipos de portas. Internamente, existem vários tipos de portas conectando unidades de disco, monitores e teclados. Externamente, os computadores pessoais possuem portas conectando modems, impressoras, mouse e outros dispositivos periféricos.

Em redes TCP/IP e UDP, um ponto final a uma conexão lógica. A número da porta identifica que tipo de porta é. Por exemplo, porta 80 é usada para tráfego HTTP.

Programas comprimidos

Um arquivo em formato comprimido. Muitos sistemas operacionais e aplicativo contêm comandos que permitem a você comprimir um arquivo de modo que ocupe menos memória. Por exemplo: suponha que você tenha um texto que contém dez caracteres de espaço consecutivos. Normalmente, isso requereria dez bytes de armazenamento.

Entretanto, um programa que compacta arquivos substituiria os caracteres de espaço por caractere especial série-espaço seguido do número de espaços que estão sendo substituídos. Esta é apenas uma técnica de compactação, existem muitas outras.

Rootkit

Um rootkit é um pacote de ferramentas de software que proporcionam um nível de acesso de administrador a um sistema. O termo foi usado em primeiro lugar nos sistemas operativos UNIX e referia-se a ferramentas recompiladas que proporcionavam aos intrusos direitos de administração, permitindo-lhes ocultar a sua presença de forma a não serem vistos pelos administradores do sistema.

O papel principal dos rootkits é ocultar processos, arquivos, logins e registos. Eles também podem interceptar dados dos terminais, ligações de rede ou periféricos, se eles incorporarem o software para tal.

Os rootkits não são maliciosos por natureza. Por exemplo, os sistemas e mesmo algumas aplicações ocultam arquivos críticos usando rootkits. No entanto, eles são essencialmente utilizados para ocultar malware ou para esconder a presença de um intruso no sistema. Quando combinados com o malware, os rootkits são

uma grande ameaça à integridade e segurança de um sistema. Eles podem monitorizar tráfego, criar backdoors no sistema, alterar arquivos e relatórios e evitarem ser detectados.

Script

Outro termo para um arquivo de macro ou arquivo de comandos, um script é uma lista de comandos que podem ser executados sem a interação do usuário.

Setor de boot

O setor de boot é um setor no começo de cada disco que identifica a arquitetura do disco (tamanho do setor, tamanho do cluster, e assim por diante). Para inicializar os discos, o setor de boot também um programa que carrega o sistema operacional.

Spam

Lixo eletrônico em forma de mensagens. Normalmente conhecido como e-mail não solicitado.

Spyware

Qualquer software que coleta informação do usuário através da conexão de Internet sem o seu consentimento, normalmente para propósitos de propaganda. Aplicativos spyware são tipicamente distribuídos de forma oculta juntamente com programas freeware ou shareware que podem ser baixados da Internet; no entanto, deve ser notado que a maioria dos programas shareware e freeware não apresentam spyware. Uma vez instalado, o spyware monitora a atividade do usuário na Internet e transmite essa informação de forma oculta para outra pessoa. O spyware pode coletar também endereços de e-mail e até mesmo número de cartões de crédito e senhas.

A similaridade do spyware com o cavalo de tróia é que o usuário instala algo que não deseja instalando algum outro produto. Um modo comum de se tornar uma vítima de spyware é baixar alguns programas de compartilhamento de arquivos (peer-to-peer) que estão disponíveis hoje em dia.

Colocando de lado as questões de ética e privacidade, o spyware prejudica o usuário consumindo memória do computador e conexão com a Internet quando manda a informação de volta a sua base usando a conexão de Internet do usuário. Porque o spyware usa a memória e os recursos do sistema, os aplicativos sendo executados podem levar o sistema ao colapso ou instabilidade geral.

TCP/IP

Transmission Control Protocol/Internet Protocol - Protocolo de controle de transmissão / protocolo da Internet. Um conjunto de protocolos largamente utilizados na Internet que fornece comunicação através de redes de computadores interconectadas com diversas arquiteturas de hardware e vários

sistemas. O TCP/IP inclui padrões de como os computadores comunicam e convenções para conexões da rede e roteamento de tráfego.

Trojan

Um programa destrutivo que oculta um aplicativo benigno. Ao contrário do vírus, um cavalo de tróia não se replica mas pode ser muito destrutivo. Um dos tipos mais incidentes de cavalos de tróia é um programa que diz se livrar dos vírus do seu computador, mas ao invés disso ele introduz vírus em seu computador.

O termo vem da estória de Ilíada de Homero, na qual os gregos deram um cavalo de madeira gigante seus inimigos, os Troianos como uma oferta de paz. Mas depois dos troianos arrastarem o cavalo para dentro dos muros da cidade, os soldados Gregos saíram furtivamente da barriga do cavalo e abriram os portões da cidade, permitindo que seus compatriotas derrubassem e capturassem Tróia.

Unidade de disco

É uma máquina que lê e escreve dados em um disco.

Uma unidade de disco rígido lê e escreve em um disco rígido.

Uma unidade de disquete acessa disquetes.

Os discos rígidos podem ser internos (armazenado dentro do computador) ou externos (armazenado em uma caixa separada que está conectada ao computador).

Virus

Um programa ou uma parte do código que é carregado no seu computador sem o seu conhecimento e se executa contra a sua vontade. A maioria dos vírus pode também se duplicar. Todos os computadores são feitos pelo homem. Um simples vírus pode fazer uma cópia dele mesmo repetidamente é fácil de se produzir. Mesmo um simples vírus é perigoso porque pode rapidamente usar toda memória disponível a fazer os sistema parar. O tipo de vírus mais perigoso é aquele que é capaz de transmitir-se através de uma rede ou contornando sistemas de segurança.

Vírus de boot

Um vírus que infecta o setor de boot do disco rígido ou de um disquete. Uma tentativa de inicialização com um disquete infectado com vírus de boot fará com que o vírus se torne ativo na memória. Toda vez que você reiniciar seu sistema daquele ponto em diante, você terá um vírus ativo na memória.

Vírus de macro

Um tipo de vírus de computador que é codificado como uma macro dentro de um documento. Muitas aplicações, como Microsoft Word e Excel, suportam poderosa linguagem de macro.

Essas aplicações permitem a você colocar uma macro em um documento, e mandam a macro ser executada cada vez que o documento é aberto.

Vírus polimórfico

Um vírus que muda sua forma cada vez que um arquivo é infectado. Como não têm nenhum padrão binário consistente, tais vírus são duros de identificar.

Worm

Um programa que se propaga pela rede, se reproduzindo enquanto isso. Ele não pode se anexar a outros programas.