


Redes



Produção:

cert.br nic.br cgi.br

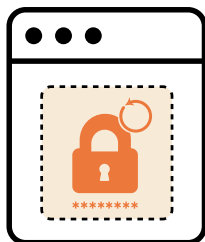
FAÇA SUA PARTE: PROTEJA SUA REDE



Quando você acessa a Internet a partir de sua casa, sua comunicação depende de equipamentos de rede, como *modem*, roteador e ponto de acesso. Cuidar da segurança deles é fundamental para proteger seus dados, sua privacidade e também a Internet como um todo.

Veja aqui dicas de como proteger sua rede.

ALTERE A SENHA DE ADMINISTRAÇÃO DOS EQUIPAMENTOS



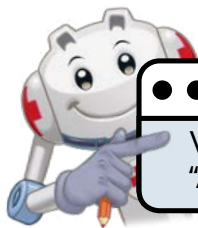
Dispositivos de rede, como *modems* e roteadores, costumam vir de fábrica com senhas padrão que podem ser descobertas por atacantes. Trocar a senha dificulta a invasão, a instalação de *malware* e a alteração das configurações do equipamento.

» Use senha forte e longa

» Evite usar em sua senha:

- informações pessoais
- sequências de teclado
- informações do equipamento, como marca, modelo e endereço MAC

» Anote e guarde a nova senha em lugar seguro



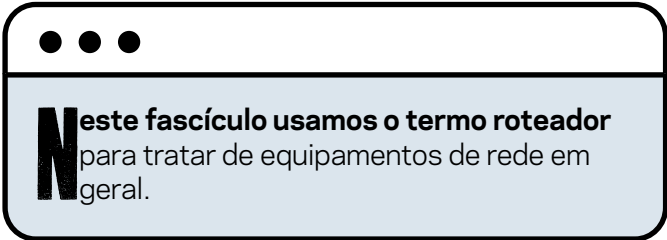
Veja mais dicas no fascículo
"Autenticação".

VOCÊ SABIA?

Modem, roteador e ponto de acesso são necessários para que o acesso à Internet funcione. Cada um tem uma função:

- o *modem* estabelece a conexão da Internet com sua rede
- o roteador conecta os dispositivos de sua rede e faz a comunicação de dados com o *modem*
- o ponto de acesso permite que seus dispositivos Wi-Fi se conectem à rede

As três funcionalidades podem estar em um único equipamento ou em equipamentos separados.



Neste fascículo usamos o termo roteador para tratar de equipamentos de rede em geral.

USE SENHA FORTE NA REDE WI-FI

Se alguém descobrir a senha de sua rede Wi-Fi, poderá se conectar a ela sem seu conhecimento, deixar a conexão lenta, propagar *malware* para seus dispositivos e/ou coletar informações sobre você, por exemplo.

» Troque a senha padrão do Wi-Fi

- senhas padrão podem ser facilmente descobertas na Internet

» Mude a senha caso:

- desconfie que tenha sido descoberta
- algum dispositivo que se conecta ao Wi-Fi tenha sido furtado



TROQUE O NOME PADRÃO DA REDE WI-FI

Usar nome (SSID) padrão em sua rede Wi-Fi pode facilitar a invasão da rede, pois certas informações podem levar à identificação de vulnerabilidades conhecidas. Além disso, nomes conhecidos podem levar seus dispositivos a se conectarem, por engano, a outras redes inseguras.

» Crie um nome único, exclusivo

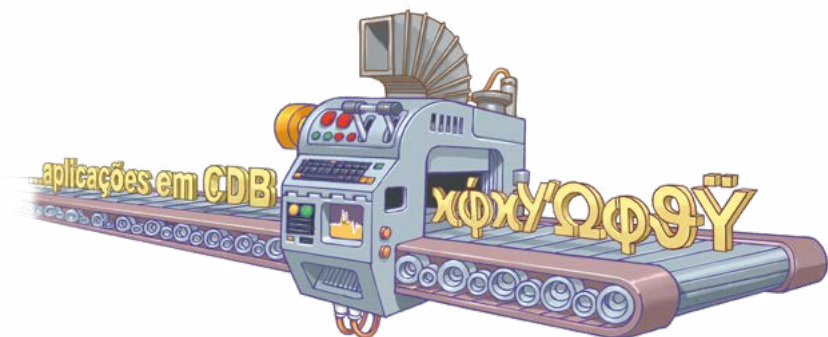
» Não use informações pessoais, como nome, número da casa ou apartamento

- isso pode facilitar a ação de assaltantes

» Evite incluir:

- dados sobre o equipamento, como marca, modelo ou endereço MAC
- nome do provedor de acesso

USSID (*Server Set Identifier*) é o nome da rede Wi-Fi. Normalmente, os SSID padrão estão descritos na lateral do roteador ou embaixo dele.

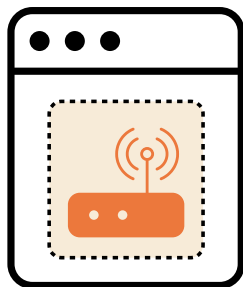


ATIVE CRIPTOGRAFIA NA REDE WI-FI

Criptografia protege o tráfego entre seus dispositivos e seu roteador para que os dados não sejam entendidos por atacantes. Faz também a autenticação dos dispositivos que podem acessar a rede Wi-Fi.

» **Escolha a versão mais atual:**

- **prefira WPA3 ou WPA2/WPA3**
- **não use WEP ou WPA**



MANTENHA O ROTEADOR ATUALIZADO

Equipamentos de rede também precisam de atualizações de *software* para corrigir vulnerabilidades de segurança. Sem essas correções, atacantes podem explorar falhas para ganhar acesso à sua rede ou invadir seu roteador para usá-lo em atividades maliciosas, como atacar outras redes.

- » **Ative a atualização automática**, sempre que possível
- » Para o roteador fornecido pelo provedor de Internet, tente saber como as atualizações são feitas
 - talvez seja necessário reiniciá-lo periodicamente para receber as atualizações



O *software* dos equipamentos é conhecido também como *firmware*.



ATIVE O FIREWALL DE REDE

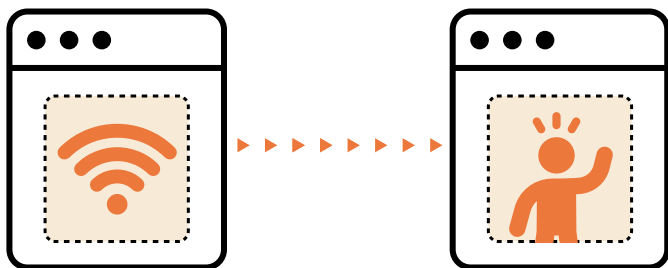
O *firewall* **protege sua rede contra ataques vindos da Internet.** Ele bloqueia conexões não autorizadas de entrada para o roteador e outros dispositivos em sua rede.

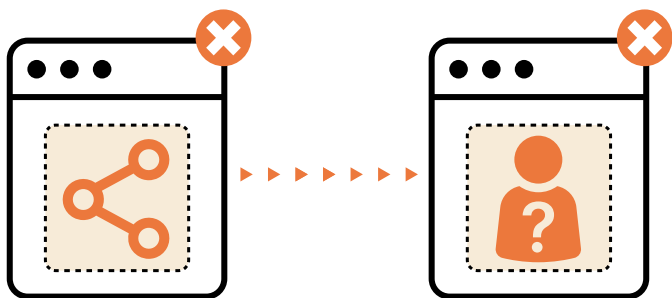
» Assegure-se de que o *firewall* está ativado

USE UMA REDE PARA CONVIDADOS

Se algum visitante pedir para usar sua Internet ou se você precisar conectar dispositivos potencialmente inseguros, é melhor mantê-los separados para que acessem apenas a Internet e não os demais dispositivos na rede da sua casa.

- » **Ative a rede para convidados (guest),**
se disponível
- » Configure-a para que os clientes fiquem isolados
 - sem comunicação entre eles, nem acesso à rede local
- » **Ative a criptografia e escolha uma senha exclusiva**
 - não use a mesma senha de sua rede principal

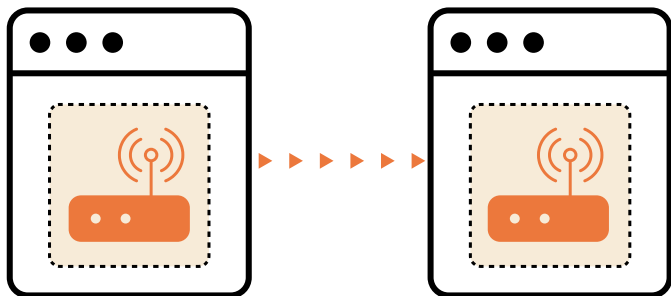




EVITE COMPARTILHAR SUA REDE COM TERCEIROS

Permitir que outras pessoas utilizem sua rede Wi-Fi pode comprometer sua privacidade e a segurança de seus dispositivos e dados, pois elas podem estar com dispositivos infectados. Além disso, **você pode ser responsabilizado por ações feitas por meio de sua rede.**

- » **Compartilhe somente com pessoas de confiança**
 - idealmente, use a rede para convidados



AVALIE SEGREGAR A REDE

Em uma rede doméstica padrão, os dispositivos podem se comunicar entre si sem restrições, o que pode facilitar a captura de dados e a propagação de *malware*. Segregar a rede ajuda a reduzir esses riscos e controlar melhor o acesso.

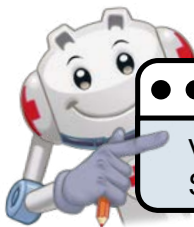
- » Considere instalar um roteador interno separado
 - configure o roteador do provedor de acesso para modo *bridge*
- » Crie segmentos de rede conforme o uso
 - ex: geral, trabalho remoto, automação residencial, filhos etc.
- » Ajuste as regras de *firewall* para que não haja comunicação de dados entre os segmentos (segregação)

CONSIDERE USAR CONTROLE PARENTAL NO ROTEADOR



Alguns roteadores têm a opção de controle parental para que pais e responsáveis possam controlar as atividades de seus filhos na Internet, incluindo limite de tempo de uso e filtros por conteúdo.

- » Adicionalmente, explore outras opções de controle parental disponíveis nos dispositivos usados pelas crianças
- » Lembre-se de conversar com as crianças sobre o uso seguro e responsável da Internet



Veja mais dicas no guia "Internet Segura - para seus filhos".



SAIBA MAIS

- » Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança para Internet, disponíveis em: **<https://cartilha.cert.br/>**
- » Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores. Confira em: **<https://internetsegura.br/>**

cert.br

O CERT.br (<https://cert.br/>) é um Grupo de Resposta a Incidentes de Segurança (CSIRT) de responsabilidade nacional de último recurso, mantido pelo NIC.br. Além da gestão de incidentes, também atua na conscientização sobre os problemas de segurança, na consciência situacional e transferência de conhecimento, sempre respaldado por forte integração com as comunidades nacional e internacional de CSIRTs.

nic.br

O Núcleo de Informação e Coordenação do Ponto BR – NIC.br (<https://nic.br/>) é uma entidade civil de direito privado e sem fins de lucro, encarregada da operação do domínio .br, bem como da distribuição de números IP e do registro de Sistemas Autônomos no País. Conduz ações e projetos que trazem benefícios à infraestrutura da Internet no Brasil.

cgi.br

O Comitê Gestor da Internet no Brasil (<https://cgi.br/>), responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados.