



A Segurança de Dados nas Redes Wi-Fi e Alternativas de Conexões

Data Security in Wi-Fi Networks and Alternative Connections

Luciano Paulino da Silva

Graduação Tecnológica em Gestão de Tecnologia da Informação pela UNICESUMAR, Pós-Graduação em Gestão de Tecnologia da Informação pela UVA, TAE - Técnico Administrativo da UFRJ.

Resumo: A expansão das tecnologias de comunicação sem fio transformou as redes Wi-Fi em uma das principais formas de acesso à Internet e aos recursos de redes locais. Atualmente, smartphones, notebooks, tablets, televisores inteligentes, dispositivos de Internet das Coisas (IoT) e equipamentos corporativos utilizam redes sem fio para comunicação e compartilhamento de informações. Entretanto, a praticidade proporcionada pelo Wi-Fi também amplia a superfície de ataque e introduz riscos relacionados à interceptação de tráfego, acesso não autorizado, ataques de engenharia social, pontos de acesso fraudulentos, exploração de vulnerabilidades e comprometimento de dispositivos. Este estudo apresenta uma análise da segurança de dados em redes Wi-Fi, abordando os fundamentos das redes IEEE 802.11, os principais mecanismos de proteção, a evolução dos protocolos WEP, WPA, WPA2 e WPA3, os riscos associados às redes públicas, a importância da segmentação, autenticação, atualização de equipamentos, monitoramento e conscientização dos usuários. Também são discutidas as relações entre segurança de redes sem fio e proteção de dados pessoais no contexto brasileiro, especialmente diante das exigências estabelecidas pela Lei Geral de Proteção de Dados Pessoais (LGPD). A pesquisa caracteriza-se como bibliográfica e documental, utilizando livros, normas técnicas, documentos institucionais e legislação. Conclui-se que a segurança de uma rede Wi-Fi não depende exclusivamente da utilização de uma senha, mas de um conjunto de controles técnicos e administrativos aplicados durante todo o ciclo de vida da infraestrutura.

Palavras-chave: Wi-Fi; IEEE 802.11; segurança da informação; segurança de redes; WPA3; Proteção de Dados; LGPD.

Abstract: The expansion of wireless communication technologies has made Wi-Fi networks one of the main means of accessing the Internet and local network resources. Smartphones, notebooks, tablets, smart televisions, Internet of Things (IoT) devices and corporate equipment currently use wireless networks for communication and information sharing. However, the convenience provided by Wi-Fi also increases the attack surface and introduces risks related to traffic interception, unauthorized access, social engineering attacks, fraudulent access points, vulnerability exploitation, and device compromise. This article analyzes data security in Wi-Fi networks, addressing the fundamentals of IEEE 802.11 networks, the main protection mechanisms, the evolution of WEP, WPA, WPA2, and WPA3 protocols, the risks associated with public networks, and the importance of network segmentation, authentication, equipment updates, monitoring, and user awareness. The relationship between wireless network security and personal data protection in Brazil is also discussed, particularly in light of the requirements established by the Brazilian General Data Protection Law (LGPD). The research is characterized as bibliographic and documentary, based on books, technical standards, institutional documents, and legislation. It is concluded that Wi-Fi network security does not depend exclusively on the use of a password, but rather on a set of technical and

administrative controls applied throughout the infrastructure life cycle.

Keywords: Wi-Fi; IEEE 802.11; information security; network security; WPA3; Data Protection; LGPD.

INTRODUÇÃO

A comunicação sem fio tornou-se parte essencial da infraestrutura tecnológica contemporânea. A utilização de redes Wi-Fi está presente em residências, empresas, instituições de ensino, hospitais, estabelecimentos comerciais, aeroportos, hotéis e espaços públicos. A possibilidade de conectar equipamentos sem a necessidade de cabeamento proporciona mobilidade, facilidade de instalação e flexibilidade para usuários e organizações.

A tecnologia Wi-Fi está relacionada à família de padrões IEEE 802.11, desenvolvida para permitir comunicação de dados por meio de ondas de rádio. De acordo com Souppaya e Scarfone (2012), uma rede local sem fio (Wireless Local Area Network – WLAN) é composta por dispositivos que se comunicam por radiofrequência dentro de determinada área geográfica, sendo sua segurança dependente da proteção de componentes como pontos de acesso, dispositivos clientes e equipamentos de infraestrutura durante todo o ciclo de vida da rede.

Apesar de suas vantagens, uma rede sem fio apresenta características particulares de segurança. Em uma rede cabeada, o acesso físico ao meio de transmissão normalmente exige que o indivíduo tenha acesso a uma porta ou ao cabeamento. No ambiente sem fio, entretanto, o sinal de rádio pode ultrapassar os limites físicos do ambiente onde o ponto de acesso está instalado. Dessa forma, um atacante localizado nas proximidades pode tentar identificar redes, explorar configurações inadequadas, realizar ataques de autenticação ou utilizar um ponto de acesso fraudulento para induzir usuários a se conectarem.

É importante destacar que o simples fato de uma rede Wi-Fi estar protegida por senha não significa que ela esteja completamente segura. A segurança depende do protocolo de proteção utilizado, da qualidade da senha, da configuração do equipamento, das atualizações de firmware, do isolamento entre clientes, da segmentação da rede, do controle de acesso e da segurança dos próprios dispositivos conectados.

A proteção também deve considerar os dados pessoais que trafegam ou são tratados por meio da infraestrutura. No Brasil, a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), estabelece que os agentes de tratamento devem adotar medidas técnicas e administrativas capazes de proteger dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas. Dessa maneira, a segurança de redes Wi-Fi deve ser compreendida como parte de uma estratégia mais ampla de segurança da informação e proteção de dados.

OBJETIVOS

Objetivo Geral

Analisar os principais riscos de segurança associados às redes Wi-Fi e apresentar medidas técnicas e administrativas capazes de reduzir vulnerabilidades e proteger os dados transmitidos e armazenados por meio dessas redes.

Objetivos Específicos

- Apresentar os fundamentos das redes Wi-Fi e do padrão IEEE 802.11;
- Analisar a evolução dos mecanismos de segurança utilizados em redes sem fio;
- Identificar os principais riscos associados às redes Wi-Fi públicas e privadas;
- Discutir as características de segurança dos protocolos WEP, WPA, WPA2 e WPA3;
- Apresentar medidas de proteção para redes domésticas e corporativas;
- Abordar a importância da segmentação e do controle de acesso;
- Analisar a importância das atualizações de firmware e sistemas;
- Discutir ataques relacionados a redes Wi-Fi;
- Relacionar a segurança das redes sem fio à proteção de dados pessoais;
- Apresentar a importância da conscientização e do treinamento dos usuários.

METODOLOGIA

Este trabalho caracteriza-se como uma pesquisa de natureza qualitativa, com abordagem exploratória, desenvolvida por meio de pesquisa bibliográfica e documental.

A pesquisa bibliográfica foi realizada a partir de livros relacionados à segurança da informação, redes de computadores e criptografia. A pesquisa documental utilizou normas técnicas, documentos de instituições especializadas em segurança cibernética, legislação brasileira e documentos técnicos relacionados às redes sem fio.

Entre as principais fontes utilizadas estão documentos do National Institute of Standards and Technology (NIST), documentos da Autoridade Nacional de Proteção de Dados (ANPD), legislação brasileira e publicações técnicas relacionadas aos protocolos de comunicação segura. A abordagem adotada busca relacionar os aspectos tecnológicos da segurança Wi-Fi com os princípios de confidencialidade, integridade, disponibilidade, autenticação e controle de acesso.

REDES WI-FI

Wi-Fi é uma tecnologia de comunicação sem fio baseada na família de padrões IEEE 802.11. Diferentemente de uma tecnologia específica de acesso à Internet, o Wi-Fi pode ser utilizado para estabelecer comunicação entre dispositivos dentro de uma rede local, permitindo o compartilhamento de arquivos, impressoras, serviços, aplicações e acesso à Internet.

Uma infraestrutura Wi-Fi básica normalmente possui um ponto de acesso (Access Point – AP), que permite a comunicação entre os dispositivos sem fio e a infraestrutura de rede. Em ambientes residenciais, é comum que o equipamento fornecido pelo provedor de Internet reúna funções de modem, roteador, switch e ponto de acesso.

Cada rede sem fio pode possuir um identificador denominado Service Set Identifier (SSID), que é o nome apresentado aos usuários durante a busca por redes disponíveis. O padrão IEEE 802.11 passou por diversas gerações e atualizações, resultando em melhorias de velocidade, eficiência espectral, capacidade, latência e segurança. Tecnologias comercialmente conhecidas como Wi-Fi 5, Wi-Fi 6 e Wi-Fi 6E estão associadas a diferentes versões da família 802.11.

O funcionamento das redes sem fio depende da utilização do espectro de radiofrequência. As faixas de 2,4 GHz e 5 GHz são amplamente utilizadas, enquanto a faixa de 6 GHz passou a ser utilizada em implementações mais recentes. A utilização simultânea de diferentes redes e dispositivos pode provocar interferência e congestionamento, principalmente na faixa de 2,4 GHz. Entretanto, interferência e segurança são problemas diferentes. A interferência pode comprometer o desempenho e a estabilidade da comunicação, enquanto uma vulnerabilidade de segurança pode comprometer a confidencialidade, integridade ou disponibilidade dos dados.

PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO NAS REDES WI-FI

A segurança das redes Wi-Fi pode ser analisada a partir dos princípios tradicionais da segurança da informação.

Confidencialidade

A confidencialidade busca garantir que as informações sejam acessíveis apenas às pessoas ou sistemas autorizados.

Em uma rede Wi-Fi, a criptografia exerce papel fundamental nesse processo. Protocolos de segurança modernos procuram impedir que terceiros consigam compreender o conteúdo das comunicações mesmo quando conseguem capturar sinais de rádio.

Integridade

A integridade busca assegurar que os dados não sejam alterados de maneira indevida durante sua transmissão ou armazenamento.

Mecanismos criptográficos de autenticação e integridade permitem identificar alterações não autorizadas nos dados.

Disponibilidade

A disponibilidade garante que sistemas e informações permaneçam acessíveis quando necessários.

Nas redes Wi-Fi, problemas de interferência, congestionamento, falhas de equipamentos, ataques de negação de serviço e configurações inadequadas podem comprometer a disponibilidade.

Autenticidade

A autenticidade está relacionada à capacidade de verificar se determinado usuário, equipamento ou serviço é realmente quem afirma ser.

Esse princípio é especialmente importante em redes corporativas, nas quais mecanismos como IEEE 802.1X e servidores de autenticação podem ser utilizados para controlar o acesso dos usuários.

EVOLUÇÃO DA SEGURANÇA: WEP, WPA, WPA2 E WPA3

A segurança das redes Wi-Fi evoluiu significativamente desde as primeiras implementações do padrão 802.11.

WEP

O Wired Equivalent Privacy (WEP) foi um dos primeiros mecanismos de proteção utilizados em redes sem fio. Entretanto, diversas fragilidades criptográficas foram identificadas, tornando o protocolo inadequado para redes modernas.

Por essa razão, redes que ainda utilizam WEP devem ser consideradas inseguras e devem ser atualizadas.

WPA

O Wi-Fi Protected Access (WPA) foi desenvolvido como uma solução de transição para solucionar problemas encontrados no WEP. Apesar de representar uma evolução importante, o WPA original utiliza mecanismos considerados legados.

Atualmente, não é recomendado utilizar WEP ou WPA como mecanismos principais de proteção.

WPA2

O WPA2 representou uma evolução significativa em relação aos protocolos anteriores e tornou-se amplamente utilizado em redes residenciais e corporativas. O WPA2 pode utilizar o padrão AES/CCMP, oferecendo um nível de proteção muito superior ao WEP e ao WPA baseado em mecanismos legados.

Apesar de ainda existir uma enorme quantidade de equipamentos WPA2 em funcionamento, a infraestrutura deve ser atualizada sempre que houver suporte ao WPA3.

WPA3

O WPA3 representa a evolução mais recente dos mecanismos de segurança Wi-Fi amplamente adotados no mercado. O NIST define WPA3 como Wi-Fi Protected Access version 3 e recomenda a utilização de tecnologias atuais de proteção sempre que possível.

Uma característica importante do WPA3-Personal é a utilização do Simultaneous Authentication of Equals (SAE), mecanismo desenvolvido para oferecer proteção mais robusta durante a autenticação baseada em senha. Em ambientes corporativos, mecanismos de autenticação baseados em infraestrutura de autenticação centralizada podem oferecer controles mais avançados do que uma única senha compartilhada por todos os usuários.

Portanto, sempre que os equipamentos forem compatíveis, recomenda-se utilizar WPA3, quando isso não for possível, WPA2 com AES/CCMP continua sendo uma alternativa para equipamentos que ainda não suportam WPA3, desde que devidamente configurada.

PRINCIPAIS AMEAÇAS À SEGURANÇA DAS REDES WI-FI

As redes sem fio podem estar sujeitas a diferentes tipos de ameaças.

Acesso não Autorizado

O acesso não autorizado ocorre quando uma pessoa consegue ingressar na rede sem possuir autorização. Isso pode acontecer devido a senhas fracas, compartilhamento indiscriminado da senha, exploração de vulnerabilidades ou comprometimento de algum dispositivo autorizado.

Uma senha Wi-Fi deve ser longa, exclusiva e difícil de adivinhar. Também é recomendável evitar informações pessoais, nomes, datas ou palavras comuns.

Pontos de Acesso Fraudulentos

Um atacante pode criar uma rede Wi-Fi com nome semelhante ou igual ao de uma rede legítima, tentando induzir os usuários a realizar a conexão.

Esse tipo de ameaça é frequentemente associado aos chamados rogue access points ou evil twins. Por esse motivo, usuários devem evitar conectar-se automaticamente a redes desconhecidas e devem verificar cuidadosamente a rede fornecida por estabelecimentos.

Captura de Tráfego

Como a comunicação Wi-Fi utiliza ondas de rádio, um atacante localizado dentro do alcance do sinal pode tentar capturar transmissões. A utilização de criptografia na camada Wi-Fi e de protocolos seguros nas aplicações reduz significativamente os riscos.

Além disso, protocolos como TLS proporcionam proteção adicional às aplicações. A especificação atual do TLS 1.3 estabelece mecanismos destinados a fornecer autenticação, confidencialidade e integridade às comunicações entre os participantes.

Ataques de Engenharia Social

Nem todos os ataques dependem de vulnerabilidades técnicas. Um usuário pode ser convencido a fornecer sua senha, clicar em um link malicioso ou conectar-se a uma rede falsa. Consequentemente, a conscientização dos usuários deve fazer parte da estratégia de segurança.

Exploração de Equipamentos Desatualizados

Roteadores, pontos de acesso, celulares, computadores e dispositivos IoT podem apresentar vulnerabilidades conhecidas. A ausência de atualizações de firmware e software aumenta o risco de exploração. O NIST recomenda manter sistemas atualizados e utilizar mecanismos atuais de proteção em redes sem fio.

SEGURANÇA EM REDES WI-FI PÚBLICAS

Redes Wi-Fi públicas são encontradas em aeroportos, hotéis, restaurantes, bibliotecas, universidades, shoppings e outros locais.

O principal problema não é simplesmente o fato de uma rede ser pública. O risco está associado ao fato de o usuário possuir pouco controle sobre a infraestrutura e sobre os demais equipamentos conectados. Além disso, uma rede pública pode apresentar configurações inadequadas, equipamentos desatualizados ou até mesmo pontos de acesso fraudulentos. Ao utilizar uma rede pública, recomenda-se:

- Confirmar o nome oficial da rede junto ao estabelecimento;
- Evitar conexões automáticas com redes desconhecidas;
- Manter o sistema operacional e os aplicativos atualizados;
- Utilizar HTTPS e aplicações que adotem comunicação criptografada;
- Evitar inserir informações sensíveis em páginas suspeitas;

- Utilizar autenticação multifator nos serviços importantes;
- Desconectar-se da rede quando ela não estiver mais sendo utilizada;
- Desativar compartilhamentos de arquivos quando não forem necessários;
- Utilizar VPN quando indicada pela política de segurança da organização.

É importante corrigir uma concepção comum: o HTTPS não torna uma rede Wi-Fi segura por si só, mas protege a comunicação entre o aplicativo/navegador e o serviço remoto quando corretamente implementado. Da mesma forma, uma VPN cria um túnel protegido entre o dispositivo e o servidor VPN, mas não substitui as demais medidas de segurança.

SEGURANÇA EM REDES DOMÉSTICAS

A rede doméstica concentra cada vez mais dispositivos. Além de computadores e smartphones, atualmente é comum encontrar câmeras, televisores, impressoras, assistentes virtuais, equipamentos de automação residencial e outros dispositivos IoT; essa diversidade aumenta a superfície de ataque. Uma configuração adequada deve considerar:

Alteração das Credenciais Padrão

As credenciais administrativas fornecidas pelo fabricante devem ser substituídas por senhas fortes e exclusivas. O mesmo cuidado deve ser aplicado ao painel administrativo do roteador.

Atualização do Firmware

O firmware do roteador deve ser atualizado sempre que o fabricante disponibilizar correções de segurança.

Desativação de Funções Desnecessárias

Serviços administrativos remotos, WPS e outras funções que não sejam necessárias devem ser desativados conforme as recomendações do fabricante e da política de segurança.

Utilização de WPA3

Quando suportado pelo equipamento, o WPA3 deve ser priorizado. Caso equipamentos antigos exijam compatibilidade, uma configuração de transição pode ser utilizada, desde que avaliada quanto aos riscos.

Senha forte para o Wi-Fi

A senha da rede deve possuir tamanho adequado e não deve ser reutilizada em outros serviços.

Rede para Convidados

Roteadores modernos normalmente permitem a criação de uma rede de convidados. Essa funcionalidade pode ser utilizada para separar dispositivos de visitantes dos equipamentos pessoais.

SEGMENTAÇÃO DE REDES WI-FI

A segmentação é uma das estratégias mais importantes em ambientes corporativos. Uma organização pode, por exemplo, possuir redes diferentes para:

- Funcionários;
- Visitantes;
- Dispositivos IoT;
- Equipamentos administrativos;
- Sistemas críticos;
- Dispositivos de terceiros.

A segmentação pode ser implementada por meio de VLANs, políticas de firewall, SSIDs distintos e mecanismos de controle de acesso. O objetivo é limitar a comunicação entre os diferentes grupos. Por exemplo, um dispositivo conectado à rede de visitantes não deveria possuir acesso direto a servidores internos ou sistemas administrativos.

A segmentação reduz o impacto de um possível comprometimento, pois impede que um atacante tenha automaticamente acesso a todos os recursos da infraestrutura.

AUTENTICAÇÃO EM REDES CORPORATIVAS

Em redes pequenas, é comum utilizar uma senha compartilhada por todos os usuários, entretanto, esse modelo apresenta limitações. Quando um funcionário deixa uma organização, por exemplo, seria necessário alterar a senha da rede e distribuí-la novamente aos usuários autorizados.

Em ambientes corporativos, pode ser mais adequado utilizar autenticação individualizada, especialmente por meio do padrão IEEE 802.1X e de mecanismos como EAP, associados a uma infraestrutura de autenticação. Esse modelo permite associar o acesso a uma identidade específica, facilitando a revogação de credenciais e a aplicação de políticas diferenciadas.

A autenticação multifator também pode ser empregada nos sistemas corporativos associados à rede. Entretanto, é importante diferenciar autenticação multifator de segurança Wi-Fi: o 2FA não substitui o WPA3, o controle de acesso ou a segmentação. Ele acrescenta uma camada de proteção aos sistemas que o suportam.

FIREWALL E MONITORAMENTO

A proteção de uma rede Wi-Fi não deve terminar no ponto de acesso, firewalls podem controlar o tráfego entre diferentes redes e limitar conexões não autorizadas.

Em ambientes corporativos, sistemas de detecção e prevenção de intrusão, registros de eventos e ferramentas de monitoramento podem ser utilizados para identificar comportamentos anormais. O monitoramento permite identificar, por exemplo:

- Novos dispositivos conectados;
- Tentativas repetidas de autenticação;
- Alterações de configuração;
- Tráfego incomum;
- Equipamentos desconhecidos;
- Falhas de autenticação;
- Possíveis ataques de negação de serviço.

O NIST destaca que a segurança de uma WLAN deve ser tratada durante todo o ciclo de vida, incluindo projeto, implementação, manutenção e monitoramento.

ATUALIZAÇÕES E GERENCIAMENTO DE VULNERABILIDADES

Uma das principais falhas encontradas em ambientes tecnológicos é a manutenção de equipamentos com software desatualizado. A atualização deve abranger:

- Roteadores;
- Pontos de acesso;
- Controladores;
- Sistemas operacionais;
- Aplicativos;
- Dispositivos IoT;
- Equipamentos de segurança;
- Servidores de autenticação.

As organizações devem manter inventário dos equipamentos e estabelecer um processo de gerenciamento de vulnerabilidades.

Também é recomendável substituir equipamentos que não recebem mais atualizações de segurança do fabricante.

AUDITORIA E TESTES DE SEGURANÇA

A auditoria de segurança permite verificar se as configurações existentes estão de acordo com as políticas da organização. Entre os aspectos que podem ser avaliados estão:

- Protocolo de segurança utilizado;
- Qualidade das senhas;
- Configuração do WPA3/WPA2;
- Existência de redes antigas;
- Atualização dos equipamentos;
- Exposição de interfaces administrativas;
- Segmentação;
- Isolamento da rede de convidados;
- Registros de eventos;
- Dispositivos autorizados;
- Políticas de firewall.

Testes de segurança e testes de penetração também podem ser realizados de maneira autorizada para identificar vulnerabilidades antes que sejam exploradas por agentes maliciosos.

Esses testes devem possuir escopo definido e autorização formal, principalmente em ambientes corporativos.

SEGURANÇA DE DISPOSITIVOS MÓVEIS

Smartphones e tablets são frequentemente utilizados para acessar redes Wi-Fi públicas e privadas. A segurança do dispositivo é tão importante quanto a segurança do ponto de acesso. É recomendável:

- Manter o sistema operacional atualizado;
- Instalar aplicativos somente de fontes confiáveis;
- Utilizar bloqueio de tela;
- Habilitar autenticação multifator nos serviços importantes;
- Utilizar aplicativos oficiais de instituições financeiras;
- Evitar conectar-se automaticamente a redes desconhecidas;
- Revisar permissões concedidas aos aplicativos;
- Realizar backups;
- Utilizar criptografia do dispositivo quando disponível.

É incorreto afirmar que uma rede móvel é automaticamente segura e que uma rede Wi-Fi é sempre insegura. A segurança depende da tecnologia empregada, da

configuração e do comportamento do usuário.

PROTEÇÃO DE DADOS E A LGPD

A segurança de redes Wi-Fi possui relação direta com a proteção de dados pessoais quando informações de usuários são tratadas por meio da infraestrutura.

A Lei nº 13.709/2018 estabelece, em seu artigo 46, que os agentes de tratamento devem adotar medidas técnicas e administrativas capazes de proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas.

A própria Autoridade Nacional de Proteção de Dados destaca a necessidade de medidas técnicas e administrativas para proteção dos dados pessoais. Entre as medidas de segurança estão controles de acesso, criptografia, atualização de sistemas, políticas internas e mecanismos de prevenção de incidentes. Em redes Wi-Fi corporativas ou públicas, podem ser tratados diversos tipos de dados, como:

- Identificadores de dispositivos;
- Informações de autenticação;
- Registros de conexão;
- Endereços IP;
- Dados de cadastro;
- Informações utilizadas em portais de acesso;
- Informações de navegação, dependendo da arquitetura e finalidade do tratamento.

Por isso, a organização deve avaliar quais dados coleta, para qual finalidade, por quanto tempo são mantidos, quem possui acesso e quais medidas são utilizadas para protegê-los.

A segurança deve ser incorporada desde a concepção dos serviços. A LGPD determina que as medidas de segurança devem ser observadas desde a fase de concepção do produto ou serviço até sua execução.

A ANPD também disponibiliza orientação específica para agentes de tratamento de pequeno porte, indicando a adoção de medidas administrativas e técnicas essenciais e necessárias, considerando o risco à privacidade e a realidade de cada organização.

WI-FI E LI-FI

Além das redes Wi-Fi, outras tecnologias de comunicação sem fio vêm sendo estudadas e desenvolvidas.

O Li-Fi (Light Fidelity) utiliza luz para realizar comunicação de dados, normalmente por meio de fontes de iluminação equipadas com componentes capazes de modular a luz. Uma diferença fundamental está no meio utilizado:

enquanto o Wi-Fi utiliza radiofrequência, o Li-Fi utiliza comunicação óptica.

O Li-Fi apresenta características interessantes para ambientes específicos, especialmente quando se deseja reduzir interferências de radiofrequência. Entretanto, sua utilização possui limitações, incluindo a necessidade de condições adequadas para propagação óptica e questões relacionadas à mobilidade.

Dessa forma, não se deve considerar necessariamente que o Li-Fi substituirá o Wi-Fi em todos os ambientes. As duas tecnologias podem ser vistas como soluções complementares para diferentes cenários.

BOAS PRÁTICAS PARA UMA REDE WI-FI SEGURA

A segurança de uma rede Wi-Fi pode ser fortalecida por um conjunto de medidas para usuários domésticos.

- Utilizar WPA3 sempre que possível;
- Utilizar WPA2 com AES/CCMP quando WPA3 não estiver disponível;
- Evitar WEP e protocolos legados;
- Criar senha Wi-Fi longa e exclusiva;
- Alterar a senha administrativa padrão do roteador;
- Atualizar o firmware;
- Desativar funções desnecessárias;
- Criar uma rede de convidados;
- Manter computadores e smartphones atualizados;
- Utilizar autenticação multifator nos serviços importantes.

Para empresas

- Utilizar autenticação individualizada;
- Implementar IEEE 802.1X quando apropriado;
- Segmentar redes por VLAN e políticas de firewall;
- Separar usuários, convidados e dispositivos IoT;
- Monitorar pontos de acesso e dispositivos;
- Manter inventário da infraestrutura;
- Realizar auditorias periódicas;
- Estabelecer políticas de segurança;
- Utilizar sistemas de detecção e prevenção de intrusão;
- Realizar testes de segurança autorizados;
- Estabelecer plano de resposta a incidentes;
- Capacitar os usuários;
- Alinhar os controles técnicos às exigências de proteção de dados.

RESPONSABILIDADE DO USUÁRIO

A tecnologia, isoladamente, não consegue eliminar todos os riscos, o usuário é parte fundamental da segurança. Uma rede configurada com WPA3, firewall e segmentação ainda pode ser comprometida se um usuário entregar voluntariamente sua senha a um atacante ou instalar um aplicativo malicioso.

Por isso, programas de conscientização devem abordar temas como phishing, engenharia social, senhas, autenticação multifator, redes públicas e identificação de sites fraudulentos. A educação dos usuários deve ser contínua, pois as técnicas utilizadas pelos atacantes também evoluem.

DISCUSSÃO

A análise apresentada demonstra que a segurança de redes Wi-Fi não pode ser reduzida à utilização de uma senha.

Existem diversas camadas de proteção que devem funcionar conjuntamente. A primeira camada envolve a segurança física e lógica dos equipamentos. A segunda está relacionada ao protocolo de proteção utilizado na comunicação sem fio. A terceira envolve autenticação e controle de acesso. A quarta consiste na segmentação e no controle do tráfego. A quinta está relacionada ao monitoramento, à atualização e à resposta a incidentes.

Em ambientes domésticos, medidas relativamente simples, como utilizar WPA3, uma senha forte, firmware atualizado e uma rede separada para convidados, já podem reduzir consideravelmente os riscos.

Em ambientes corporativos, entretanto, são necessários controles mais abrangentes, incluindo autenticação centralizada, segmentação, monitoramento, gestão de vulnerabilidades, políticas de segurança e resposta a incidentes.

Outro ponto importante é que segurança e privacidade estão relacionadas, mas não são conceitos idênticos. Uma rede pode estar tecnicamente protegida contra determinados ataques e, ainda assim, uma organização pode coletar mais dados pessoais do que o necessário ou armazená-los durante um período inadequado. Nesse sentido, a segurança deve ser integrada à governança de dados.

CONSIDERAÇÕES FINAIS

As redes Wi-Fi desempenham papel fundamental na sociedade conectada e continuarão sendo utilizadas em residências, empresas, instituições públicas, hospitais, escolas, estabelecimentos comerciais e diversos outros ambientes.

A mobilidade e a facilidade de implantação proporcionadas pela tecnologia, entretanto, devem ser acompanhadas de mecanismos adequados de segurança.

A análise realizada neste trabalho demonstra que os riscos existentes nas redes Wi-Fi não estão relacionados exclusivamente à transmissão por ondas de

rádio. Vulnerabilidades podem surgir em equipamentos, protocolos, configurações, aplicações, sistemas operacionais e, principalmente, no comportamento dos usuários.

Protocolos antigos como WEP e WPA devem ser considerados tecnologias legadas, enquanto WPA3 representa uma evolução importante para a proteção das redes modernas. O NIST recomenda a utilização de mecanismos atuais como WPA2/WPA3 e senhas difíceis de adivinhar, além da atualização dos dispositivos.

Em ambientes corporativos, a segurança deve ser ampliada por meio de autenticação individualizada, segmentação, firewall, monitoramento, atualização de equipamentos, auditorias e gestão de vulnerabilidades.

Também é necessário considerar a proteção dos dados pessoais tratados pela infraestrutura. No Brasil, a LGPD estabelece obrigações relacionadas à adoção de medidas técnicas e administrativas para proteção dos dados pessoais.

Assim, uma rede Wi-Fi segura deve ser compreendida como resultado de uma combinação de tecnologia, processos e pessoas.

A segurança não é uma configuração realizada uma única vez. Trata-se de um processo contínuo que exige avaliação de riscos, atualização tecnológica, monitoramento, treinamento e melhoria permanente.

Por fim, é possível concluir que a utilização adequada de mecanismos modernos de criptografia, autenticação, segmentação e monitoramento permite reduzir significativamente os riscos associados às redes sem fio. A evolução do Wi-Fi, incluindo novas gerações do padrão IEEE 802.11, deverá continuar acompanhando o crescimento do número de dispositivos conectados. Paralelamente, organizações e usuários precisarão manter uma postura preventiva para garantir a confidencialidade, integridade, disponibilidade e proteção dos dados que circulam nessas redes.

REFERÊNCIAS

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte**. Brasília, DF: ANPD, 2021. Disponível em: <https://www.gov.br/anpd/>. Acesso em: 5 set. 2026.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: <https://www.planalto.gov.br/>. Acesso em: 5 set. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: <https://www.planalto.gov.br/>. Acesso em: 5 set. 2026.

BRASIL. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Resolução CD/**

ANPD nº 2, de 27 de janeiro de 2022. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, para agentes de tratamento de pequeno porte. Brasília, DF: ANPD, 2022. Disponível em: <https://www.gov.br/anpd/>. Acesso em: 5 set. 2026.

IEEE. **IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks—Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.** IEEE Std 802.11. New York: IEEE, 2020.

MARIMOTO, Carlos E. **Guia completa de redes.** 3. ed. Porto Alegre: GDH Press; Sul Editores, 2014.

RESCORLA, E. **The Transport Layer Security (TLS) Protocol Version 1.3.** RFC 9846. Internet Engineering Task Force (IETF), 2026. Disponível em: <https://www.rfc-editor.org/>. Acesso em: 5 set. 2026.

SABRY, Fouad. **Li-Fi.** [S.l.]Um Bilhão Bem Informado; PublishDrive, 2022.

SOUPPAYA, Murugiah P.; SCARFONE, Karen. **Guidelines for securing wireless local area networks (WLANs).** NIST Special Publication 800-153. Gaithersburg: National Institute of Standards and Technology, 2012. DOI: <https://doi.org/10.6028/NIST.SP.800-153>. Acesso em: 5 set. 2026.

TERADA, Routo. **Segurança de dados: criptografia em redes de computador.** São Paulo: Edgard Blücher, 2000.

TORRES, Gabriel. **Redes Wi-Fi.** 2. ed. [S.l.]: Clube do Hardware, 2023.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Cybersecurity awareness month: securing devices at home and work.** Gaithersburg: NIST, 2020. Disponível em: <https://www.nist.gov/>. Acesso em: 5 set. 2026.