# MEIO DE ACESSO SEM FIO (WIRELESS)


- SOBRE MEIO DE ACESSO SEM FIO (WIRELESS)
- QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?
- QUAIS SÃO AS NOSSAS SUGESTÕES?

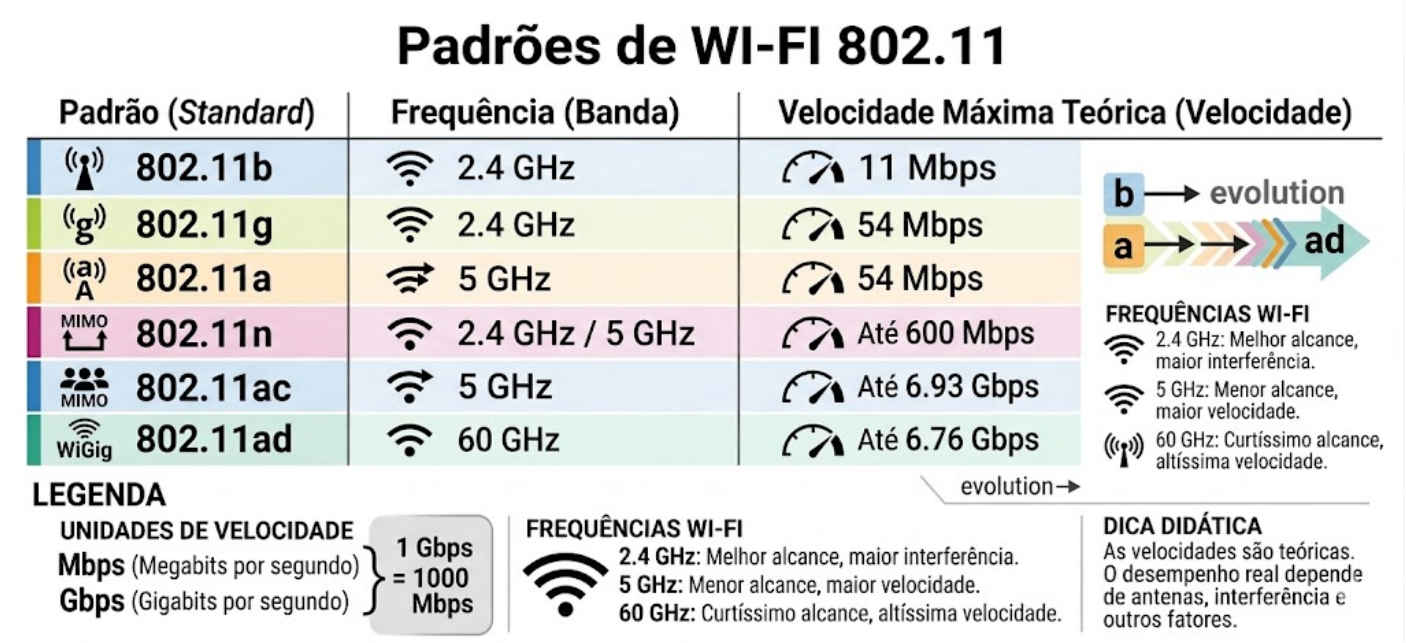
# SOBRE MEIO DE ACESSO SEM FIO (WIRELESS)

As redes sem fio estão cada vez mais populares para as pessoas que exercem atividades em vários locais e também como uma alternativa de baixo custo para a aquisição e instalação de cabos de rede em um novo local. As redes sem fio oferecem flexibilidade e mobilidade, uma vez que as pessoas não ficam mais restritas aos seus locais de trabalho pela necessidade de conexões físicas à rede.

Ademais, permite uma implantação mais econômica para redes locais (LANs), além de possibilitar a utilização em espaços onde o cabeamento não pode ser executado, como áreas ao ar livre e edifícios históricos. Além disso, os fabricantes estão incluindo placas de rede wireless na maioria dos dispositivos atuais.

Quando viável, a rede wi-fi deve dispor de autenticação integrada com o Active Directory, permitindo que os usuários se autentiquem na rede com as mesmas credenciais empregadas para acessar o e-mail corporativo.

Os principais padrões de transmissão para rede sem fio mais utilizados no mercado e algumas de suas características são observadas a seguir.



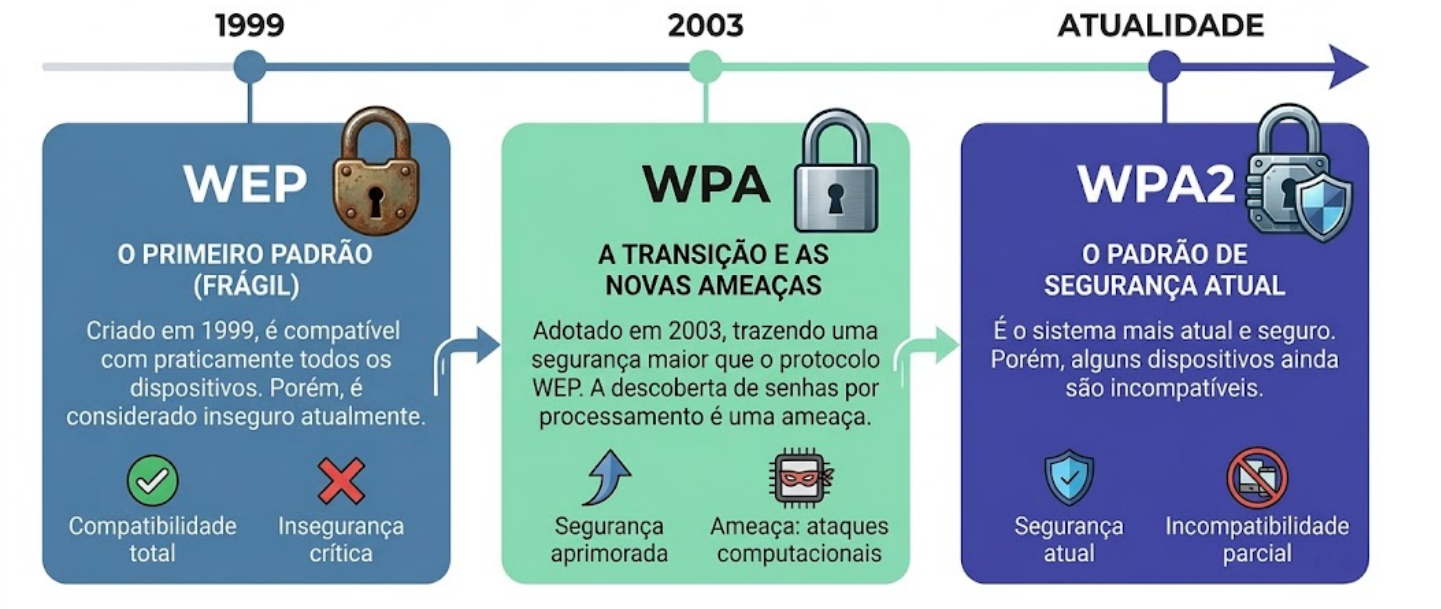

Além dos padrões de transmissão apresentados, é essencial adotar um protocolo de criptografia para redes sem fio.

A segurança é um ponto de atenção das redes sem fio, uma vez que o sinal é propagado pelo ar em todas as direções e pode ser captado a distâncias de centenas de metros, tornando-as

vulneráveis à interceptação.

Para mitigar essas vulnerabilidades, surgiram alguns protocolos que são utilizados na segurança de redes sem fio.

Dentre os principais, podemos elencar:




> Apesar do padrão WPA2 ser considerado o mais seguro, o ataque KRACK, de outubro de 2017, expôs grandes fragilidades sobre o protocolo.

# QUAIS SÃO AS NOSSAS RECOMENDAÇÕES?

- Fazer uso de equipamentos que suportem o padrão 802.11n ou superior.
- Atualizar periodicamente os firmwares dos ativos de redes sem fio, para mitigar vulnerabilidades de segurança.
- Implantar padrão WPA, no mínimo. Idealmente, WPA2 com algoritmo AES-CCMP, abstendo-se ao máximo de utilizar WPA-TKIP ou GCMP.
- Utilizar a Orientação Técnica – 002 Interconectividade de Rede como referência para interconectividade da rede sem fio com as demais redes.
- Alterar todas as senhas padrão dos equipamentos para senhas mais seguras.

# QUAIS SÃO AS NOSSAS SUGESTÕES?

- Priorizar o uso de um sistema de rede sem fio (WLAN System) ao invés de Access Points autônomos (APs).
- Avaliar o canal wi-fi utilizado no equipamento e nas redes próximas, uma vez que o desempenho da rede poderá ser comprometido caso haja muitos equipamentos utilizando o mesmo canal em um raio próximo. Ativar, nos switches gerenciados com capacidade de bloqueio de acesso a nível de porta, o controle de acesso à porta afim de evitar o uso da rede por equipamentos não autorizados.