

***Maria Eliza Pessoa Picorelli**

Graduanda em Análise e Desenvolvimento de Sistemas na Fatec de Mogi das Cruzes, João Pessoa, Brasil.

ORCID: 0009-0000-5729-1521.

E-mail:

maria.picorelli@aluno.cps.sp.gov.br

****Raquel Gomes de Oliveira**

Graduanda em Análise e Desenvolvimento de Sistemas na Fatec de Mogi das Cruzes, Mogi das Cruzes, Brasil.

ORCID: 0009-0009-0650-4158

E-mail:

raquel.oliveira5@aluno.cps.sp.gov.br

*****Luciano Gonçalves de Carvalho**

Professor e Orientador do curso de Análise e Desenvolvimento de Sistemas da Fatec de Mogi das Cruzes, Mogi das Cruzes, Brasil.

ORCID: 0009-0009-3528-0480.

E-mail:

luciano.carvalho@cps.sp.gov.br

ESTRATÉGIAS DE MIGRAÇÃO GRADUAL DO WPA2 PARA O WPA3 EM AMBIENTES CORPORATIVOS

DOI: doi.org/10.5281/zenodo.22665283

RESUMO

O estudo analisa as estratégias de migração gradual do protocolo WPA2 para o WPA3 em ambientes corporativos, tema relevante diante da crescente sofisticação dos ataques a redes sem fio e da ampla utilização do WPA2 nas organizações, mesmo após o lançamento de um protocolo mais seguro. Por meio de uma revisão bibliográfica qualitativa e exploratória, o trabalho examina as vulnerabilidades do WPA2, e apresenta os avanços do WPA3 especialmente o protocolo SAE, que garante *Forward Secrecy* e maior resistência a ataques de força bruta. São analisadas três estratégias de transição: o *Transition Mode*, que permite a coexistência entre dispositivos WPA2 e WPA3; o uso de múltiplos SSIDs, que segmenta dispositivos legados dos modernos; e o *Only Mode*, etapa final em que toda a infraestrutura opera exclusivamente com WPA3. O estudo conclui que a migração é viável, desde que planejada de acordo com as particularidades de cada ambiente organizacional, e embora o processo possa ser custoso, os riscos associados à manutenção de protocolos vulneráveis como exposição de dados, impactos legais e financeiros tornam a transição uma decisão estratégica indispensável para a segurança corporativa.

Palavras-Chave: Ambientes Corporativos; Migração Gradual; Segurança em Redes Sem Fio; Protocolos de Segurança.

GRADUAL MIGRATION STRATEGIES TO WPA3 IN CORPORATE ENVIRONMENTS

ABSTRACT

This study analyzes the strategies for the gradual migration from the WPA2 protocol to WPA3 in corporate environments, a relevant topic given the increasing sophistication of wireless network attacks and the widespread use of WPA2 in organizations, even after the release of a more secure protocol. Through a qualitative and exploratory literature review, the study examines the vulnerabilities of WPA2 and presents the advances introduced by WPA3, especially the SAE protocol, which provides Forward Secrecy and greater resistance to brute-force attacks. Three transition strategies are analyzed: Transition Mode, which allows coexistence between WPA2 and WPA3 devices; the use of multiple SSIDs, which segments legacy and modern devices; and Only Mode, the final stage in which the entire infrastructure operates exclusively with WPA3. The study concludes that migration is feasible, provided it is planned according to the specific characteristics of each organizational environment. Although the process may be costly, the risks associated with maintaining vulnerable protocols, such as data exposure and legal and financial impacts, make the transition an essential strategic decision for corporate security.

Keywords Corporate Environments; Gradual Migration; Wireless Network Security; Security Protocols.

ESTRATEGIAS DE MIGRACIÓN GRADUAL A WPA3 EN ENTORNOS CORPORATIVOS

RESUMEN

El estudio analiza las estrategias de migración gradual del protocolo WPA2 hacia WPA3 en entornos corporativos, un tema relevante debido a la creciente sofisticación de los ataques a redes inalámbricas y al amplio uso de WPA2 en las organizaciones, incluso después del lanzamiento de un protocolo más seguro. Mediante una revisión bibliográfica cualitativa y exploratoria, el trabajo examina las vulnerabilidades de WPA2 y presenta los avances de WPA3, especialmente el protocolo SAE, que garantiza Forward Secrecy y una mayor resistencia a ataques de fuerza bruta. Se analizan tres estrategias de transición: el Transition Mode, que permite la coexistencia entre dispositivos WPA2 y WPA3; el uso de múltiples SSID, que segmenta dispositivos heredados y modernos; y el Only Mode, etapa final en la que toda la infraestructura opera exclusivamente con WPA3. El estudio concluye que la migración es viable, siempre que se planifique de acuerdo con las particularidades de cada entorno organizacional. Aunque el proceso puede ser costoso, los riesgos asociados al mantenimiento de protocolos vulnerables, como la exposición de datos y los impactos legales y financieros, convierten la transición en una decisión estratégica indispensable para la seguridad corporativa.

Palabras clave: Entornos Corporativos; Migración Gradual; Seguridad en Redes Inalámbricas; Protocolos de Seguridad.

INTRODUÇÃO

Com o surgimento das transmissões de dados sem conexão cabeada, a segurança e a autenticação tornaram-se uma preocupação central, uma vez que as novas tecnologias trouxeram novas vulnerabilidades. Como observa Neto (2025), o crescimento do uso de redes Wi-Fi tem proporcionado maior conveniência para usuários em ambientes domésticos e corporativos, entretanto aumentou a exposição a ciberameaças, tornando a segurança em redes sem fio uma necessidade crítica. Em resposta, foram desenvolvidos protocolos de segurança, iniciando em 1997 com o WEP (Wired Equivalent Privacy), seguido pelo WPA, WPA2 e o mais recente WPA3.

Ao longo dessa evolução, cada novo protocolo buscou corrigir falhas dos anteriores. O WEP apresentava vulnerabilidades significativas que comprometiam sua eficiência, levando ao desenvolvimento do WPA, que ainda se mostrou insuficiente em termos de segurança. Posteriormente, surgiu o WPA2, tornando-se amplamente utilizado, contudo, apresentou vulnerabilidades, como o ataque KRACK, impulsionando o desenvolvimento do WPA3, o padrão mais recente e robusto para redes sem fio.

Apesar da disponibilidade de um protocolo mais seguro, dados do relatório Wi-Fi Security Market Research Report 2034 indicam que o WPA2 ainda protege cerca de 62,1% das redes sem fio globais, enquanto o WPA3 detém apenas 18,4% do mercado (Sharma, 2026). Contudo, à medida que as organizações reconhecem as vulnerabilidades do padrão anterior e planejam a transição para normas mais recentes, espera-se que a participação do WPA3 alcance 31,7% até 2034 (Sharma, 2026). Sob essa perspectiva, mesmo após anos do lançamento do protocolo mais robusto em 2018, constata-se uma brecha entre os avanços tecnológicos de segurança e sua efetiva aplicação prática nas empresas. Esse cenário impõe um desafio comum às organizações: realizar a transição para tecnologias mais seguras sem comprometer a continuidade de suas operações.

Diante desse contexto, este trabalho tem como objetivo comparar estratégias para a migração gradual do WPA2 para o WPA3 em ambientes corporativos, com base nos critérios do trabalho de Barbosa (2018). Com métricas estabelecidas, as corporações realizam a transição de maneira assertiva e compatível com as necessidades organizacionais.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Importância da segurança da informação em redes corporativas

A segurança em redes Wi-Fi é fundamental tanto para usuários domésticos quanto para organizações. No ambiente corporativo, ela desempenha um papel crucial na preservação da confidencialidade de dados estratégicos, na proteção da propriedade intelectual e na integridade de transações financeiras. Onde falhas de segurança podem gerar não apenas prejuízos econômicos, mas também impactos legais e danos à reputação institucional. Nesse contexto, a adoção de protocolos de segurança atualizados, associada a boas práticas de configuração e gestão, torna-se indispensável para enfrentar ataques cada vez mais sofisticados e garantir a confiabilidade das comunicações sem fio.

2.2 WPA2: Funcionamento do protocolo e desvantagens

Em 2001, o National Institute of Standards and Technology (NIST) formalizou a adoção do Advanced Encryption Standard (AES), que estabelece as bases criptográficas que fundamentam o WPA2, ratificado em 2004 pelo IEEE como parte do padrão 802.11i, que

estabelece os requisitos para redes sem fio, contemplando aspectos da camada física e os métodos de segurança aplicados à transmissão de dados (Najar; Mir, 2021).

Essa adoção representou um avanço significativo nos protocolos de segurança, impulsionado pela evolução dos algoritmos de criptografia. Seguindo uma estrutura semelhante às implementações precedentes, o WPA2 opera em dois modos de segurança: WPA2-Pessoal (ou PSK – Pre-Shared Key) e WPA2-Enterprise (ou EAP – Extensible Authentication Protocol). Ambos oferecem mecanismos de proteção contra acessos não autorizados à rede, baseando-se no uso de uma senha pré-definida ou, no caso corporativo, em métodos de autenticação mais robustos.

O WPA2 é constituído por mecanismos de autenticação, criptografia e controle de integridade que operam de forma integrada. O WPA2 utiliza o CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) como principal mecanismo de criptografia, nesse modo o AES opera como cifra em blocos, segmentando a comunicação em blocos de 128 bits e garantindo a verificação de integridade. Nesse processo, a Pairwise Transient Key (PTK) é gerada durante o 4-Way Handshake, responsável por estabelecer as chaves de sessão.

Esse conjunto de chaves pode ser usado na forma de chaves pareadas (pairwise), quando a comunicação é unicast, ou como Group Temporal Key (GTK), quando o tráfego é broadcast, sendo compartilhado entre todos os dispositivos da rede. Tanto o ponto de acesso quanto o cliente utilizam a Pairwise Master Key (PMK), derivada do processo de autenticação, para gerar a PTK. Esta, por sua vez, dá origem ao Message Integrity Code (MIC), responsável por assegurar a integridade dos dados transmitidos.

No protocolo, a maior desvantagem, é a segurança que depende da PTK, derivada diretamente da senha, a partir dos valores aleatórios trocados no 4-Way Handshake, renovados a cada sessão (Ghanim; Thanoun, 2025). A PTK é gerada a partir da Pre-Shared Key (PSK) e de informações transmitidas em texto claro, como SSID (Service Set Identifier), ANonce, SNonce e endereços MAC, o que permite que invasores capturem esses dados e realizem tentativas sucessivas de obtenção da PSK. Embora a senha não seja transmitida, ela pode ser recuperada por força bruta, já que a PSK é calculada pela função Password-Based Key Derivation Function 2 (PBKDF2), combinando senha e SSID.

Nos ataques de dicionário, uma vulnerabilidade explorada no WPA2, cada senha candidata é utilizada para gerar uma PSK e uma PTK, verificando se o MIC resultante corresponde ao de um pacote do handshake. Se a validação ocorrer, a senha correta será identificada. A eficiência do ataque pode ser ampliada pelo uso de endereços MAC falsificados e pela criação de múltiplos Virtual Wireless Clients (VWCs), que testam senhas em paralelo e facilitam a captura repetida do handshake. Ademais, o protocolo permite ataques de reinicialização de chaves, conhecida como ataque KRACK, utiliza-se da vulnerabilidade do 4-way-handshake, que o protocolo usa para autenticar os usuários enquanto conectam à rede, forçando a reinstalação com uma chave já utilizada.

A presença dessas vulnerabilidades é especialmente preocupante em ambientes corporativos, onde os danos podem ser significativos e de difícil reversão. O objetivo desses ataques é a violação da privacidade dos usuários, de modo que expõe dados sensíveis como credenciais de acesso, informações financeiras e documentos institucionais, evidenciando a necessidade de migração para um protocolo que ofereça mecanismos de segurança mais robustos.

2.3 WPA3: Funcionamento do protocolo e a melhoria em relação ao protocolo WPA2

O WPA3, lançado pela Wi-Fi Alliance em 2018, representa o padrão mais avançado de segurança para redes sem fio e tem sido apontado como substituto natural do WPA2 em ambientes corporativos. Seu principal mecanismo é o protocolo SAE (Simultaneous Authentication of Equals), também conhecido como Dragonfly Handshake, que substitui o PSK do WPA2 por uma troca de chaves baseadas em criptografia de curva elíptica e diferente do WPA2, o SAE, garante Forward Secrecy, onde cada sessão gera chaves independentes, de modo que a descoberta futura da senha não compromete comunicações anteriores. Além disso, o WPA3 torna obrigatório o uso de MFP (Management Frame Protection), prevenindo ataques de desautenticação, e oferecendo criptografia de 192 bits no modo enterprise, indicado para ambientes de alta segurança (Ghanim; Thanoun, 2025; Mathew; Jackson; Tobesman, 2025).

Entretanto, o WPA3 não está isento de vulnerabilidade, pesquisadores identificaram ataques de canal lateral e ataques de downgrade no handshake Dragonfly, vulnerabilidade conhecidas

como Dragonblood (Vanhoeft; Ronen, 2020), e o modo de transição que permite a coexistência com WPA2 para facilitar a migração gradual, também reintroduz brechas exploráveis, evidenciando que a adoção do WPA3 exige planejamento cuidadoso, especialmente em ambientes corporativos.

Apesar dos avanços de segurança, a adoção do WPA3 em ambientes corporativos apresenta desafios concretos. O principal deles é a compatibilidade, já que a maioria dos dispositivos em uso nas organizações suporta apenas WPA2, tornando a transição dependente de substituição de hardware ou atualizações de firmware nem sempre disponíveis para equipamentos mais antigos. Em ambientes mistos, nos quais o modo de transição é habilitado para garantir coexistência, ataques de downgrade podem forçar dispositivos a se conectarem via WPA2, reintroduzindo vulnerabilidade que o WPA3 se propõe a mitigar.

No contexto corporativo, a complexidade se amplifica pela necessidade de atualizar simultaneamente múltiplos pontos de acesso e dispositivos, além de configurações específicas para operação segura. Incompatibilidades durante essa fase podem gerar instabilidades e interrupções nas redes, riscos que tornam a migração gradual não apenas uma opção, mas uma necessidade estratégica para as organizações.

2.4 WPA3: Estratégias para migração do WPA2 para WPA3 em organizações

O Transition Mode, uma estratégia de migração gradual recomendada pela Wi-Fi Alliance, permite a coexistência entre dispositivos WPA2 e WPA3 durante a migração. De acordo com as diretrizes da Wi-Fi Alliance (2025), o modo de transição do WPA3-Enterprise opera de forma semelhante ao WPA2-Enterprise, porém com restrições e requisitos de segurança adicionais. Nessa configuração, o uso do protocolo de criptografia legado TKIP é estritamente proibido e o recurso de Proteção de Frames de Gerenciamento (Protected Management Frames – PMF) deve estar ativado. Além disso, torna-se obrigatória a habilitação simultânea dos mecanismos de Autenticação e Gerenciamento de Chaves (Authentication and Key Management – AKM), englobando tanto o SHA-1 AKM, voltado ao suporte dos dispositivos WPA2-Enterprise, quanto o SHA-256 AKM, associado aos recursos avançados do WPA3-Enterprise.

Trata-se de uma solução temporária, recomendada até que toda a infraestrutura suporte integralmente o WPA3, o principal benefício da adoção da técnica é a redução do impacto operacional, que evita as substituições imediatas e minimiza os custos e riscos de indisponibilidade. Entretanto como limitação destaca-se que, a coexistência entre os protocolos, mantém ainda a rede suscetíveis a ataques de downgrade, além de possíveis incompatibilidades em clientes legados que não interpretam corretamente múltiplos mecanismos de autenticação anunciados simultaneamente.

Ademais, a utilização de múltiplos SSID segundo a Wi-Fi Alliance, é uma estratégia recomendada como alternativa ao WPA3 Transition Mode em cenários nos quais dispositivos antigos apresentam problemas de interoperabilidade com redes configuradas em modo de transição. Nesse modelo, cada SSID utiliza configurações de segurança independentes, podendo inclusive operar com credenciais e políticas distintas. A principal vantagem é a segmentação clara entre dispositivos legados e modernos, permitindo que estes últimos utilizem integralmente os recursos do WPA3, como Protected Management Frames (PMF) obrigatório e uma maior proteção contra-ataques de força bruta e downgrade. Em contrapartida, a manutenção de múltiplas redes aumenta a complexidade administrativa e prolonga a exposição às vulnerabilidades do WPA2, exigindo planejamento contínuo para a eliminação progressiva dos dispositivos legados.

A etapa final da migração é o Only Mode, no qual o suporte ao WPA2-Enterprise é completamente eliminado e todos os dispositivos passam a operar exclusivamente com WPA3. Os APs (Access Point, ou Pontos de Acessos) anunciam apenas conexões WPA3-Enterprise, eliminando o risco de ataques de downgrade. Nessa configuração, recomenda-se o uso de CCMP-128 como suíte de cifras de dados em grupo e BIP-CMAC-128 para o gerenciamento, garantindo compatibilidade com dispositivos que não suportam Extremely High Throughput (EHT).

A transição para esse modo é facilitada pelo mecanismo de Transition Disable (Desativação de Transição), que consiste em uma indicação enviada por um AP para um STA (Station, ou estação/dispositivo com interface Wi-Fi, aplicando-se na prática aos dispositivos clientes como laptops e smartphones), fazendo com que o dispositivo desative o modo de transição no perfil de rede correspondente ao AP (Wi-Fi Alliance, 2025). No caso de redes

corporativas que adotam o WPA3-Enterprise a rede passa a operar no modo WPA3-Only Enterprise (configuração do bit 2).

Para garantir consistência, esse mecanismo deve estar habilitado em todos os BSSs (Basic Service Sets, ou conjuntos básicos de serviço que representam as células de cobertura de cada ponto de acesso) que compartilham o mesmo SSID, com o KDE (Key Data Encapsulation) de Transition Disable idêntico entre todos os APs, em inconsistências a respeito das configurações de redes poderá haver falhas de conectividade em ambientes multi-site. Vale destacar que o Only Mode é distinto do WPA3-Enterprise de 192 bits, ele é voltado a organizações com requisitos de segurança máxima, que exige métodos EAP compatíveis com a suíte CNSA e cifras como GCMP-256.

3 MATERIAIS E MÉTODOS

Este trabalho caracteriza-se como um estudo qualitativo, exploratório e bibliográfico, voltado à comparação das estratégias de migração do protocolo WPA2 para o WPA3 em ambientes corporativos utilizando as métricas que foram definidas com base no trabalho de Barbosa (2018). Entre os critérios apresentados pelo autor, foram selecionados aqueles considerados mais adequados ao objetivo, que incluem a estimativa de investimento da migração, tempo, mudança nos processos internos e a análise dos riscos do modelo atual.

A investigação baseou-se em artigos científicos, periódicos especializados e fontes digitais de referência na área de segurança da informação, selecionados pela relevância e atualidade, considerando publicações a partir de 2016. O estudo concentrou-se no contexto de redes corporativas, limitando-se aos protocolos WPA2 e WPA3. Contudo ambientes acadêmicos, públicos e protocolos anteriores, como WEP e WPA, foram considerados apenas para contextualização histórica.

A investigação foi conduzida exclusivamente por meio de análise documental e revisão bibliográfica. A metodologia adotada buscou identificar e analisar as vantagens e limitações relacionadas à migração do protocolo WPA2 para o WPA3 em ambientes corporativos. A análise considerou aspectos relacionados à segurança da informação em redes sem fio, as vulnerabilidades presentes nesse contexto e as melhorias de segurança que podem ser obtidas a partir da adoção de estratégias adequadas de transição entre os protocolos.

4 RESULTADOS E DISCUSSÃO

O artigo desenvolvido permitiu identificar três estratégias de como realizar a migração do protocolo Wi-Fi WPA2 para o protocolo WPA3 em ambientes corporativos. A escolha efetiva da melhor estratégia para cenários, levando em consideração riscos e a capacidade financeira da empresa para modernizar sua segurança, depende de métricas que avaliam todas as decisões importantes em relação à migração.

A avaliação do investimento na migração deve ser refletida frente às vulnerabilidades intrínsecas ao protocolo WPA2 abordado pelo presente estudo, surge a necessidade da migração especialmente em ambientes que necessitam garantir uma maior segurança, estar adaptado e em conformidade com o protocolo mais robusto, garantindo a segurança dos processos internos e relacionados aos produtos e/ou serviços oferecidos ao mercado e clientes.

Para além de requisitos financeiros, a análise de esforço técnico para a migração deve ser considerada, uma vez que a migração escolhida caso possua uma maior complexidade no método utilizado para a transição resultará em um maior tempo gasto do ponto de vista organizacional. As três estratégias identificadas são analisadas a seguir com base nas métricas estabelecidas, permitindo uma comparação estruturada entre as abordagens disponíveis.

No que diz respeito ao investimento financeiro necessário para a migração, as três estratégias apresentam níveis distintos de custo. O Transition Mode configura-se como a opção de menor impacto orçamentário, uma vez que apresenta menor interferência operacional, pois permite que dispositivos WPA2 e WPA3 coexistam na mesma infraestrutura, dispensando assim a substituição imediata de equipamentos legados.

O uso de múltiplos SSIDs para migração implica um custo moderado, visto que oferece a possibilidade de operarem com credenciais e políticas distintas, acabam demandando a configuração de Virtual LANs (VLANs) e o mapeamento de tráfegos entre redes paralelas. Ademais, o Only Mode representa o maior investimento entre as três abordagens, já que exige a substituição de todos os dispositivos incompatíveis com o WPA3, este custo tende a ser grande em ambientes corporativos com infraestrutura ampla e variada.

Quando se trata do critério de tempo, do ponto de vista organizacional, para a transição ser realizada dentro do cenário do aumento da segurança dentro do menor prazo, isto é, o uso total do WPA3, o Only Mode se destaca entre as demais abordagens, caso todas as STAs da rede forem compatíveis com o WPA3, a rede poderá ser configurada com um SSID protegido pelo protocolo mais robusto. A criação de múltiplos SSIDs permite um prazo maior para a mudança de dispositivos legados, dado que dispositivos compatíveis podem acessar a uma SSID com a segurança do WPA3 e os legados conectem-se ao WPA2, enquanto o Transition Mode mantém a retrocompatibilidade, o que pode manter a exposição a ataques baseados em downgrade induzindo dispositivos WPA3 a retroceder ao WPA2.

A expectativa de resultado positivo varia significativamente entre as estratégias e depende do critério pelo qual o sucesso é avaliado, se pela continuidade operacional ou pelo nível de segurança efetiva alcançado. A estratégia de múltiplos SSIDs apresenta a maior probabilidade de resultado positivo sob ambos os critérios simultaneamente, pois dispositivos compatíveis passam a operar com os mecanismos de segurança do WPA3 no novo SSID, enquanto dispositivos legados permanecem funcionais na rede WPA2, sem gerar interrupções ou sobrecarga no suporte técnico, permitindo que o administrador acompanhe e o controle o andamento da migração.

O Transition Mode oferece um resultado positivo do ponto de vista da conectividade, uma vez que nenhum dispositivo é interrompido, mas representa um risco no quesito de segurança, porque como o WPA2 permanece ativo sob o mesmo nome de rede, atacantes podem forçar dispositivos a realizar downgrade de conexão, explorando as vulnerabilidades que a migração deveria eliminar. Diferentemente do Only Mode, que embora seja a estratégia mais segura a longo prazo, apresenta a menor expectativa de resultado positivo no curto prazo, pois se for ativado sem um inventário rigoroso prévio poderá haver interoperabilidade na rede, comprometendo a operação até que os dispositivos sejam substituídos ou atualizados.

O impacto sobre os processos internos da organização varia conforme o nível de controle e reestruturação que cada estratégia exige. O Only Mode provoca as mudanças mais drásticas durante o seu processo de migração, considerado a substituição dos dispositivos incompatíveis da empresa, tendo em vista que se deve garantir que nenhum dispositivo

esteja sem certificação explícita de suporte ao WPA3. A estratégia de múltiplos SSIDs implica mudanças moderadas, em virtude da equipe de TI que passa a gerenciar e monitorar duas ou mais VLANs e uma nova etapa de triagem onde é definido para qual rede cada equipamento será conectado. O Transition Mode, por sua vez, é a estratégia de menor impacto nos processos internos, convém ressaltar que a rede aceita ambos os protocolos sob o mesmo nome, praticamente nenhuma rotina tende a ter uma grande mudança, sendo a única mudança relevante a necessidade de documentar formalmente que a rede ainda opera com os riscos associados ao WPA2. A partir dos critérios analisados, o Quadro 1 apresenta uma síntese comparativa das estratégias de migração do WPA2 para o WPA3 em ambientes corporativos.

Quadro 1 – Comparação das estratégias de migração do WPA2 para o WPA3 em ambientes corporativos

Critério	Transition Mode	Múltiplos SSIDs	Only Mode
Investimento financeiro	Baixo. Permite manter temporariamente os equipamentos legados.	Moderado. Exige configuração de redes paralelas, políticas distintas e possível segmentação por VLANs.	Alto. Pode exigir substituição ou atualização de todos os dispositivos incompatíveis.
Prazo para a adoção integral do WPA3	Indefinido enquanto o WPA2 permanecer habilitado.	Gradual. Os dispositivos são transferidos progressivamente para a rede WPA3.	Imediato após a adequação completa da infraestrutura.
Nível de segurança alcançado	Limitado. Mantém a compatibilidade, mas preserva riscos associados ao WPA2.	Intermediário durante a transição. Permite adotar WPA3 gradualmente, mantendo os dispositivos legados em uma rede separada.	Elevado. Elimina a dependência do WPA2 após a migração.
Continuidade operacional	Elevada. Os dispositivos legados continuam conectados sem alterações significativas.	Elevada. A migração pode ocorrer progressivamente, reduzindo interrupções.	Condicional ao inventário prévio. Dispositivos incompatíveis podem perder conectividade.

Esforço técnico da equipe de TI	Baixo. Exige poucas mudanças operacionais imediatas.	Moderado. Requer gerenciamento de diferentes SSIDs, políticas de acesso e possíveis VLANs.	Alto. Exige inventário detalhado, testes de compatibilidade e adequação da infraestrutura.
Impacto nos processos internos	Baixo. A rotina da organização sofre poucas alterações.	Baixo. A rotina da organização sofre poucas alterações.	Alto. Pode exigir substituição de dispositivos e reorganização da infraestrutura.

Fonte: Elaborada pelos autores.

Conforme apresentado no Quadro 1, nenhuma das estratégias pode ser considerada acentuadamente superior em todos os critérios analisados. O Transition Mode apresenta menor custo e menor impacto inicial, mas não elimina integralmente os riscos associados ao WPA2. Em contraste, o Only Mode oferece o maior nível de segurança, embora dependa da compatibilidade dos dispositivos e possa demandar investimentos elevados. Nesse contexto, a estratégia de múltiplos SSIDs mostra-se a alternativa mais equilibrada para ambientes corporativos que necessitam realizar uma transição gradual, mantendo a continuidade operacional e ampliando progressivamente a adoção do WPA3.

5 CONCLUSÃO E PERSPECTIVAS

Ao longo do estudo, evidencia-se a importância da segurança em ambientes corporativos, todas as estratégias abordadas possuem processos de migração diferentes. Considerando aspectos financeiros e de negócios, foi possível demonstrar que a transição do WPA2 para o WPA3 é realizável sem comprometer a continuidade operacional, respeitando as limitações de compatibilidade dos dispositivos antigos, desde que seja conduzida de forma planejada, gradual e orientada às necessidades de cada organização.

Nota-se que a estratégia de múltiplos SSIDs oferece uma mudança sem suscetibilidade às vulnerabilidades aos novos dispositivos, permitindo a conexão à rede Wi-Fi dos dispositivos legados. A estratégia torna o processo mais equilibrado em termos financeiros e de negócio, haja vista seu impacto em tempo do ponto de vista técnico, demonstrando

mais estabilidade nas conexões, com menor risco sobre a segurança dos dispositivos compatíveis ao WPA3.

Essa possibilidade de utilização do protocolo incentiva a política de práticas de segurança, mesmo que o processo de substituição progressiva dos dispositivos possa ser considerado um custo a mais, é significativamente mais vantajoso do que remediar os danos causados por incidentes decorrentes do descuido com a proteção do ambiente corporativo. Dessa forma, conclui-se que a estratégia de migração gradual utilizando múltiplos SSIDs com o objetivo da adesão total do protocolo WPA3 em médio a curto prazo traz ganhos em confiabilidade na segurança da rede, evidenciando a importância do planejamento estratégico assegurando a responsabilidade da empresa para a sua conformidade legal e para com os seus clientes.

REFERÊNCIAS

- BARBOSA, Renan Rodrigo. Migração de redes tradicionais para SDN. **Dissertação (Mestrado em Ciência da Computação)** - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2018. Disponível em: https://teses.usp.br/teses/disponiveis/45/45134/tde-26032019-102837/publico/Dissertacao_Renan_Corrigida.pdf. Acesso em: 1 jun. 2026.
- CONCEIÇÃO JÚNIOR, André Lisboa da. História dos protocolos de redes sem fio. **Revista Tempo Amazônico**, v. 4, n. 1, jul.–dez. 2016, p. 62–90. Disponível em: https://www.ap.anpuh.org/download/download?ID_DOWNLOAD=1966. Acesso em: 28 fev. 2026.
- GHANIM, Asmaa A.; THANOUN, Mohammed Y. Evaluating the Effectiveness of WPA3 Protocol against Advanced Hacking Attacks. **International Journal of Wireless and Microwave Technologies**, v. 15, n. 4, p. 1-18, 2025. Disponível em: <https://doi.org/10.5815/ijwmt.2025.04.01>. Acesso em: 20 mar. 2026.
- MATHEW, Alex; JACKSON, Emma; TOBESMAN, Audrey. Evaluating the Efficacy of WPA3 against Advanced Attacks: A Comparative Analysis with WPA2 in Real-World. **Journal of Information Technology and Integrity**, v.3, n.1, p.105, 2025. Disponível em: <https://doi.org/10.33790/jiti1100105>. Acesso em: 20 mar. 2026.

NAJAR, Zahoor Ahmad; MIR, Roohe Naaz. Wi-Fi: WPA2 Security Vulnerability and Solutions. **Wireless Engineering and Technology**, v. 12, n. 02, p. 15–22, 2021. Disponível em: <https://doi.org/10.4236/wet.2021.12200>. Acesso em: 28 fev. 2026

NETO, José Pedro Alves. Segurança e Vulnerabilidades em Redes Wi-Fi E Móveis: Riscos e Proteção de Dados em Transações Bancárias. **Revista Contemporânea**, [S. l.], v. 5, n. 5, p. e8257, 2025. Disponível em: <https://ojs.revistacontemporanea.com/ojs/index.php/home/article/view/8257>. Acesso em: 30 jul. 2026.

SHARMA, Raksha. Wi-Fi Security Market Research Report 2034. **Market Intelo**, 11 jun. 2026. Disponível em: <https://marketintelo.com/report/wi-fi-security-market>. Acesso em: 30 jul. 2026.

VANHOEF, Mathy; PIESENS, Frank. Key reinstallation attacks: Forcing nonce reuse in WPA2. In: **New York, NY, USA: ACM**, 2017. Disponível em: <https://doi.org/10.1145/3133956.3134027>. Acesso em: 21 abr. 2026

VANHOEF, Mathy; RONEN, Eyal. Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. **Cryptology ePrint Archive**, Paper 2019/383. Disponível em: <https://eprint.iacr.org/2019/383>. Acesso em: 21 abr. 2026.

WI-FI ALLIANCE. WPA3™ and Wi-Fi Enhanced™ Open Deployment and Implementation Guide Version 1.1. **Wi-Fi Alliance**: 2025. PDF. Disponível em: <https://www.wi-fi.org/system/files/WPA3%20and%20Wi-Fi%20Enhanced%20Open%20Deployment%20Guide%20v1.1.pdf>. Acesso em: 27 maio 2026.

WI-FI ALLIANCE. **WPA3™ deployment Options**. Wi-Fi Alliance: 2024. PDF. Disponível em: https://www.wi-fi.org/system/files/WPA3_Deployment_Options_Highlights_20241125.pdf. Acesso em: 27 maio 2026.