INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA

CAMPUS CAMPINA GRANDE

CURSO SUPERIOR DE TECNOLOGIA EM TELEMÁTICA

KILARY BAYMA XIMENES VASCONCELOS

REVISÃO SISTEMÁTICA DE SEGURANÇA EM REDES 5G: DESAFIOS E SOLUÇÕES PARA A NOVA ERA DAS TELECOMUNICAÇÕES

CAMPINA GRANDE - PB

2025

KILARY BAYMA XIMENES VASCONCELOS

REVISÃO SISTEMÁTICA DE SEGURANÇA EM REDES 5G: DESAFIOS E SOLUÇÕES PARA A NOVA ERA DAS TELECOMUNICAÇÕES

Trabalho de Conclusão de Curso apresentado ao Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, Campus Campina Grande, como requisito parcial para conclusão do Curso Superior de Tecnologia em Telemática.

CAMPINA GRANDE - PB

2025

Catalogação na fonte:
Ficha catalográfica elaborada por Gustavo César Nogueira da Costa - CRB 15/479

V331r Vasconcelos, Kilary Bayma Ximenes.

Revisão sistemática de segurança em redes 5G: desafios e soluções para a nova era das telecomunicações / Kilary Bayma Ximenes Vasconcelos. - Campina Grande, 2025.
47 f.: il.

Trabalho de Conclusão de Curso (Graduação em Tecnologia em Telemática) - Instituto Federal da Paraíba, 2025.
Orientadores: Prof. Dr. Éwerton Rômulo S. Castro.

1. Redes móveis - 5G. 2. Segurança da informação. 3. Cibersegurança em telecomunicações. 4. Telemática - Aplicações em cidades inteligentes. I. Castro, Éwerton Rômulo S. II. Título.
.

CDU 004.056

KILARY BAYMA XIMENES VASCONCELOS

REVISÃO SISTEMÁTICA DE SEGURANÇA EM REDES 5G: DESAFIOS E SOLUÇÕES PARA A NOVA ERA DAS TELECOMUNICAÇÕES

Trabalho de Conclusão de Curso apresentado ao Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, Campus Campina Grande, como requisito parcial para conclusão do Curso Superior de Tecnologia em Telemática.

Aprovado em 11 de agosto de 2025.

BANCA EXAMINADORA

_____

Prof. Dr. Éwerton Rômulo S. Castro (Orientador - IFPB)

_____

Profª. M.Sc. Iana Daya Cavalcante Facundo Passos (Examinador - IFPB)

_____

Prof. M.Sc. Bruno de Brito Leite (Examinador - IFPB)

AGRADECIMENTOS

Primeiramente, agradeço a minha esposa Alana Ramalho, por me guiar, motivar e me dar forças em todos os momentos dessa jornada. Sem a sua presença constante, este trabalho não seria possível. Seu amor sempre me deu coragem para seguir em frente, mesmo nas dificuldades.

Aos meus pais, minha eterna gratidão por me proporcionarem tudo o que sou hoje. O exemplo de dedicação, amor e sacrifício que sempre demonstraram, é a base sobre a qual construí minha trajetória acadêmica e pessoal.

Ao meu orientador, Prof. Dr. Éwerton Rômulo S. Castro, pela orientação, paciência e sabedoria ao longo de todo o processo. Suas contribuições foram fundamentais para a realização deste trabalho e para o meu crescimento acadêmico e profissional.

Aos meus amigos e a todos que são importantes para mim, meu sincero agradecimento por estarem ao meu lado, oferecendo palavras de apoio, motivação e, muitas vezes, um ombro amigo. Cada um de vocês fez a diferença nesta caminhada.

A todos, meu muito obrigado.

LISTA DE SIGLAS

3GPP	*3rd Generation Partnership Project* (Projeto de Parceria de 3ª Geração)
5G	Quinta geração de redes móveis
5G-AKA	*5G Authentication and Key Agreement* (Autenticação de Acesso para Redes Móveis 5G)
5GC	*5G Core (Núcleo da Rede 5G)*
5G NR	*5G New Radio* (5G Novo Rádio)
AES	*Advanced Encryption Standard* (Padrão Avançado de Criptografia)
AM	Aprendizado de Máquina
AMF	*Access and Mobility Management Function* (Função de Gerenciamento de Acesso e Mobilidade)
AMPS	*Advanced Mobile Phone System* (Sistema Avançado de Telefonia Móvel)
ANATEL	Agência Nacional de Telecomunicações
CEBRI	Centro Brasileiro de Relações Internacionais
CNN	*Convolutional Neural Networks* (Redes Neurais Convolucionais)
CUPS	*Control and User Plane Separation* (Separação do Plano de Controle e Usuário)
DoS	*Denial of Ser*vice (Negação de Serviço)
DDoS	*Distributed Denial of Service* (Negação de Serviço Distribuído)
ECC	*Elliptic Curve Cryptography* (Criptografia de Curvas Elípticas)
eMBB	*Enhanced Mobile Broadband* (Banda Larga Móvel Aprimorada)
EPC	*Evolved Packet Core* (Núcleo de Pacotes Evoluído)
ETSI	*European Telecommunications Standards Institute* (Instituto Europeu de Padrões de Telecomunicações)
GDPR	*General Data Protection Regulation* (Regulamento Geral de Proteção de Dados)
GS NFV-SEC	*Group Specification; Network Functions Virtualization; Security* (Especificações de Grupo; Virtualização de Funções de Rede; Segurança)
GSM	*Global System for Mobile Communications* (Sistema Global para Comunicações Móveis)
IA	Inteligência Artificial
IEC	*International Electrotechnical Commission* (Comissão Eletrotécnica Internacional)
IMSI	*International Mobile Subscriber Identity* (Identidade Internacional de Assinante Móvel)
IMT-2020	*International Mobile Telecommunications-2020* (Telecomunicações Móveis Internacionais-2020)
IoT	*Internet of Things* (Internet das Coisas)
ISO	*International Organization for Standardization* (Organização Internacional de Normalização)
ITU	*International Telecommunication Union* (União Internacional de Telecomunicações)
LGPD	Lei Geral de Proteção de Dados
LSTM	*Long Short-Term Memory* (Memória de Longo e Curto Prazo)
LTE	*Long Term Evolution* (Evolução de Longo Prazo)
MANO	*Management and Orchestration* (Gerenciamento e Orquestração)

MEC	*Multi-access Edge Computing* (Computação de Borda de Acesso Múltiplo)
MitM	*Man-in-the-Middle* (Homem no Meio)
mMTC	*massive Machine-Type Communications* (Comunicações Massivas entre Máquinas)
NFV	*Network Functions Virtualization* (Virtualização de Funções de Rede)
NFVI	*Network Functions Virtualization Infrastructure* (Infraestrutura de Virtualização de Funções de Rede)
NIST	*National Institute of Standards and Technology* (Instituto Nacional de Padrões e Tecnologia)
PCF	*Policy Control Function* (Função de Controle de Políticas)
PQC	*Post-Quantum Cryptography* (Criptografia Pós-Quântica)
PRISMA	*Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (Itens Preferenciais para Relato de Revisões Sistemáticas e Meta-análises)
QoS	*Quality of Service* (Qualidade do Serviço)
RAN	*Radio Access Network* (Rede de Acesso por Rádio)
RNN	*Recurrent Neural Networks* (Redes Neurais Recorrentes)
RSA	*Rivest–Shamir–Adleman* (Rivest–Shamir–Adleman – algoritmo de criptografia)
SBA	*Service-Based Architecture* (Arquitetura Baseada em Serviços)
SDN	*Software Defined Networking* (Redes Definidas por Software)
SEPP	*Security Edge Protection Proxy* (Proxy de Proteção de Borda de Segurança)
SMF	*Session Management Function* (Função de Gerenciamento de Sessão)
SMS	*Short Message Service* (Serviço de Mensagens Curtas)
SUCI	*Subscription Concealed Identifier* (Identificador de Assinante Oculto)
SUPI	*Subscription Permanent Identifier* (Identificador Permanente de Assinante)
UAVs	*Unmanned Aerial Vehicles* (Veículos Aéreos Não Tripulados)
UPF	*User Plane Function* (Função do Plano de Usuário)
URLLC	*Ultra-Reliable Low-Latency Communications* (Comunicações Ultra-Confiáveis e de Baixa Latência)
V2X	*Vehicle-to-Everything* (Veiculo Para Tudo)
VANETs	*Vehicular Ad Hoc Networks* (Redes Veiculares Ad Hoc)
VNF	*Virtual Network Functions* (Funções de Rede Virtualizadas)
XAI	*Explainable AI* (Inteligência Artificial Explicável)
XR	*Extended Reality* (Realidade Estendida)
ZTA	*Zero Trust Architecture* (Arquitetura de Confiança Zero)

LISTA DE QUADROS

RESUMO

Este trabalho faz uma revisão sistemática buscando analisar as vulnerabilidades e estratégias de proteção associadas à segurança nas redes 5G, destacando seu papel como infraestrutura crítica para aplicações em áreas como saúde, transporte e cidades inteligentes. A pesquisa apresenta a evolução das gerações de redes móveis, com ênfase nas mudanças introduzidas pela arquitetura 5G, que incorpora tecnologias como SDN (*Software Defined Networking* - Redes Definidas por Software), NFV (*Network Functions Virtualization* - Virtualização de Funções de Rede), SBA (*Service-Based Architecture* - Arquitetura Baseada em Serviços) e computação em borda, as quais ampliam tanto o desempenho quanto os vetores de ataque. A abordagem metodológica foi fundamentada em revisão sistemática, englobando documentos normativos, publicações técnicas e artigos científicos. O estudo discute ameaças específicas à privacidade, autenticação, integridade de dados e gerenciamento de identidades, propondo soluções baseadas em criptografia avançada, *blockchain* e inteligência artificial. Além disso, considera os impactos regulatórios de normativas como a LGPD (Lei Geral de Proteção de Dados), GDPR (*General Data Protection Regulation* - Regulamento Geral de Proteção de Dados) e recomendações da ITU (*International Telecommunication Union* - União Internacional de Telecomunicações). Conclui-se que a segurança na 5G requer uma atuação conjunta entre inovação tecnológica, padronização internacional e políticas públicas voltadas à cibersegurança.

Palavras-chave: Redes 5G, Segurança, Cibersegurança, Criptografia, Inteligência Artificial.

ABSTRACT

This paper conducts a systematic review seeking to analyze the vulnerabilities and protection strategies associated with security in 5G networks, highlighting their role as critical infrastructure for applications in areas such as healthcare, transportation, and smart cities. The research presents the evolution of mobile network generations, with an emphasis on the changes introduced by 5G architecture, which incorporates technologies such as SDN (Software Defined Networking), NFV (Network Functions Virtualization), SBA (Service-Based Architecture), and edge computing, which expand both performance and attack vectors. The methodological approach was based on a systematic review, encompassing regulatory documents, technical publications, and scientific articles. The study discusses specific threats to privacy, authentication, data integrity, and identity management, proposing solutions based on advanced cryptography, blockchain, and artificial intelligence. In addition, it considers the regulatory impacts of standards such as LGPD (*Lei Geral de Proteção de Dados* - General Data Protection Law), GDPR (General Data Protection Regulation), and ITU (International Telecommunication Union) recommendations. It concludes that security in 5G requires joint action between technological innovation, international standardization, and public policies focused on cybersecurity.

Key-words: 5G Networks, Security, Cybersecurity, Cryptography, Artificial Intelligence.

SUMÁRIO

1. INTRODUÇÃO

A evolução das redes móveis tem sido um marco determinante na transformação digital contemporânea. Desde a primeira geração, limitada a chamadas de voz analógicas, até as tecnologias 2G, 3G e 4G, cada avanço proporcionou maior conectividade e acesso à informação (MICELI et al., 2022; BARBOSA et al., 2021).

A implementação da 4G, por exemplo, possibilitou a consolidação da internet móvel de alta velocidade, ampliando a utilização de aplicações multimídia e serviços baseados em dados (AHAD et al., 2023).

Neste cenário em constante evolução, a quinta geração (5G) surge não como uma simples atualização incremental, mas como um verdadeiro divisor de águas para as telecomunicações.

Caracterizada por altas taxas de transmissão, baixa latência, elevada densidade de conexões e eficiência energética, essa tecnologia representa a base para uma série de aplicações críticas, tais como IoT (*Internet of Things* - Internet das Coisas), veículos autônomos, telemedicina e cidades inteligentes (MICELI et al., 2022; AHAD et al., 2023). Com essa nova infraestrutura, espera-se uma transformação profunda nos setores industrial, governamental e social, consolidando a 5G como alicerce da economia digital.

Entretanto, os benefícios associados a 5G vêm acompanhados de desafios crescentes em termos de cibersegurança. A arquitetura desta tecnologia, que incorpora recursos avançados como *edge computing* (computação em borda), NFV (*Network Functions Virtualization* - Virtualização de Funções de Rede) e SDN (*Software Defined Networking* - Redes Definidas por Software), amplia significativamente a superfície de ataque, tornando insuficientes os mecanismos tradicionais de proteção (SOBRINHO; SILVA; SANTOS, 2023).

A hiperconectividade resultante, envolvendo bilhões de dispositivos em rede, eleva a criticidade da proteção de dados e a necessidade de mecanismos robustos para mitigar riscos, especialmente em aplicações sensíveis, como saúde, transporte automatizado e gestão urbana (LIMA, 2024).

Esse contexto evidencia a urgência no desenvolvimento e na implementação de estratégias inovadoras de segurança. Entre as abordagens emergentes, destacam-se soluções baseadas em autenticação robusta, criptografia avançada, fatiamento

lógico de redes, orquestração segura e uso de inteligência artificial para monitoramento e prevenção de ataques. Além dos aspectos técnicos, questões regulatórias e normativas, como a LGPD (Lei Geral de Proteção de Dados) e padrões internacionais definidos por entidades como 3GPP (*3rd Generation Partnership Project* - Projeto de Parceria de 3ª Geração) e ETSI (*European Telecommunications Standards Institute* - Instituto Europeu de Padrões de Telecomunicações), exercem papel central na governança dessas infraestruturas críticas (MICELI et al., 2022).

A justificativa para este estudo fundamenta-se na relevância acadêmica, social e prática do tema. Do ponto de vista acadêmico, a pesquisa contribui para a ampliação do conhecimento acerca da segurança em redes móveis de nova geração, fornecendo um panorama consolidado sobre desafios e soluções tecnológicas já propostas ou em desenvolvimento.

Socialmente, o tema mostra-se essencial diante da rápida implementação de tecnologias que sustentam setores críticos da economia digital, como a Indústria 4.0, os serviços de saúde conectados e os sistemas inteligentes de transporte, cuja continuidade e confiabilidade dependem diretamente da segurança das comunicações (SOBRINHO; SILVA; SANTOS, 2023).

Para atingir os objetivos propostos, este trabalho empregará uma revisão sistemática da literatura, analisando artigos científicos, relatórios técnicos e documentos normativos que abordam a segurança no contexto da 5G.

Essa abordagem permitirá identificar vulnerabilidades, mapear riscos, avaliar soluções tecnológicas e regulamentares, além de comparar estratégias de mitigação implementadas em diferentes cenários, garantindo uma análise crítica e abrangente das tendências atuais.

Dessa forma, busca-se oferecer subsídios para uma melhor compreensão do problema e a proposição de recomendações fundamentadas para a proteção das redes de quinta geração.

No âmbito dessa investigação, o objetivo geral consiste em realizar uma revisão sistemática da literatura especializada para identificar e analisar os principais desafios de segurança das redes 5G, bem como as soluções técnicas, científicas e regulatórias propostas para mitigar esses riscos.

1.1. OBJETIVO GERAL

Realizar uma revisão sistemática da literatura para identificar e analisar os principais desafios de segurança das redes 5G, bem como as soluções técnicas, científicas e regulatórias propostas para mitigar esses riscos.

1.2. OBJETIVOS ESPECÍFICOS

a) Mapear as vulnerabilidades e ameaças mais relevantes na arquitetura 5G, considerando sua integração com tecnologias emergentes como IoT, conforme suas identificações em outros trabalhos acadêmicos.

b) Identificar e descrever as estratégias tecnológicas e científicas aplicadas à proteção das redes 5G, incluindo criptografia, autenticação, fatiamento de rede e inteligência artificial.

c) Analisar soluções implementadas por organizações e empresas internacionais, destacando resultados e limitações.

d) Comparar diferentes abordagens de mitigação, avaliando sua efetividade frente aos riscos mapeados.

e) Discutir os impactos regulatórios e normativos relacionados à segurança nas redes 5G, com base em padrões internacionais e legislações vigentes.

2. METODOLOGIA

A presente pesquisa adotou uma abordagem metodológica aplicada, com caráter bibliográfico e exploratório, fundamentada na realização de uma revisão sistemática da literatura. Essa escolha se justifica pela necessidade de consolidar informações técnicas, científicas e normativas sobre segurança em redes 5G, permitindo compreender de forma crítica os desafios existentes e as soluções propostas para mitigar vulnerabilidades. A opção por uma revisão sistemática, em detrimento de revisões narrativas, garante maior rigor metodológico e transparência no processo de seleção, análise e síntese dos estudos (PRISMA, 2020).

O estudo contemplou publicações produzidas no período de 2019 a 2024, intervalo definido por coincidir com a fase de intensificação da implantação das redes 5G em escala global. Essa delimitação temporal assegura que as soluções analisadas reflitam as demandas atuais e as tendências mais recentes em segurança cibernética.

As fontes foram obtidas em bases acadêmicas amplamente reconhecidas, como IEEE Xplore, ScienceDirect e Scopus, bem como em repositórios de normas técnicas e regulatórias, tais como 3GPP, ETSI e ITU (*International Telecommunication Union* - União Internacional de Telecomunicações). Adicionalmente, foram analisados relatórios técnicos e "*white papers"* de fabricantes líderes do setor, como Huawei, Ericsson e Nokia, dada a relevância prática dessas informações para o ecossistema de telecomunicações. A busca foi conduzida em português e inglês, utilizando-se as seguintes palavras-chave: "segurança em redes 5G", "*5G security*", "*cybersecurity* 5G", "*network slicing*", "NFV", "SDN", "*blockchain*" e "inteligência artificial em redes móveis".

O processo de seleção dos estudos seguiu rigorosamente as diretrizes estabelecidas pelo método PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses* – Itens Preferenciais para Relato de Revisões Sistemáticas e Meta-análises), amplamente reconhecido por conferir transparência e padronização a revisões sistemáticas (PRISMA, 2020).

Inicialmente, na etapa de Identificação, foram levantados 83 registros a partir das estratégias de busca definidas, abrangendo as bases de dados e repositórios previamente selecionados.

Em seguida, ocorreu a fase de Triagem, que consistiu na exclusão de 19 duplicatas, resultando em 64 documentos únicos. Nessa fase, foram aplicados filtros relacionados ao escopo da pesquisa, como tema, período de publicação (2019–2024), idioma (Português e Inglês) e tipo de documento, levando à exclusão de 32 estudos que não atendiam a esses critérios (MOHER et al., 2009).

Na sequência, procedeu-se à etapa de Elegibilidade, com leitura de resumos e análise preliminar do conteúdo para verificar a pertinência das publicações em relação ao objetivo central do estudo. Nessa fase, 32 trabalhos foram avaliados integralmente e, após a leitura crítica em texto completo, 25 foram excluídos por razões como ausência de evidências técnicas consistentes, foco fora do escopo 5G, redundância ou acesso incompleto ao conteúdo.

Finalmente, na fase de Inclusão, permaneceram apenas 7 estudos, os quais atenderam integralmente aos critérios metodológicos estabelecidos, garantindo, assim, a relevância e a qualidade do material utilizado na análise crítica.

Os critérios de inclusão, conforme o Quadro 1, abrangeram publicações revisadas por pares (*peer-reviewed*), normas técnicas oficiais e documentos emitidos por organizações reconhecidas internacionalmente. Foram excluídos estudos redundantes, duplicados ou que não abordassem diretamente aspectos relacionados à segurança em redes 5G.

Quadro 1 - Critérios Metodológicos da Escolha de Bibliografia

Critério	Descrição Aplicada na Pesquisa
Bases de Dados Consultadas	IEEE Xplore, ScienceDirect, Scopus, 3GPP, ETSI, ITU, relatórios técnicos e *white papers* de fabricantes (Huawei, Ericsson, Nokia).
Período de Publicação	2019 a 2024
Palavras-chave Utilizadas	"segurança em redes 5G", "*5G security*", "*cybersecurity 5G*", "*network slicing*", "NFV", "SDN", "*blockchain*", "inteligência artificial em redes móveis", "LGPD e 5G".
Idioma dos Documentos	Português e Inglês
Critérios de Qualidade	Publicações revisadas por pares (*peer-reviewed*), normas técnicas oficiais e *white papers* de fornecedores líderes com reconhecimento internacional.
Exclusão de Duplicatas	Documentos duplicados ou com conteúdo redundante foram eliminados durante a triagem.
Etapas de Seleção (PRISMA)	- **Identificação**: levantamento inicial nas bases e repositórios listados.
	- **Triagem**: aplicação de filtros de tema, ano, tipo de documento e idioma.
	- **Elegibilidade**: verificação do conteúdo e relevância técnica.
	- **Inclusão**: seleção final para análise e discussão crítica.

Fonte: Elaborado pelo Autor, 2025.

Após a seleção, os trabalhos foram organizados em três eixos temáticos: (i) ameaças e vulnerabilidades; (ii) soluções tecnológicas (como criptografia, autenticação, inteligência artificial e *blockchain*); e (iii) governança normativa e regulatória. Essa estruturação possibilitou a realização de uma análise crítica e comparativa entre diferentes abordagens, considerando aplicabilidade prática, grau de inovação, efetividade e conformidade com padrões internacionais. Embora a pesquisa seja predominantemente qualitativa, incorporou elementos quantitativos, como a contagem de publicações por eixo temático e ano de publicação, a fim de identificar tendências relevantes.

O fluxograma metodológico baseado no PRISMA sintetizou as etapas realizadas, garantindo rigor na triagem e redução da amostra. O processo partiu de um levantamento inicial com aproximadamente 83 trabalhos, após a aplicação dos critérios de inclusão e exclusão, resultou-se em um total de 7 publicações escolhidas, para a análise final, conforme o Quadro 2. Essa filtragem assegurou consistência e relevância para a análise desenvolvida, oferecendo uma base sólida para a discussão crítica apresentada nos capítulos subsequentes.

Quadro 2 - Artigos Bibliográficos Selecionados

Autor/Instituição	**Título do Documento**	**Ano**
Barbosa, G. N. N. et al.	*Segurança em Redes 5G: Oportunidades e Desafios em Detecção de Anomalias e Predição de Tráfego*	2021
CEBRI	*A Segurança Cibernética e a Tecnologia 5G no Cenário Brasileiro*	2020
ETSI	*ETSI GS NFV-SEC 012 – Security Guidelines for NFV*	2022
3GPP	*TS 33.501 – Security architecture and procedures for 5G System*	2023
Huawei, Ericsson, Nokia	*White Papers sobre segurança e redes 5G*	2020–2023
Lima, L. C.	*Segurança em Redes 5G: Desafios Atuais e Perspectivas Futuras*	2024
Salahdine, F. et al.	*Security in 5G and beyond: Recent advances and future challenges*	2022

Fonte: Elaborado pelo Autor, 2025.

3. REVISÃO DE LITERATURA

A evolução das redes móveis, desde a 1G até a 5G, reflete um processo de transformação tecnológica contínua, que tem atendido à crescente demanda por conectividade e desempenho. À medida que cada geração trouxe avanços significativos em termos de velocidade, capacidade e mobilidade, novos desafios surgiram, especialmente no que tange à segurança e governança das redes.

A transição para a 5G não apenas revoluciona as telecomunicações, mas também exige uma revisão e atualização de normas e regulamentos, que precisam acompanhar a complexidade das novas arquiteturas e tecnologias implementadas. Este tópico abordará as principais normas, padrões técnicos e diretrizes regulatórias que sustentam a segurança das redes 5G, além de explorar o papel de organismos internacionais e agências reguladoras na construção de um ambiente seguro e resiliente.

3.1. EVOLUÇÃO DAS REDES MÓVEIS: DA 1G À 5G

A trajetória da telefonia móvel, desde sua origem analógica até as avançadas redes digitais de quinta geração, reflete uma evolução tecnológica guiada pela crescente demanda por conectividade, velocidade e mobilidade. Cada geração de rede móvel marcou um estágio significativo no desenvolvimento das telecomunicações, respondendo a diferentes necessidades sociais, técnicas e econômicas ao longo do tempo.

A primeira geração (1G), introduzida no final da década de 1970 e início dos anos 1980, utilizava sinais analógicos e oferecia apenas serviços de voz. Sistemas como o AMPS (*Advanced Mobile Phone System* – Sistema Avançado de Telefonia Móvel) apresentavam baixa capacidade de comunicação, quase nenhuma segurança e qualidade de áudio vulnerável a ruídos e interferências (BARBOSA et al., 2021; LIMA, 2024).

Com os avanços da tecnologia digital, surgiu a segunda geração (2G), no início dos anos 1990. Utilizando modulação digital, essa geração trouxe melhorias significativas na qualidade das chamadas, maior capacidade de rede e a introdução de protocolos de criptografia, ampliando a segurança das comunicações. Além disso,

possibilitou o envio de SMS (*Short Message Service* – Serviço de Mensagens Curtas). O padrão GSM (*Global System for Mobile Communications* – Sistema Global para Comunicações Móveis) tornou-se dominante em diversas regiões, permitindo o *roaming* internacional e promovendo a popularização da telefonia móvel (AHAD et al., 2023; SOBRINHO; SILVA; SANTOS, 2023).

A terceira geração (3G), lançada no final dos anos 1990, introduziu o acesso à internet móvel em velocidades compatíveis com navegação na *web*, envio de *e-mails* e uso de redes sociais. Com taxas de transmissão de até 2 Mbps, essa geração impulsionou a disseminação dos *smartphones* e o crescimento dos aplicativos móveis. Também trouxe mecanismos mais robustos de autenticação, elevando o nível de segurança das redes móveis (BARBOSA et al., 2021; SALAHDINE et al., 2022).

A quarta geração (4G), implementada a partir da década de 2010, representou um avanço qualitativo importante com a adoção da tecnologia LTE (*Long Term Evolution* - Evolução de Longo Prazo). Essa tecnologia proporcionou velocidades superiores a 100 Mbps, baixa latência e suporte a aplicações multimídia, como vídeos em alta definição e videoconferências. O 4G consolidou o conceito de banda larga móvel, ampliando significativamente o acesso à informação e ao entretenimento em qualquer lugar (MICELI et al., 2022; LIMA, 2024).

Contudo, limitações como latência elevada, baixa eficiência espectral, suporte restrito a dispositivos e insuficiente robustez para aplicações críticas motivaram o desenvolvimento da quinta geração (5G). Essa nova geração surgiu como uma plataforma convergente, capaz de oferecer conectividade ultrarrápida, latência inferior a 1 milissegundo, alta confiabilidade e suporte a conexões massivas de dispositivos (ITU, 2020; AHAD et al., 2023).

Mais do que uma simples evolução, a 5G representa uma ruptura tecnológica. Com recursos como *network slicing* (fatiamento de rede), NFV, *edge computing* e inteligência artificial embarcada, a 5G permite a personalização de serviços conforme o setor ou aplicação. Essa flexibilidade é essencial para viabilizar aplicações críticas, como cirurgias remotas, veículos autônomos, cidades inteligentes, sistemas industriais automatizados e dispositivos IoT em larga escala (AHAD et al., 2023; BARBOSA et al., 2021; SALAHDINE et al., 2022).

No cenário da transformação digital, a 5G constitui a base para a implementação de conceitos como Indústria 4.0, cidades inteligentes, telemedicina e

sistemas de transporte conectados. Sua capacidade de lidar com grandes volumes de dados em tempo real, aliada à resiliência operacional, o torna fundamental para o avanço de setores estratégicos e para o desenvolvimento sustentável dos países (CEBRI, 2020; LIMA, 2024).

Em síntese, a evolução das redes móveis representa não apenas um avanço técnico, mas uma transformação profunda nas formas de interação entre pessoas, dispositivos e sistemas. A 5G, com seu caráter disruptivo, configura-se como o alicerce dessa nova era digital, embora traga consigo novos desafios em termos de segurança, privacidade e governança — temas que serão abordados nas próximas seções deste trabalho.

3.2. ARQUITETURA E TECNOLOGIAS-CHAVE DA 5G

A arquitetura da quinta geração de redes móveis (5G) representa uma transformação profunda em relação às gerações anteriores, promovendo não apenas ganhos em desempenho, mas também uma nova forma de conceber, operar e proteger redes de telecomunicações. A 5G foi desenhada para atender a três principais cenários de uso definidos pela ITU: eMBB (*Enhanced Mobile Broadband* - banda larga móvel aprimorada), URLLC (*Ultra-Reliable Low-Latency Communications* - Comunicações Ultra-Confiáveis e de Baixa Latência) e mMTC (*massive Machine-Type Communications* - Comunicações Massivas entre Máquinas) (ITU, 2020).

3.2.1. Estrutura Geral da Arquitetura 5G

A arquitetura das redes 5G foi concebida para atender a demandas contemporâneas de conectividade, como baixa latência, alta confiabilidade, escalabilidade e integração de dispositivos heterogêneos. Diferentemente das gerações anteriores, a 5G é estruturada sobre uma arquitetura orientada a serviços SBA (*Service-Based Architecture* - Arquitetura Baseada em Serviços), onde as funções de rede são desmembradas em módulos independentes, acessíveis por meio de interfaces abertas e padronizadas, em substituição ao modelo monolítico tradicional utilizado até o 4G (3GPP, 2020).

Essa desagregação funcional permite a implementação de serviços em ambientes nativamente virtualizados e baseados em nuvem, com grande flexibilidade para escalar funções de rede sob demanda. Em outras palavras, ao invés de depender de dispositivos físicos específicos para executar funções de controle, roteamento ou autenticação, a arquitetura 5G viabiliza a execução dessas funções como *softwares* distribuídos em infraestruturas de *data centers*, sejam locais (*edge*), regionais ou centrais (*core*), conforme o caso de uso e os requisitos de desempenho (AHAD et al., 2023).

Um dos aspectos centrais dessa arquitetura é a separação entre o plano de controle e o plano de usuário. Essa distinção, já presente de forma incipiente na 4G/LTE, foi aprofundada na 5G, com o objetivo de permitir o processamento independente de sinalização e tráfego de dados, otimizando a alocação de recursos e a distribuição funcional da rede (SALAHDINE et al., 2022). Enquanto o plano de controle trata de tarefas como gerência de sessão, mobilidade, autenticação e políticas de segurança, o plano de usuário é responsável pela transmissão dos dados do usuário final, como vídeos, chamadas e dados de sensores IoT.

Esse modelo é potencializado pelo uso de SDN, que promovem a abstração da infraestrutura física e possibilitam o gerenciamento centralizado e programável da rede. A combinação de SDN com NFV permite que os provedores criem, ajustem e encerrem funções de rede virtualizadas dinamicamente, segundo as exigências de tráfego, segurança e prioridade (BARBOSA et al., 2021).

Adicionalmente, a SBA promove comunicação entre funções de rede via *APIs RESTful*, o que simplifica a interoperabilidade e a integração com aplicações de terceiros. As funções de rede no núcleo da 5G — como o AMF (*Access and Mobility Management Function* - Função de Gerenciamento de Acesso e Mobilidade), o SMF (*Session Management Function* - Função de Gerenciamento de Sessão) e o UPF (*User Plane Function* - Função do Plano de Usuário) — são implementadas como microsserviços, que podem ser escalados e orquestrados de maneira granular, reduzindo o risco de falhas sistêmicas e aumentando a resiliência da rede (MICELI et al., 2022).

Outro elemento distintivo da arquitetura da 5G é sua capacidade de operar de forma convergente com múltiplas tecnologias de acesso, incluindo *5G* NR (5G *New Radio* – 5G Novo Rádio), 4G LTE, Wi-Fi e futuras gerações, utilizando o mesmo núcleo

de rede. Essa convergência é gerenciada por meio do conceito de CUPS (*Control and User Plane Separation* - Separação do Plano de Controle e Usuário), que oferece suporte à mobilidade entre diferentes acessos com mínima interrupção e sobrecarga (SOBRINHO; SILVA; SANTOS, 2023).

A arquitetura 5G, portanto, marca a transição de redes estáticas e inflexíveis para um ecossistema altamente dinâmico, orientado a serviços, interoperável e fortemente dependente de *software*. Essa nova lógica traz ganhos significativos, mas também amplia os vetores de ataque, exigindo novas estratégias de segurança, como veremos em seções posteriores.

3.2.2. Evolução do *Core* da Rede 5G

O núcleo da rede 5G, conhecido como 5GC (*5G Core* - Núcleo da Rede 5G), constitui um avanço disruptivo em relação às arquiteturas anteriores, substituindo o EPC (*Evolved Packet Core* – Núcleo de Pacotes Evoluído) da 4G. Enquanto o EPC era baseado em elementos físicos e apresentava uma estrutura relativamente rígida, o 5GC é nativamente virtualizado, baseado em nuvem e estruturado sob uma arquitetura orientada a serviços, o que proporciona maior flexibilidade, escalabilidade e segurança (3GPP, 2020).

Essa transformação responde às crescentes demandas por conectividade de alta densidade, baixa latência, resiliência operacional e customização de rede para diferentes verticais industriais. No 5GC, funções antes monolíticas são reorganizadas em microsserviços autônomos — como o AMF, o SMF, o PCF (*Policy Control Function* - Função de Controle de Políticas) e o UPF. Essas funções operam como instâncias independentes e se comunicam por meio de interfaces padronizadas baseadas em *APIs RESTful*, o que permite uma orquestração inteligente da rede (MICELI et al., 2022; SALAHDINE et al., 2022).

Um dos principais diferenciais do 5GC é sua capacidade de atuar como um núcleo convergente para diversas tecnologias de acesso, como 5G NR, LTE, Wi-Fi 6 e futuras evoluções. Essa convergência é viabilizada pelo CUPS (*Control and User Plane Separation* – Separação do Plano de Controle e Usuário), que otimiza o encaminhamento do tráfego de dados, independentemente da tecnologia de acesso, mantendo o controle e a gestão de sessões de forma centralizada (AHAD et al., 2023).

Essa separação é essencial para assegurar o desempenho de aplicações críticas, como cirurgias remotas, comunicações veiculares V2X (*Vehicle-to-Everything* – Veiculo Para Tudo) e sistemas industriais autônomos.

O 5GC foi concebido para operar em ambientes virtualizados sobre infraestruturas de computação em nuvem — públicas ou privadas — compatíveis com NFV e SDN. Essa arquitetura permite a instanciação sob demanda, escalabilidade automática e realocação dinâmica das funções de rede conforme a carga de tráfego ou eventos específicos. Além disso, a computação em nuvem facilita a automação da segurança, por meio da aplicação de políticas em tempo real, uso de inteligência artificial para detecção de anomalias e mecanismos como autenticação contínua, microsegmentação e controle adaptativo de acesso (BARBOSA et al., 2021; LIMA, 2024).

Outra inovação central do 5GC é o suporte nativo ao *network slicing*. Cada slice compreende instâncias específicas das funções do núcleo, adaptadas a distintos requisitos de qualidade de serviço, latência, largura de banda e políticas de segurança. Esse recurso permite que setores como saúde, energia e mobilidade compartilhem uma mesma infraestrutura física com total isolamento lógico, garantindo desempenho, segurança e conformidade regulatória (SOBRINHO; SILVA; SANTOS, 2023).

Entretanto, a complexidade do 5GC introduz novos desafios. A multiplicidade de funções desagregadas e instâncias dinâmicas amplia a superfície de ataque, exigindo modelos avançados de segurança e observabilidade. Aspectos como a gestão de identidades, proteção de *APIs* e controle de confiança entre funções tornam-se cruciais para assegurar a integridade e a confiabilidade do sistema (SALAHDINE et al., 2022).

Dessa forma, o 5GC configura-se não apenas como a espinha dorsal da rede 5G, mas como um ambiente inteligente e dinâmico, no qual virtualização, automação e segurança se integram para viabilizar uma nova era de conectividade, moldada às necessidades dos mais diversos setores da sociedade digital.

3.2.3. Virtualização de Funções de Rede

A NFV constitui um dos pilares estruturantes da arquitetura 5G. Sua premissa fundamental é dissociar as funções de rede da infraestrutura física tradicional, permitindo que elementos como roteadores, *firewalls* e balanceadores de carga sejam executados como instâncias de *software* sobre plataformas de virtualização padronizadas, utilizando servidores genéricos (SALAHDINE et al., 2022).

Essa abordagem transforma profundamente a operação das redes móveis, promovendo maior agilidade na provisão de serviços, redução de custos, escalabilidade dinâmica e melhor utilização dos recursos computacionais. No contexto da 5G, o NFV é indispensável para garantir a elasticidade necessária a aplicações de latência crítica e ambientes com alta variabilidade de carga, como cidades inteligentes, redes veiculares e sistemas industriais autônomos (AHAD et al., 2023).

Arquiteturalmente, as VNFs (*Virtual Network Functions* - Funções de Rede Virtualizadas) operam sobre uma NFVI (*Network Functions Virtualization Infrastructure* - Infraestrutura de Virtualização de Funções de Rede), composta por recursos de computação, armazenamento e rede. A gestão dessas funções é realizada por uma camada de orquestração e gerenciamento conhecida como MANO (*Management and Orchestration* - Gerenciamento e Orquestração). Esse *framework*, padronizado pelo ETSI, é responsável por instanciar, monitorar, escalar e reconfigurar automaticamente as VNFs, conforme políticas e requisitos de desempenho previamente definidos (BARBOSA et al., 2021).

Apesar das inúmeras vantagens, a adoção do NFV também introduz novos vetores de risco e desafios de segurança. Um dos principais reside no compartilhamento de recursos entre VNFs distintas, o que pode comprometer o isolamento lógico e possibilitar *side-channel attacks* (ataques laterais) entre máquinas virtuais, ameaçando a confidencialidade dos dados em trânsito ou em processamento (SOBRINHO; SILVA; SANTOS, 2023).

Outro ponto crítico diz respeito à segurança do *hipervisor* (componente responsável pela mediação entre as VNFs e o hardware físico). Vulnerabilidades nesse nível podem ser exploradas para obtenção de acesso privilegiado, permitindo o comprometimento simultâneo de múltiplas funções de rede. Além disso, o alto dinamismo das instâncias virtuais dificulta a aplicação de controles tradicionais, como

firewalls baseados em perímetro, exigindo mecanismos adaptativos e contextuais, tais como segmentação por identidade, inspeção profunda de tráfego e autenticação contínua (LIMA, 2024).

A gestão segura do ciclo de vida das VNFs representa mais um desafio relevante. Desde o desenvolvimento e validação dos pacotes de *software* até sua implantação e desativação, cada etapa pode representar um ponto de vulnerabilidade. O uso de códigos maliciosos inseridos em VNFs comprometidas ou bibliotecas de terceiros não auditadas constitui uma ameaça concreta à integridade da rede. A isso se soma a necessidade de manter registros de auditoria confiáveis, que documentem alterações, interações e movimentações entre funções virtualizadas, possibilitando a detecção de anomalias e o rastreamento de incidentes (SALAHDINE et al., 2022; BARBOSA et al., 2021).

Além disso, o NFV é frequentemente implementado em conjunto com o *network slicing*, no qual múltiplas redes lógicas independentes compartilham a mesma infraestrutura física. Esse compartilhamento torna a segurança ainda mais sensível, pois falhas no isolamento entre *slices* ou na segmentação das VNFs podem viabilizar ataques transversais entre domínios distintos, afetando serviços críticos em setores estratégicos como saúde, energia e transporte (AHAD et al., 2023).

Portanto, embora a virtualização de funções de rede seja essencial para a eficiência e flexibilidade da 5G, ela impõe novas exigências aos mecanismos de segurança. Esses mecanismos precisam evoluir de modelos reativos e estáticos para abordagens proativas, contextuais e resilientes, capazes de atuar em ambientes altamente distribuídos, heterogêneos e dinâmicos.

3.2.4. *Network Slicing*

O *network slicing*, é uma das funcionalidades mais inovadoras da arquitetura 5G, representando uma ruptura em relação ao modelo monolítico das gerações anteriores. Essa tecnologia permite a criação de múltiplas redes lógicas independentes — chamadas *slices* — sobre uma única infraestrutura física compartilhada. Cada fatia é configurada com parâmetros específicos de desempenho, segurança, QoS (*Quality of Service* – Qualidade do Serviço) e disponibilidade,

podendo ser ajustada dinamicamente conforme as demandas de cada aplicação ou cliente (3GPP, 2020).

Essa flexibilidade torna a 5G altamente adaptável a diversos setores industriais. Por exemplo, uma fatia pode ser otimizada para aplicações de realidade aumentada e *streaming* em 4K, com ênfase em largura de banda e latência ultrabaixa; outra pode atender à telemedicina, com exigência de confiabilidade elevada e criptografia reforçada; enquanto um terceiro *slice* pode operar em ambientes de IoT massiva, tolerando maior latência, mas demandando alta escalabilidade para conectar milhares de dispositivos simultaneamente (AHAD et al., 2023; MICELI et al., 2022).

Do ponto de vista técnico, o fatiamento é implementado tanto no núcleo da rede (5GC) quanto na RAN (*Radio Access Network* - Rede de Acesso por Rádio), viabilizado por tecnologias como NFV, SDN e computação em borda. Cada *slice* é composto por uma combinação específica de VNFs instanciadas de forma independente, e por caminhos logicamente isolados que asseguram a separação entre tráfego e controle (BARBOSA et al., 2021).

Apesar de seus benefícios, o *network slicing* impõe desafios relevantes em termos de segurança, orquestração e interoperabilidade. Um dos principais riscos é a garantia de isolamento entre as fatias. Falhas nesse isolamento podem permitir movimentos laterais (*lateral movement*), nos quais um invasor que compromete uma fatia menos segura tenta acessar ou interferir em outra mais crítica, como aquelas dedicadas a serviços de emergência ou infraestrutura energética (SOBRINHO; SILVA; SANTOS, 2023).

Além disso, a gestão de *slices* em ambientes *multitenant (multilocação), cada um com seus dados e configurações isolados* e com múltiplos fornecedores é altamente complexa. A orquestração dessas redes exige visibilidade de ponta a ponta sobre cada instância, bem como políticas de controle de acesso granulares, autenticação refinada e auditoria em tempo real. Tais exigências tornam indispensável o uso de ferramentas com inteligência artificial para segurança adaptativa e automação da detecção de anomalias, considerando que os *slices* podem ser criados, modificados ou encerrados sob demanda (SALAHDINE et al., 2022).

Outro aspecto crítico refere-se à governança e à padronização dos *slices*, especialmente em contextos de *roaming* ou integração internacional, nos quais diferentes operadoras e jurisdições compartilham a mesma infraestrutura. Nesse

cenário, é essencial o alinhamento com normas e diretrizes estabelecidas por organismos como o 3GPP, ITU, ETSI e agências reguladoras nacionais, como a ANATEL (Agência Nacional de Telecomunicações), a fim de garantir interoperabilidade, conformidade legal e proteção de dados sensíveis (LIMA, 2024; CEBRI, 2020).

Portanto, o *network slicing* configura-se como uma tecnologia estratégica que potencializa a capacidade da 5G de atender, simultaneamente, a múltiplos cenários com requisitos distintos. No entanto, sua eficácia depende diretamente da implementação de mecanismos robustos de segurança, segmentação lógica, monitoramento contínuo e padronização internacional — sem os quais o risco de falhas, vazamentos e ataques transversais pode comprometer a confiabilidade da rede como um todo.

3.2.5. *Edge Computing*

O *Edge Computing* é um componente fundamental da arquitetura da 5G, pois viabiliza o processamento de dados de forma descentralizada, ou seja, mais próximo da origem do tráfego ou do usuário final. Essa abordagem contrasta com o modelo tradicional baseado em *data centers* remotos, sendo projetada para reduzir a latência, o consumo de largura de banda, os congestionamentos no núcleo da rede e o tempo de resposta em aplicações sensíveis ao tempo (AHAD et al., 2023).

Na prática, o *edge computing* transfere o poder de processamento para os nós periféricos da rede, como estações-base, *gateways*, *micro data centers* e dispositivos intermediários, tornando possível a execução local de tarefas como inferência, análise de dados, cache de informações e controle operacional. Tal abordagem mostra-se particularmente eficaz em cenários que exigem alta confiabilidade e baixa latência, como veículos autônomos, sistemas industriais robotizados, cirurgias assistidas remotamente, aplicações de XR (*Extended Reality* – Realidade Estendida) e infraestruturas urbanas críticas (SALAHDINE et al., 2022; BARBOSA et al., 2021).

No ecossistema da 5G, o *edge computing* está intimamente ligado ao conceito de MEC (*Multi-access Edge Computing* - Computação de Borda de Acesso Múltiplo), padronizado pelo ETSI. O MEC possibilita a execução de funções de rede, aplicações e serviços diretamente na borda, com acesso contextual a dados como localização,

utilização do espectro e padrões de tráfego. Isso potencializa o desempenho das aplicações e viabiliza novos modelos de negócios baseados em experiências personalizadas e respostas em tempo real (ETSI, 2019).

Apesar de suas inúmeras vantagens, a adoção da computação em borda impõe desafios relevantes em termos de segurança, gerenciamento e interoperabilidade. Em primeiro lugar, a superfície de ataque torna-se consideravelmente maior, já que os dados passam a ser processados e armazenados em diversos pontos físicos e lógicos, muitos dos quais fora dos limites tradicionais de proteção (SOBRINHO; SILVA; SANTOS, 2023). Soma-se a isso o fato de que o ambiente *edge* é geralmente caracterizado por uma grande heterogeneidade e fragmentação, sendo composto por dispositivos com arquiteturas distintas, diferentes sistemas operacionais, padrões de segurança variados e capacidades computacionais desiguais. Essa diversidade dificulta a aplicação uniforme de políticas de proteção, favorecendo a ocorrência de brechas, especialmente em contextos onde há integração com dispositivos IoT de baixo custo e limitada capacidade de atualização (BARBOSA et al., 2021).

Dentre as ameaças mais recorrentes nesse cenário, destacam-se os ataques físicos a dispositivos de borda mal protegidos, frequentemente instalados em locais públicos; a interceptação de dados em trânsito, notadamente quando não há criptografia de ponta a ponta nos segmentos locais; o comprometimento de aplicações executadas na borda, que podem ser alvos de *malwares* (softwares maliciosos) ou atualizações comprometidas; e as vulnerabilidades nos mecanismos de autenticação e controle de acesso, agravadas pela mobilidade dos usuários e pela multiplicidade de domínios administrativos.

Para mitigar esses riscos, tornam-se necessárias estratégias de defesa distribuídas, tais como a microsegmentação da rede com controles granulares por aplicação, a adoção de modelos de segurança do tipo *zero trust* (confiaça zero) — nos quais identidades e comportamentos são constantemente verificados, mesmo em ambientes internos —, o uso de técnicas de inteligência artificial e aprendizado de máquina para detecção de anomalias em tempo real, bem como a aplicação de criptografia adaptativa e mecanismos robustos de gerenciamento de chaves, especialmente adaptados a dispositivos com recursos computacionais limitados (AHAD et al., 2023; SALAHDINE et al., 2022).

Além dessas estratégias, é fundamental o uso de infraestruturas confiáveis e auditáveis, que suportem atualizações remotas seguras de *firmware*, certificação adequada de dispositivos e coleta contínua de telemetria. A resiliência operacional na borda deve considerar, ainda, mecanismos de redundância local, isolamento de falhas e comunicação tolerante a atrasos, características particularmente críticas para aplicações em setores como redes elétricas inteligentes e transporte autônomo.

Dessa forma, embora o *edge computing* represente um pilar estratégico para garantir a eficiência, escalabilidade e inovação nas redes 5G, seu sucesso está intrinsecamente ligado à implementação de soluções robustas e integradas de segurança, orquestração e governança, em consonância com a natureza distribuída e dinâmica das redes contemporâneas.

3.3. AMEAÇAS E VULNERABILIDADES EM REDES 5G

A transição para a quinta geração de redes móveis representa um salto tecnológico significativo, mas também inaugura uma nova era de complexidade e exposição a riscos de segurança.

A adoção de paradigmas como virtualização, *network slicing*, *edge computing* e integração com bilhões de dispositivos IoT amplia de forma considerável a superfície de ataque, além de introduzir novos vetores de exploração não existentes ou não relevantes nas gerações anteriores.

Nesse cenário, as redes 5G não apenas herdaram vulnerabilidades conhecidas, mas também introduziram desafios inéditos, exigindo uma revisão crítica das estratégias de defesa tradicionais (SALAHDINE et al., 2022; LIMA, 2024).

3.3.1. Ampliação da Superfície de Ataque

A arquitetura distribuída e orientada a serviços das redes 5G torna o ecossistema altamente expansível, mas também mais vulnerável a múltiplos pontos de falha. Um dos principais fatores que contribuem para essa vulnerabilidade é a integração massiva de dispositivos IoT.

A previsão é que, até 2025, mais de 75 bilhões de dispositivos estejam conectados globalmente, muitos dos quais com capacidade computacional limitada,

firmware desatualizado ou inexistência de protocolos de segurança robustos (BARBOSA et al., 2021).

Dispositivos IoT, especialmente os de uso doméstico e industrial, são frequentemente projetados com foco na funcionalidade e baixo custo, negligenciando aspectos essenciais de segurança.

Uma vez comprometidos, esses dispositivos podem ser explorados como pontos de entrada para ataques de *botnet* (rede de dispositivos, computadores, smartphones, dispositivos IoT, infectados com malware e controlados remotamente por um atacante), espionagem de tráfego, ou movimentações laterais em ambientes corporativos e industriais. Além disso, sua diversidade tecnológica — diferentes sistemas operacionais, padrões de comunicação e níveis de proteção — dificulta a aplicação de políticas de segurança padronizadas (AHAD et al., 2023).

Outro vetor importante está nos ambientes heterogêneos e altamente dinâmicos que caracterizam a 5G. A capacidade de suportar múltiplos tipos de acesso (NR, LTE, Wi-Fi, redes privativas) e a mobilidade constante dos usuários em contextos de *roaming*, *slicing* e *edge computing* criam cenários onde as fronteiras de segurança são difusas.

A interoperabilidade entre domínios administrativos distintos — como operadoras, fornecedores de nuvem e clientes empresariais — impõe desafios adicionais à coordenação de políticas, autenticação federada e rastreamento de eventos de segurança (SOBRINHO; SILVA; SANTOS, 2023).

3.3.2. Tipos de Ameaças Mais Comuns

As redes 5G estão expostas a uma ampla gama de ameaças que comprometem não apenas a integridade da comunicação, mas também a privacidade dos usuários, a disponibilidade dos serviços e a confiabilidade dos dados processados.

No que diz respeito à privacidade, a ampliação de mecanismos de geolocalização, autenticação contínua e identificação de dispositivos introduz novas formas de rastreamento e criação de perfis comportamentais. Ainda que o identificador temporário criptografado SUCI (*Subscription Concealed Identifier* - Identificador de Assinante Oculto) tenha substituído o IMSI *(International Mobile Subscriber Identity* -

Identidade Internacional de Assinante Móvel) como medida de proteção, pesquisas demonstram que padrões de tráfego ainda podem ser correlacionados para inferir informações sensíveis, como localização e atividades dos usuários (SALAHDINE et al., 2022). Essa vulnerabilidade se agrava quando dados pessoais trafegam por redes de borda, onde podem ser capturados por aplicações maliciosas ou comprometidos em casos de violação de fatias específicas da rede.

Quanto à interceptação de comunicações, embora a 5G tenha introduzido melhorias significativas na criptografia dos planos de controle e de usuário, persistem brechas relevantes, sobretudo em interfaces abertas ou mal configuradas. APIs de orquestração, funções de computação em borda e canais entre elementos do núcleo virtualizado representam pontos críticos. Ataques MitM (*Man-in-the-Middle* - Homem no Meio), exploração de certificados digitais inválidos ou *downgrade attacks* — em que o atacante força a conexão a utilizar protocolos menos seguros — continuam viáveis e representam riscos concretos (BARBOSA et al., 2021).

Os ataques DoS (*Denial of Service* - Negação de Serviço) e DDoS (*Distributed Denial of Service* - Negação de Serviço Distribuído) permanecem entre as ameaças mais perigosas, agravadas no contexto da 5G devido à densidade de conexões e à criticidade de algumas aplicações. Um ataque direcionado, por exemplo, a uma fatia de rede utilizada por serviços de emergência pode gerar uma indisponibilidade generalizada. A virtualização de funções de rede e a centralização promovida por arquiteturas baseadas em SDN aumentam a vulnerabilidade a ataques que visam exaurir recursos computacionais, especialmente em ambientes de borda (AHAD et al., 2023).

A virtualização intensiva, por meio de NFV e SDN, introduz ainda vulnerabilidades específicas associadas à orquestração de serviços e à segurança de instâncias virtualizadas. A exposição de *APIs* de gerenciamento, falhas de isolamento entre funções virtuais e a dependência de hipervisores criam um cenário propício para ataques de escalonamento de privilégios. Um invasor que comprometa uma VNF pode realizar movimentos laterais (*pivoting*), atingindo funções críticas do core e violando a segmentação entre *slices* (SOBRINHO; SILVA; SANTOS, 2023).

Outro vetor de ameaça relevante diz respeito à integridade dos dados, tanto durante a transmissão quanto no armazenamento, sobretudo em aplicações sensíveis como saúde, transporte autônomo e sistemas industriais. A manipulação maliciosa

pode ocorrer por meio de ataques como injeção de dados, *spoofing* e *replay*, especialmente na ausência de mecanismos robustos de verificação de integridade. A natureza distribuída do armazenamento na borda e a dificuldade de monitoramento contínuo dificultam a detecção precoce dessas violações (LIMA, 2024).

Desse modo, embora a 5G represente um avanço significativo em termos de desempenho e flexibilidade, sua arquitetura inovadora introduz novas superfícies de ataque que exigem abordagens igualmente inovadoras de proteção, com ênfase em segurança distribuída, validação contínua e governança adaptativa.

3.4. TECNOLOGIAS DE SEGURANÇA APLICADAS A REDES 5G

A segurança nas redes 5G representa um dos pilares críticos para a viabilidade de sua adoção em larga escala, especialmente diante da crescente sofisticação das ameaças cibernéticas e da complexidade da infraestrutura de telecomunicações. Diferentes tecnologias emergentes vêm sendo aplicadas com o objetivo de proteger a confidencialidade, integridade e disponibilidade dos dados em trânsito e em repouso. Dentre as principais soluções, destacam-se mecanismos avançados de autenticação e criptografia, o uso de inteligência artificial e aprendizado de máquina para detecção de ameaças, e o emprego de tecnologias descentralizadas como o *blockchain*.

3.4.1. Autenticação e Criptografia Avançadas

A segurança das redes 5G está fortemente ancorada em mecanismos robustos de autenticação e criptografia, essenciais para assegurar a confidencialidade, integridade e autenticidade das comunicações. Dada a complexidade e a diversidade dos serviços viabilizados por essa tecnologia — como IoT, veículos autônomos, cirurgias remotas e redes industriais inteligentes — o desenvolvimento de soluções criptográficas avançadas e protocolos de autenticação tornou-se imprescindível para a proteção da informação nesse novo paradigma digital.

A criptografia simétrica e a criptografia assimétrica constituem os pilares centrais da segurança em redes 5G. A primeira, exemplificada pelo algoritmo AES (*Advanced Encryption Standard* - Padrão Avançado de Criptografia), é amplamente empregada em transmissões de alta velocidade devido à sua eficiência

computacional. Já a criptografia assimétrica, por meio de algoritmos como RSA (*Rivest–Shamir–Adleman* - Rivest–Shamir–Adleman – algoritmo de criptografia) e ECC (*Elliptic Curve Cryptography* - Criptografia de Curvas Elípticas), é mais apropriada para ambientes que demandam segurança na troca de chaves e na verificação de identidade, embora tenha maior custo computacional (LIMA, 2024).

No escopo da 5G, o 3GPP definiu, na especificação técnica TS 33.501, um conjunto de mecanismos que representa um avanço em relação às gerações anteriores. Um dos mais relevantes é o protocolo 5G-AKA (5G *Authentication and Key Agreement* - Autenticação de Acesso para Redes Móveis 5G), que viabiliza autenticação mútua entre o dispositivo do usuário e a rede, fortalecendo a proteção contra ataques de interceptação e falsificação de identidade. A identidade permanente do usuário, representada pelo SUPI (*Subscription Permanent Identifier* - Identificador Permanente de Assinante), é ocultada durante a comunicação por meio do SUCI, o qual utiliza criptografia assimétrica para proteger os dados mesmo diante de atacantes passivos ou ativos (SOBRINHO et al., 2023).

Outro componente essencial da arquitetura 5G é o SEPP (*Security Edge Protection Proxy* - Proxy de Proteção de Borda de Segurança), responsável por proteger as comunicações entre redes públicas e privadas em situações de roaming. O SEPP utiliza túneis criptografados e políticas rígidas de controle de acesso e auditoria para garantir a segurança dessas interações (LIMA, 2024).

Com o avanço iminente da computação quântica, surgem preocupações quanto à segurança dos algoritmos criptográficos clássicos. Computadores quânticos terão potencial para resolver problemas matemáticos complexos que hoje sustentam a segurança de sistemas como RSA e ECC — como a fatoração de grandes números primos e o cálculo de logaritmos discretos. Nesse contexto, ganha destaque a PQC (*Post-Quantum Cryptography* – Criptografia Pós-Quântica), desenvolvida para resistir a esse novo tipo de ameaça.

O NIST (*National Institute of Standards and Technology* - Instituto Nacional de Padrões e Tecnologia) lidera os esforços de padronização de algoritmos pós-quânticos, destacando-se o *CRYSTALS-Kyber* (para criptografia de chave pública) e o *CRYSTALS-Dilithium* (para assinatura digital). Ambos se baseiam em problemas matemáticos que, até o momento, não são solucionáveis de forma eficiente por algoritmos quânticos, apresentando desempenho compatível com aplicações de larga

escala, como as exigidas por redes 5G e as futuras redes 6G (SALAHDINE et al., 2022; BARBOSA et al., 2021).

Adicionalmente, a adoção de criptografia avançada e autenticação reforçada atende não apenas a demandas técnicas, mas também a exigências legais e regulatórias. Leis como a LGPD, no Brasil, e o GDPR (*General Data Protection Regulation* - Regulamento Geral de Proteção de Dados), na União Europeia, impõem padrões rigorosos de privacidade e segurança da informação, pressionando operadores e fabricantes a investirem em soluções tecnológicas robustas e atualizadas.

Dessa forma, os mecanismos de autenticação e criptografia incorporados às redes 5G constituem uma resposta à crescente complexidade das ameaças digitais, além de prepararem o caminho para infraestruturas mais seguras, resilientes e confiáveis.

3.4.2. Inteligência Artificial e Aprendizado de Máquina

Com o avanço da digitalização e a crescente complexidade das redes móveis de quinta geração, a segurança passou a ser uma das principais preocupações de operadores e desenvolvedores de soluções em telecomunicações. Nesse contexto, a IA (Inteligência Artificial) e o AM (Aprendizado de Máquina) têm se consolidado como ferramentas fundamentais na construção de mecanismos de defesa proativos, capazes de identificar e mitigar ameaças cibernéticas em tempo real, com alta capacidade de adaptação contínua.

As redes 5G, ao interconectarem bilhões de dispositivos, ampliam consideravelmente a superfície de ataque, tornando os métodos tradicionais de segurança — baseados em assinaturas e regras fixas — insuficientes diante da velocidade e volume de dados trafegados. Para suprir essas lacunas, técnicas de IA, como RNN (*Recurrent Neural Networks* - Redes Neurais Recorrentes), LSTM (*Long Short-Term Memory* - Memória de Longo e Curto Prazo) e CNN (*Convolutional Neural Networks* - Redes Neurais Convolucionais), têm sido aplicadas com sucesso na detecção de anomalias e na predição de tráfego malicioso, permitindo a identificação precoce de ataques como DDoS, varreduras de rede e exploração de vulnerabilidades do tipo *zero-day* (dia zero) (BARBOSA et al., 2021).

Esses modelos são treinados com grandes volumes de dados e se ajustam de forma dinâmica a novos padrões de tráfego. A LSTM, por sua capacidade de analisar sequências temporais e dependências de longo prazo, destaca-se na antecipação de comportamentos anômalos. Por sua vez, as CNNs são eficazes na extração de características espaciais complexas, o que contribui significativamente para a classificação precisa de tráfego com base em pacotes e fluxos (AHAD et al., 2023).

Paralelamente ao desempenho técnico, cresce a exigência por soluções de IA que sejam explicáveis e auditáveis. O conceito de XAI (*Explainable Artificial Inteligence* - Inteligência Artificial Explicável) visa tornar os modelos de aprendizado de máquina mais compreensíveis para especialistas e operadores, permitindo não apenas detectar ameaças, mas também entender as razões que levaram à sua classificação como tal. Isso é particularmente importante em ambientes regulados, nos quais decisões automatizadas devem ser justificáveis (Salahdine et al., 2022).

A privacidade dos dados utilizados no treinamento dos modelos é outro desafio relevante. O uso inadequado de informações sensíveis, sobretudo em aplicações envolvendo dados pessoais, pode violar legislações como a LGPD, no Brasil, e o GDPR, na União Europeia. Para enfrentar essa questão, o *Federated Learning* (Aprendizado Federado) tem sido adotado como alternativa. Essa abordagem permite treinar modelos diretamente nos dispositivos dos usuários, eliminando a necessidade de centralizar os dados e, consequentemente, preservando a privacidade (Lima, 2024).

Apesar do seu potencial, essas tecnologias ainda enfrentam limitações. Entre os principais obstáculos estão a ocorrência de falsos positivos — quando tráfego legítimo é classificado como malicioso — e de falsos negativos — que permitem a passagem de ameaças despercebidas. Além disso, a escalabilidade dos algoritmos e o consumo elevado de recursos computacionais representam desafios adicionais, especialmente em ambientes com restrições de *hardware*, como nos dispositivos de IoT.

Em síntese, o uso de IA e AM nas redes 5G representa um avanço significativo na segurança cibernética, proporcionando mecanismos mais ágeis, inteligentes e adaptativos. No entanto, a eficácia dessas soluções está condicionada à sua implementação ética, transparente e alinhada com os princípios de proteção de dados e governança digital responsável.

3.4.3. *Blockchain* e Descentralização

A crescente demanda por redes móveis seguras, escaláveis e resilientes, impulsionada pela chegada da 5G, tem favorecido a aplicação da tecnologia *blockchain* como recurso estratégico no fortalecimento da cibersegurança. Originalmente desenvolvida para suportar criptomoedas, a *blockchain* passou a ser reinterpretada no contexto das telecomunicações, configurando-se como uma solução promissora para desafios relacionados à segurança, privacidade e confiança em ambientes distribuídos, como a IoT e o *edge computing*.

Nas redes 5G, a *blockchain* é empregada em diversas frentes, incluindo gestão de identidade digital, autenticação descentralizada, integridade de dados e registro imutável de eventos. Sua arquitetura distribuída e resistente a alterações possibilita que dispositivos e nós validem transações e comunicações autonomamente, eliminando a necessidade de uma autoridade central e promovendo um modelo de confiança horizontal (LIMA, 2024).

Implementações práticas demonstram a viabilidade da *blockchain* em autenticação multifator baseada em contratos inteligentes, eliminando intermediários e reduzindo pontos únicos de falha. Em VANETs (*Vehicular Ad Hoc Networks* - Redes Veiculares Ad Hoc) e sistemas baseados em UAVs (*Unmanned Aerial Vehicles* - Veículos Aéreos Não Tripulados), a tecnologia garante trilhas de comunicação seguras, proteção de rotas e integridade dos comandos. Além disso, viabiliza controle de acesso baseado em reputação e rastreamento confiável de transações em tempo real (AHAD et al., 2023; SALAHDINE et al., 2022).

Outro destaque é a transparência operacional proporcionada pelo registro em *ledger (*registro compartilhado de informações*)* público ou privado, permitindo auditoria completa e fortalecendo a responsabilização diante de incidentes. Esse recurso é especialmente relevante em ambientes críticos, como redes hospitalares, cadeias de suprimentos automatizadas e infraestruturas urbanas inteligentes.

Apesar dos avanços, a adoção da *blockchain* em tempo real nas redes 5G enfrenta desafios técnicos, como latência elevada, alto consumo energético e limitações de escalabilidade das *blockchains* públicas tradicionais, como Bitcoin e Ethereum. Tais restrições dificultam a integração com aplicações que demandam

respostas em milissegundos, como veículos autônomos e sistemas industriais (BARBOSA et al., 2021).

Para contornar essas barreiras, têm sido propostas soluções híbridas, como *blockchains* privadas e permissionadas, que oferecem maior controle e melhor desempenho. Outras estratégias incluem uso de *sidechains* (canais paralelos), *ledgers* leves (*lightweight*) e integração com inteligência artificial e aprendizado de máquina, visando ampliar a segurança preditiva por meio de validação distribuída (SOBRINHO et al., 2023).

Em síntese, a *blockchain* consolida-se como pilar complementar na arquitetura de segurança das redes 5G, especialmente em cenários que exigem descentralização, transparência e resiliência. Embora persistam desafios técnicos e de padronização, a tendência é sua integração crescente com mecanismos de proteção, contribuindo para redes mais confiáveis e autogerenciáveis.

3.5. NORMAS, PADRÕES E REGULAMENTAÇÕES EM SEGURANÇA 5G

A implementação das redes 5G exige não apenas inovação tecnológica, mas também a adesão a um conjunto robusto de normas técnicas, padrões de segurança e diretrizes regulatórias. A conformidade com esses marcos normativos é fundamental para garantir a interoperabilidade entre sistemas, a proteção de dados pessoais e a resiliência cibernética em escala global. Em especial, destaca-se o papel de organismos técnicos internacionais e agências reguladoras nacionais na definição de *frameworks* e requisitos mínimos de segurança para essas redes críticas.

3.5.1. Padrões técnicos internacionais

A arquitetura de segurança das redes 5G baseia-se em um conjunto estruturado de normas e padrões técnicos internacionais, elaborados por entidades especializadas para assegurar interoperabilidade, robustez e resiliência frente a ameaças cibernéticas. Esses padrões são essenciais não apenas para a operação segura das redes, mas também para seu alinhamento com requisitos regulatórios e melhores práticas globais em segurança da informação.

Entre os principais documentos normativos, destaca-se a especificação técnica TS 33.501, desenvolvida pelo 3GPP. Essa especificação define os mecanismos de segurança de ponta a ponta do sistema 5G, abrangendo desde a interface aérea até o núcleo da rede. Suas contribuições incluem autenticação mútua entre o equipamento do usuário e a rede, gerenciamento seguro de chaves criptográficas, proteção da identidade permanente do usuário por meio do SUPI e sua versão ofuscada, o SUCI, além da introdução do SEPP, que atua como elemento protetor nas interfaces de *roaming* e na comunicação entre redes públicas e privadas (SOBRINHO; SILVA; SANTOS, 2023).

Paralelamente ao 3GPP, a ITU, por meio do setor de padronização ITU-T, exerce papel relevante na definição de requisitos técnicos e arquiteturais para redes móveis de nova geração. A recomendação ITU-T Y.3101, por exemplo, descreve os requisitos arquiteturais para redes IMT-2020 (*International Mobile Telecommunications-2020* - Telecomunicações Móveis Internacionais-2020), designação técnica da ITU para a 5G, com foco em segurança, escalabilidade, interoperabilidade e suporte a múltiplos cenários de serviço. O ITU-T também estabelece normas sobre segurança da interface de rádio, *network slicing* e orquestração de serviços, garantindo uma estrutura segura e adaptável para aplicações emergentes (CEBRI, 2020).

Outro ator de destaque no ecossistema de padronização é o ETSI, responsável por contribuições fundamentais em cibersegurança, virtualização e redes definidas por software. Entre suas principais publicações está a ETSI GS NFV-SEC (ETSI *Group Specification; Network Functions Virtualization; Security* – ETSI Especificações de Grupo; Virtualização de Funções de Rede; Segurança), que define diretrizes de segurança para ambientes virtualizados, abordando controle de acesso, segregação de funções, proteção contra ataques internos e gestão de vulnerabilidades em ambientes baseados em nuvem e *edge computing*. Essas normas são especialmente relevantes para a arquitetura 5G, que incorpora amplamente a NFV e ambientes computacionais distribuídos (BARBOSA et al., 2021).

Complementando esse conjunto, o subcomitê ISO/IEC JTC 1/SC 27, formado pela ISO (*International Organization for Standardization* - Organização Internacional de Normalização) e pela IEC (*International Electrotechnical Commission* - Comissão Eletrotécnica Internacional), desenvolve normas internacionais voltadas à segurança

da informação, proteção da privacidade e gestão de riscos. Entre as mais aplicáveis às redes 5G estão a ISO/IEC 27001, referente à gestão de segurança da informação, e a ISO/IEC 27017, direcionada à segurança em computação em nuvem. Essas normas são fundamentais para as camadas de virtualização e orquestração de serviços, que demandam políticas rigorosas de controle, auditoria e conformidade (LIMA, 2024).

Em síntese, a padronização técnica internacional em segurança para redes 5G constitui um campo consolidado, multidisciplinar e em constante evolução. A harmonização entre os padrões do 3GPP, ITU, ETSI e ISO/IEC compõe a espinha dorsal da segurança em uma das tecnologias mais críticas da atualidade, garantindo que a transição para a conectividade massiva ocorra de forma segura, confiável e alinhada aos princípios da engenharia de redes modernas.

3.5.2. Legislação e regulação nacional e internacional

A implantação das redes 5G em escala global não se limita a um desafio tecnológico, envolvendo também um complexo aparato jurídico-regulatório. Normas nacionais e internacionais buscam acompanhar a rápida evolução tecnológica, impondo requisitos relacionados à segurança, proteção de dados e governança digital, com o objetivo de mitigar riscos ligados à exposição de informações sensíveis e ao controle estratégico de infraestruturas críticas.

No Brasil, a ANATEL exerce papel central na regulação do setor e na coordenação da implementação da 5G. O leilão do espectro, realizado em novembro de 2021, constituiu um marco regulatório e estratégico. Além de definir as operadoras autorizadas, o edital incluiu cláusulas sobre segurança das redes, exigência de infraestrutura nacionalizada em determinadas faixas e obrigatoriedade de investimentos para ampliar a conectividade em regiões remotas. Também foram previstas diretrizes sobre resiliência da infraestrutura e proteção contra vulnerabilidades cibernéticas (CEBRI, 2020).

Do ponto de vista jurídico, destaca-se a LGPD – Lei nº 13.709/2018 –, que estabelece princípios e obrigações para o tratamento de dados pessoais, inclusive no meio digital. A LGPD impõe requisitos como finalidade específica, necessidade do dado, transparência no tratamento e adoção de medidas técnicas e administrativas

para proteger informações contra acessos não autorizados ou incidentes de perda e destruição. Em redes 5G, que intensificam a coleta massiva e distribuída de dados por meio da IoT, *edge computing* e sensores inteligentes, a LGPD atua como instrumento essencial de controle (ROCHA, 2022).

No âmbito internacional, destaca-se a GDPR da União Europeia, em vigor desde 2018. Reconhecido por seu caráter abrangente e rigoroso, a GDPR estabelece diretrizes mais exigentes que a LGPD em aspectos como consentimento explícito, direito ao esquecimento, portabilidade de dados e obrigatoriedade de notificação de incidentes. Sua influência ultrapassa as fronteiras europeias, servindo como referência para empresas multinacionais e legisladores em outros países. Para projetos de redes 5G que envolvem intercâmbio transnacional de dados, a conformidade com a GDPR é não apenas uma exigência legal, mas também estratégica, evitando sanções severas e garantindo parcerias internacionais sustentáveis (SALAHIDINE et al., 2022).

Outro ponto relevante é o debate sobre soberania digital e segurança nacional. Considerando a criticidade das infraestruturas 5G – que suportam serviços essenciais como saúde, transporte, energia e segurança pública –, diversos países têm adotado políticas restritivas quanto à origem dos equipamentos, especialmente de fornecedores estrangeiros. Essas medidas visam reduzir riscos de espionagem industrial, acesso indevido a dados estratégicos e implantação de *backdoors*. Como resposta, governos têm exigido auditorias de segurança, certificações independentes e, em alguns casos, a exclusão de determinados fabricantes das redes centrais de comunicação (CEBRI, 2020; LIMA, 2024).

Nesse contexto, a segurança das redes 5G vai além da adoção de ferramentas tecnológicas. Ela exige alinhamento consistente com estruturas jurídicas nacionais e internacionais, além de uma postura proativa de Estados e empresas em relação à governança da informação e à proteção da soberania digital. Assim, a construção de redes seguras depende da interseção entre tecnologia, direito e geopolítica.

4. RESULTADOS

A partir da revisão sistemática conduzida com base em fontes técnico-científicas publicadas entre 2020 e 2024, foi possível identificar um conjunto expressivo de desafios e soluções relacionados à segurança em redes 5G. A análise crítica permitiu agrupar os resultados em três eixos principais: desafios enfrentados, soluções e boas práticas e uma discussão sobre limitações e tendências emergentes.

4.1. PRINCIPAIS DESAFIOS ENCONTRADOS

A consolidação das redes 5G trouxe novos desafios à segurança cibernética, ampliando a superfície de ataque das infraestruturas digitais e elevando a complexidade na proteção de dados. A integração de tecnologias como NFV, SDN e *network slicing*, aliada à expansão da IoT, proporcionou maior dinamismo, mas também aumentou a vulnerabilidade a ataques sofisticados.

Entre as ameaças mais críticas, destaca-se a exposição da interface aérea a ataques de *spoofing* e interceptação, especialmente durante a autenticação inicial. Essas vulnerabilidades comprometem a confidencialidade e a integridade das comunicações, permitindo que agentes maliciosos capturem credenciais e assumam sessões legítimas (SALAHDINE et al., 2022).

Outro ponto sensível é a segmentação virtual da rede por meio do *network slicing*. Quando implementado de forma inadequada, esse recurso pode se tornar porta de entrada para ataques laterais, possibilitando movimentação entre fatias e violação de dados sensíveis (SOBRINHO; DIAS DA SILVA; SANTOS, 2023).

Os ataques DDoS permanecem como ameaça relevante, direcionando-se, sobretudo, às funções virtualizadas do núcleo da rede 5G. Esses ataques visam esgotar os recursos computacionais, comprometendo serviços críticos, como saúde conectada, transporte inteligente e comunicações de emergência (BARBOSA et al., 2021).

A gestão de identidades digitais também se apresenta como um desafio, dado que mecanismos frágeis de autenticação e verificação favorecem rastreamentos não autorizados, clonagem de perfis e exposição de dados pessoais. Tais falhas vão de

encontro às exigências de privacidade definidas por legislações como a LGPD (ROCHA, 2022).

A heterogeneidade dos dispositivos IoT conectados às redes 5G agrava esse cenário, já que muitos não seguem padrões mínimos de segurança. Esses dispositivos tornam-se alvos fáceis para exploração remota, ataques de *botnets* e controle indevido. A ausência de certificações e padronizações obrigatórias intensifica o problema, dificultando ações de mitigação em larga escala (AHAD et al., 2023).

Diante desse panorama, evidencia-se que a segurança nas redes 5G não depende apenas de soluções tecnológicas, mas exige um modelo de governança robusto, com normas claras, integração regulatória e capacitação contínua dos agentes envolvidos.

4.2. SOLUÇÕES E BOAS PRÁTICAS IDENTIFICADAS

Diante das vulnerabilidades identificadas nas redes 5G, diferentes mecanismos foram propostos para reforçar a proteção de dados, preservar a integridade da infraestrutura e garantir conexões confiáveis. As soluções analisadas nesta pesquisa destacam abordagens tecnológicas avançadas, compatíveis com a complexidade da arquitetura 5G.

Entre as medidas de maior relevância está a autenticação avançada por meio do protocolo 5G-AKA, definido na especificação 3GPP TS 33.501, que estabelece verificação robusta entre dispositivo e núcleo da rede antes da troca de dados. Esse mecanismo inclui proteções contra ataques de repetição e interceptação, assegurando a confidencialidade e a integridade das comunicações (3GPP, 2023).

No âmbito da criptografia, as redes 5G empregam algoritmos consagrados, como AES e ECC. Entretanto, com o avanço da computação quântica, estudos apontam para a necessidade da criptografia pós-quântica, projetada para resistir a ataques realizados por computadores quânticos, que podem comprometer os métodos atuais (LIMA, 2024).

A aplicação de IA constitui outra estratégia relevante, especialmente na detecção de ameaças. Modelos baseados em aprendizado profundo, como redes RNN, CNN e LSTM, apresentam eficácia na identificação precoce de anomalias e

comportamentos maliciosos, possibilitando monitoramento contínuo e resposta ágil a novos padrões de ataque (BARBOSA et al., 2021).

A tecnologia *blockchain* surge como solução inovadora para autenticação descentralizada e rastreabilidade de transações digitais. Sua estrutura distribuída e imutável impede alterações não autorizadas, garantindo transparência e confiança, especialmente em setores críticos, como saúde e finanças (AHAD et al., 2023).

Por fim, a ZTA (*Zero Trust Architecture* - Arquitetura de Confiança Zero) destaca-se por romper com o modelo tradicional de confiança implícita. Nessa abordagem, nenhum dispositivo ou usuário é considerado confiável por padrão, o que exige verificações contínuas, segmentação rigorosa e controle de acesso granular, reduzindo o risco de movimentações laterais por invasores (SALAHDINE et al., 2022).

De forma integrada, essas soluções se complementam, criando um ecossistema de rede mais resiliente, alinhado aos objetivos de proteção e preparado para ameaças emergentes.

4.3. CASOS DE SUCESSO

A consolidação das redes 5G tem impulsionado a adoção de soluções avançadas de segurança, com empresas líderes do setor desenvolvendo aplicações práticas que comprovam a viabilidade das tecnologias emergentes. Essas iniciativas demonstram não apenas a capacidade de mitigação de riscos, mas também a contribuição para a resiliência e a confiabilidade da infraestrutura.

A Ericsson destaca a aplicação de inteligência artificial embarcada no núcleo da rede 5G para detecção e mitigação de ataques DDoS em tempo real. Em testes com operadoras europeias, essa solução reduziu em 65% as interrupções inesperadas, garantindo maior disponibilidade e estabilidade dos serviços (ERICSSON, 2023).

A Huawei, por sua vez, apresenta avanços na utilização do *network slicing* com isolamento de tráfego, permitindo que múltiplos serviços operem de forma independente e segura sobre a mesma infraestrutura física. Essa estratégia é especialmente relevante para setores críticos, como saúde, segurança pública e mobilidade urbana, onde latência reduzida e confiabilidade são fundamentais (HUAWEI, 2022).

Já a Nokia foca na orquestração automatizada baseada em inteligência artificial para o gerenciamento dinâmico das NFVs. Essa abordagem possibilita ajustes em tempo real diante de ameaças ou variações operacionais, garantindo flexibilidade e segurança em um cenário marcado por tráfego variável e diversidade de dispositivos conectados (NOKIA, 2022).

No contexto brasileiro, iniciativas relatadas pelo CEBRI (Centro Brasileiro de Relações Internacionais) indicam a aplicação de *big data* e análise comportamental em ambientes industriais e infraestruturas críticas, como logística e defesa cibernética. Essas práticas viabilizam a detecção precoce de anomalias e a resposta rápida a incidentes, aumentando a resiliência das operações (CEBRI, 2020).

De modo geral, as soluções analisadas apresentam características complementares: enquanto a IA aplicada pela Ericsson e Nokia potencializa a detecção adaptativa e a resposta automatizada, o *network slicing* da Huawei fortalece a segmentação lógica e o isolamento de serviços. Já as práticas baseadas em *big data* no Brasil reforçam a análise preditiva e o monitoramento contínuo. Em conjunto, esses mecanismos respondem ao objetivo central de fortalecer a segurança no ecossistema 5G, confirmando que a integração progressiva dessas tecnologias tende a consolidar redes mais robustas e confiáveis.

4.4. DISCUSSÃO

Apesar dos avanços nas soluções de segurança para redes 5G, persistem desafios estruturais que comprometem sua eficácia plena. Um dos principais entraves é a falta de padronização e interoperabilidade entre sistemas, decorrente da diversidade de fabricantes, arquiteturas e protocolos. Essa heterogeneidade dificulta a integração de mecanismos de proteção em ambientes *multivendor*, tornando distante o objetivo de defesas unificadas em escala global (SALAHIDINE et al., 2022).

Outro obstáculo relevante é a escassez de profissionais especializados em cibersegurança voltada a 5G. A alta demanda por especialistas em NFV, SDN, aprendizado de máquina e proteção de dados supera a oferta atual de mão de obra, criando um déficit técnico que impacta diretamente a implementação segura dessas tecnologias (AHAD et al., 2023).

No campo regulatório, a aplicação da LGPD enfrenta limitações práticas diante das características da 5G, como coleta massiva e contínua de dados em tempo real. Essa realidade impõe a necessidade de atualização normativa, considerando a descentralização e automação intrínsecas à nova arquitetura de rede (ROCHA, 2022).

Para superar essas lacunas, surgem tendências tecnológicas que prometem fortalecer a segurança. A criptografia quântica se apresenta como alternativa aos métodos tradicionais, com algoritmos baseados em reticulados e funções *hash* resistentes a ataques por computadores quânticos (LIMA, 2024). A inteligência artificial explicável, por sua vez, visa aumentar a transparência e auditabilidade das decisões automatizadas, reforçando a confiança nos sistemas autônomos de defesa (BARBOSA et al., 2021).

Outra abordagem inovadora envolve os sistemas autoimunes digitais, inspirados na resposta adaptativa biológica, que ajustam reações a novas ameaças em tempo real, dispensando assinaturas prévias (SOBRINHO et al., 2023). Complementarmente, modelos como a arquitetura *Zero Trust* e as identidades digitais autossoberanas, integradas ao *blockchain*, eliminam pontos únicos de falha e fortalecem os mecanismos de autenticação (HUAWEI, 2022).

Essas inovações demonstram a convergência entre tecnologia avançada e governança digital, apontando para um ecossistema 5G mais seguro e resiliente, alinhado às exigências de privacidade e confiabilidade necessárias às próximas gerações de conectividade.

5. CONSIDERAÇÕES FINAIS

As redes 5G representam um marco na evolução das telecomunicações, possibilitando aplicações críticas em áreas como saúde, mobilidade, cidades inteligentes e indústria. Este estudo cumpriu seus objetivos ao identificar vulnerabilidades, analisar soluções tecnológicas, avaliar abordagens regulatórias e comparar estratégias de mitigação para os riscos associados à arquitetura 5G.

A pesquisa demonstrou que a integração de tecnologias como SDN, NFV, *network slicing* e *edge computing* amplia significativamente as possibilidades de conectividade, mas também aumenta a superfície de ataque, elevando os riscos de segurança (BARBOSA et al., 2021; AHAD et al., 2023; LIMA, 2024). Essa complexidade torna insuficientes os modelos tradicionais de defesa, exigindo a adoção de novas estratégias, como criptografia avançada, autenticação robusta, *blockchain* para autenticação descentralizada, criptografia pós-quântica e arquiteturas de confiança zero, associadas ao uso de inteligência artificial para detecção adaptativa de ameaças (SALAHIDINE et al., 2022; SOBRINHO et al., 2023; AHAD et al., 2023).

Apesar dos avanços, os resultados indicam desafios persistentes, entre eles a falta de padronização global, a interoperabilidade limitada, a escassez de profissionais especializados e lacunas regulatórias, como a adaptação da LGPD às especificidades da 5G no Brasil e a harmonização com normas internacionais, como o GDPR (ROCHA, 2022; MICELI et al., 2022). Esses fatores revelam que a segurança nas redes 5G vai além da aplicação de soluções técnicas, demandando governança sólida, regulamentação eficaz e colaboração constante entre governos, empresas e instituições de pesquisa (LIMA, 2024; CEBRI, 2020).

Conclui-se que a construção de um ecossistema digital seguro para a 5G exige uma abordagem proativa, adaptativa e multidisciplinar, capaz de integrar rapidamente novas tecnologias e responder a ameaças emergentes. A segurança deve ser compreendida como um elemento estratégico para a confiabilidade das redes e para a sustentabilidade da transformação digital, e não apenas como uma exigência técnica (BARBOSA et al., 2021; 3GPP, 2020).

Este estudo apresenta algumas limitações, como a ênfase em literatura acadêmica e técnica, o que pode ter restringido a análise de práticas mais recentes

aplicadas por empresas e órgãos reguladores. Além disso, a diversidade de legislações nacionais impõe obstáculos à criação de um marco regulatório global, reforçando a necessidade de estudos comparativos sobre regulamentações regionais e suas aplicações. Recomenda-se, portanto, que pesquisas futuras investiguem a aplicação prática de criptografia pós-quântica e inteligência artificial explicável em redes 5G, a viabilidade de modelos descentralizados de autenticação, como identidades digitais autossoberanas associadas ao *blockchain*, e estratégias para a convergência regulatória que promovam interoperabilidade e segurança em escala global. Esses caminhos são fundamentais para consolidar uma infraestrutura 5G resiliente, confiável e preparada para enfrentar os desafios da próxima geração de conectividade.

REFERÊNCIAS

3GPP – 3rd Generation Partnership Project. System Architecture for the 5G System (Release 16). 3GPP TS 23.501 V16.9.0, 2020. Disponível em: https://portal.3gpp.org. Acesso em 01 de abr de 2025.

AHAD, Md. A. et al. 5G security: A review of standardization and research trends. **Computer Science Review**, [S. l.], v. 47, 2023. Disponível em: https://doi.org/10.1016/j.cosrev.2022.100540. Acesso em: 23 abr. 2025.

BARBOSA, G. N. N. et al. **Segurança em Redes 5G: Oportunidades e Desafios em Detecção de Anomalias e Predição de Tráfego baseadas em Aprendizado de Máquina.** In: XXI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg), 2021. p. 145–159.

CEBRI – CENTRO BRASILEIRO DE RELAÇÕES INTERNACIONAIS. A segurança cibernética e a tecnologia 5G no cenário brasileiro. Rio de Janeiro: CEBRI, 2020. Disponível em: https://www.cebri.org. Acesso em 02 de abr de 2025.

CHAVES, R. et al. Tecnologias emergentes para segurança em redes 5G. **Revista Brasileira de Cibersegurança**, v. 6, n. 2, p. 54-65, 2021.

ERICSSON. 5G **Security: Securing the Future of Communications.** White Paper, 2023. Disponível em: https://www.ericsson.com. Acesso em: 10 abr. 2025.

ETSI – European Telecommunications Standards Institute. Multi-access Edge Computing (MEC); Framework and Reference Architecture. ETSI GS MEC 003 V2.1.1, 2019. Disponível em: https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/02.01.01_60/gs_mec003v020101p.pdf. Acesso em 18 de abr de 2025.

HUAWEI, ERICSSON, NOKIA. **White Papers sobre segurança e redes 5G**, 2020–2023.

HUAWEI. **5G Security in Practice: Building Trust in a Connected World.** White Paper, 2022. Disponível em: https://www.huawei.com. Acesso em 18 de abr de 2025.

ITU – International Telecommunication Union. Minimum Requirements Related to Technical Performance for IMT-2020 Radio Interface(s). Report ITU-R M.2410-0, Genebra, 2020.

LIMA, L. C. **5G e segurança cibernética: uma análise dos desafios e perspectivas no cenário brasileiro.** 2024. Trabalho de Conclusão de Curso (Bacharelado em Engenharia de Computação) – Centro Universitário Unifacisa, Campina Grande, 2024.

MICELI, E. et al. Tecnologia 5G: fundamentos, aplicações e desafios. **Revista de Tecnologia da Informação e Comunicação**, São Paulo, v. 14, n. 2, p. 45-67, 2022.

MOHER D. et al. **Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement**. PLoS Med. 2009;6:e1000097. doi: 10.1371/journal.pmed.1000097.

NOKIA. **5G Security and Trust: A Holistic Approach.** White Paper, 2022. Disponível em: https://www.nokia.com. Acesso em: 10 abr. 2025.

ROCHA, L. E. Os impactos da tecnologia 5G ao direito à privacidade no Brasil. **Rev. FDUSP**, v.117, p.801–830, 2022.

SALAHDINE, F. et al. Security in 5G and beyond: Recent advances and future challenges. **Security and Privacy**, v. 6, e271, 2022. DOI: 10.1002/spy2.271.

SOBRINHO, R.; SILVA, T.; SANTOS, D. **Cibersegurança e redes 5G: riscos, vulnerabilidades e soluções emergentes.** Policy Paper – CEBRI, Rio de Janeiro, Grupo Cyber, 2023.

UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES. **Recommendation ITU-T Y.3101 – Requirements of the IMT-2020 network.** Geneva: ITU, 2018.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA
Campus Campina Grande - Código INEP: 25137409
R. Tranqüilino Coelho Lemos, 671, Dinamérica, CEP 58432-300, Campina Grande (PB)
CNPJ: 10.783.898/0003-37 - Telefone: (83) 2102.6200

Documento Digitalizado Restrito

Trabalho de Conclusão de Curso

Assunto:	Trabalho de Conclusão de Curso
Assinado por:	Kilary Bayma
Tipo do Documento:	Anexo
Situação:	Finalizado
Nível de Acesso:	Restrito
Hipótese Legal:	Informação Pessoal (Art. 31 da Lei no 12.527/2011)
Tipo do Conferência:	Cópia Simples

Documento assinado eletronicamente por:

- **Kilary Bayma Ximenes Vasconcelos**, **DISCENTE (202511210026) DE TECNOLOGIA EM TELEMÁTICA - CAMPINA GRANDE**, em 22/08/2025 21:14:18.

Este documento foi armazenado no SUAP em 22/08/2025. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifpb.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1583675
Código de Autenticação: dff8d7b273