UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS DE QUIXADÁ

CURSO DE GRADUAÇÃO EM REDES DE COMPUTADORES

JHONATAN DA SILVA CACIANO

SEGURANÇA EM REDES 5G COM IPV6: UMA REVISÃO SISTEMÁTICA DA LITERATURA

QUIXADÁ

2025

JHONATAN DA SILVA CACIANO

SEGURANÇA EM REDES 5G COM IPV6: UMA REVISÃO SISTEMÁTICA DA LITERATURA

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Redes de Computadores da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de Tecnólogo em Redes de Computadores.

Orientador: Prof. Dr. Alisson Barbosa de Souza.

QUIXADÁ

2025

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

C127s Caciano, Jhonatan da Silva.
Segurança Em Redes 5G Com IPV6: Uma Revisão Sistemática Da Literatura / Jhonatan da Silva Caciano. – 2025.
118 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Quixadá, Curso de Redes de Computadores, Quixadá, 2025.
Orientação: Prof. Dr. Alisson Barbosa de Souza.

1. 5G. 2. IPv6. 3. Segurança. 4. Cibersegurança. I. Título.

CDD 004.6

JHONATAN DA SILVA CACIANO

SEGURANÇA EM REDES 5G COM IPV6: UMA REVISÃO SISTEMÁTICA DA LITERATURA

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Redes de Computadores da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de Tecnólogo em Redes de Computadores.

Aprovada em: 14/07/2025.

BANCA EXAMINADORA

Prof. Dr. Alisson Barbosa de Souza (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Michel Sales Bonfim
Universidade Federal do Ceará (UFC)

Prof. Dr. Antonio Rafael Braga
Universidade Federal do Ceará (UFC)

RESUMO

A integração das tecnologias 5G e IPv6 representa um avanço significativo para a evolução das redes de comunicação, oferecendo maior capacidade de conectividade, redução de latência e ampliação do espaço de endereçamento. Contudo, essa convergência também introduz novos desafios no campo da segurança, especialmente em ambientes virtualizados, *multitenant* e altamente dinâmicos. Este trabalho apresenta uma revisão sistemática da literatura com foco nas vulnerabilidades, soluções e desafios relacionados à segurança em redes 5G/IPv6. Os estudos analisados foram classificados por meio da elaboração de uma taxonomia estruturada em três eixos: Tecnologias, Problemas de Segurança e Soluções. A metodologia adotada seguiu diretrizes reconhecidas, assegurando rigor e reprodutibilidade. Como resultado, foram identificadas falhas persistentes, soluções recorrentes e lacunas críticas, além de direções futuras para pesquisas na área. O estudo contribui para a consolidação do conhecimento sobre segurança em redes 5G com IPv6, oferecendo uma base técnica para pesquisadores e profissionais da área.

Palavras-chave: 5g; ipv6; segurança; cibersegurança; virtualização de funções de rede.

ABSTRACT

The integration of 5G and IPv6 technologies represents a significant advancement in the evolution of communication networks, providing greater connectivity capacity, reduced latency, and an expanded addressing space. However, this convergence also introduces new challenges in the field of security, especially in virtualized, multitenant, and highly dynamic environments. This study presents a systematic literature review focused on vulnerabilities, solutions, and challenges related to security in 5G/IPv6 networks. The analyzed studies were classified through the development of a taxonomy structured into three main axes: Technologies, Security Issues, and Solutions. The adopted methodology followed established guidelines, ensuring academic rigor and reproducibility. As a result, persistent flaws, recurring mitigation strategies, and critical gaps were identified, along with future research directions. This work contributes to the consolidation of knowledge on security in 5G networks with IPv6, offering a technical foundation for researchers and professionals in the field.

Keywords: 5g; ipv6; network; cybersecurity; network function virtualization.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

O avanço contínuo da tecnologia da informação tem impulsionado transformações significativas na forma como os dados são transmitidos, processados e protegidos. Nesse cenário, duas tecnologias emergentes se destacam por seu impacto potencial: o *Internet Protocol version 6* (IPv6) e a quinta geração de redes móveis (5G). O IPv6 surge como resposta à limitação de endereçamento do *Internet Protocol version 4* (IPv4), oferecendo uma capacidade virtualmente ilimitada de endereços IP, além de melhorias em eficiência de roteamento, suporte à mobilidade e segurança nativa com o uso obrigatório do *Internet Protocol Security* (IPsec) (Tanenbaum; Wetherall, 2011). Por sua vez, o 5G representa uma revolução nas comunicações móveis ao proporcionar maior largura de banda, latência ultrabaixa e suporte massivo a dispositivos conectados, habilitando aplicações críticas como veículos autônomos, cidades inteligentes e Internet das Coisas (IoT) (Ahmad *et al.*, 2018).

A integração entre 5G e IPv6, embora essencial para suportar a demanda crescente por conectividade, também introduz uma nova gama de vulnerabilidades e desafios de segurança. A eliminação do uso de *Network Address Translation* (NAT), característica marcante do IPv6, amplia a exposição direta de dispositivos à internet pública, dificultando o uso de mecanismos tradicionais de isolamento de rede. Além disso, o 5G adota arquiteturas baseadas em *network slicing*, funções virtualizadas e interfaces abertas, ampliando a superfície de ataque e exigindo mecanismos robustos de autenticação, criptografia, controle de acesso e orquestração segura (Khan *et al.*, 2019a). Apesar do suporte nativo ao IPsec no IPv6, incidentes relacionados a autenticação insegura, vazamento de dados e ataques de orquestração ainda são recorrentes, levantando dúvidas sobre a efetividade prática dos mecanismos de segurança atualmente empregados.

A escolha deste tema é motivada pela crescente dependência de redes 5G com IPv6 em aplicações críticas, como infraestrutura urbana inteligente, monitoramento médico remoto e sistemas industriais automatizados. A segurança dessas redes tornou-se fator essencial para a continuidade de serviços sensíveis e, ao mesmo tempo, um alvo recorrente de estudos, devido à complexidade de sua arquitetura e à necessidade de padronizações mais eficazes. Essa relevância prática, aliada ao dinamismo do campo, reforça a importância de organizar o conhecimento científico acumulado sobre o tema, especialmente diante de sua aplicação em cenários críticos e potencialmente vulneráveis.

Dessa forma, este trabalho tem como objetivo realizar uma revisão sistemática da literatura científica, seguindo as diretrizes estabelecidas por Kitchenham (2004) e Kitchenham *et*

al. (2009), com foco na segurança em redes que integram 5G e IPv6. Foram selecionados estudos publicados entre 2018 e 2025, período que coincide com a expansão global da implantação do 5G e o avanço da adoção do IPv6. As buscas foram conduzidas nas bases *IEEE Xplore* e *Google Scholar*, utilizando critérios rigorosos de inclusão, exclusão e avaliação da qualidade metodológica.

A partir dos estudos selecionados, propõe-se inicialmente uma taxonomia descritiva que organiza os achados da literatura em três eixos analíticos: Tecnologias, Problemas de Segurança e Soluções. Em seguida, uma análise crítica subsidiará a construção de uma taxonomia analítica, com o intuito de identificar padrões, lacunas de pesquisa e relações entre os elementos analisados. Essa abordagem dupla visa proporcionar uma visão tanto estruturada quanto reflexiva do estado da arte.

Para nortear a investigação, este estudo busca responder às seguintes perguntas de pesquisa:

- Quais são as principais vulnerabilidades de segurança associadas à integração entre 5G e IPv6?
- Quais são as soluções mais eficazes propostas na literatura para mitigar as vulnerabilidades de segurança em redes que integram 5G e IPv6?
- Quais lacunas de pesquisa e problemas em aberto ainda persistem na segurança de redes que integram 5G e IPv6?

Responder a essas questões contribuirá para consolidar o conhecimento técnico-científico na área, além de fornecer subsídios ao desenvolvimento de soluções mais seguras e eficazes para redes de próxima geração

1.1 Objetivos

Nesta seção, serão apresentados o objetivo geral e os objetivos específicos do trabalho.

1.1.1 Objetivo Geral

Analisar de forma sistemática a produção científica relacionada à segurança na integração entre as tecnologias 5G e IPv6, por meio da aplicação de uma revisão sistemática da literatura, com o intuito de propor uma taxonomia que permita classificar os estudos existentes e identificar lacunas, desafios e tendências relevantes no tema.

1.1.2 Objetivos Específicos

- Levantar, classificar e analisar os principais trabalhos acadêmicos relacionados à segurança em redes 5G com IPv6 no período de 2018 a 2025;
- Identificar os principais desafios, ameaças e fragilidades de segurança descritos na literatura;
- Descrever as soluções, mecanismos criptográficos e abordagens mais recorrentes para mitigação dos problemas identificados;
- Propor uma taxonomia descritiva estruturada em três eixos: tecnologias, problemas de segurança e soluções;
- Construir uma taxonomia analítica com base na síntese crítica dos dados, relacionando ameaças, soluções e lacunas de pesquisa;
- Fornecer uma base sistematizada que auxilie pesquisadores e profissionais na compreensão dos principais desafios e direcionamentos futuros para segurança em redes 5G com IPv6.

2 FUNDAMENTAÇÃO TEÓRICA

Esta seção apresenta os conceitos fundamentais relacionados ao estudo da segurança em redes de próxima geração, com foco na integração entre 5G e IPv6.

2.1 5G

A quinta geração, ou 5G, de redes móveis é uma infraestrutura de comunicação sem fio projetada para proporcionar conectividade de alta velocidade, latência ultrabaixa e maior capacidade de suporte a dispositivos conectados. Ao contrário das tecnologias anteriores, o 5G não representa apenas um progresso, mas uma mudança tecnológica que estabelece novos padrões operacionais para satisfazer as necessidades de um mundo altamente interligado (Mendes, 2019).

A sua base tecnológica se fundamenta em avanços como ondas milimétricas, *Massive Multiple Input Multiple Output* (MIMO), e virtualização de redes, o que o torna mais flexível e adaptável a diferentes cenários de uso. O MIMO é uma tecnologia de redes sem fio que possibilita a transmissão e recepção simultânea de diversos sinais de dados por meio do mesmo canal de rádio. Enquanto as redes MIMO convencionais utilizam geralmente duas ou quatro antenas, o MIMO Massivo expande significativamente essa capacidade, podendo ultrapassar 100 antenas por estação base. Este aumento na quantidade de antenas requer o uso de frequências mais altas e comprimentos de onda mais curtos, em contraste aos padrões empregados pelas gerações anteriores de redes móveis (Moreira, 2018).

2.1.1 Características

Segundo Spadinger (2024), as redes de quinta geração (5G) representam um salto significativo em relação às gerações anteriores, oferecendo avanços expressivos em termos de desempenho e capacidade. Suas principais características incluem:

- **Alta Velocidade:** O 5G fornece velocidades de até 20 Gbps em condições ideais, permitindo transmissões de dados em tempo real, como *streaming* em 8K e aplicações de realidade aumentada (AR) e virtual (VR).
- **Baixa Latência:** A latência no 5G é reduzida para cerca de 1 milissegundo (ms), essencial para aplicações críticas como carros autônomos, cirurgias remotas e controle industrial em tempo real.
- **Suporte a IoT:** Com capacidade para conectar até 1 milhão de dispositivos por quilômetro

quadrado, o 5G é projetado para sustentar a Internet das Coisas (IoT) em larga escala, incluindo dispositivos industriais e residenciais.

"O 5G foi concebido para atender às exigências estabelecidas pelo IMT-2020, conforme descrito na especificação ITU-R M.2083" (Mendes, 2019). A Figura 1 destaca os principais parâmetros do IMT-2020, que atuam como orientações estratégicas fundamentais para orientar o desenvolvimento dessa tecnologia.

Figura 1 – Principais Parâmetros do IMT-2020.

Requisitos	Medidas		
Taxa de Dados	Pico	Downlink	20 Gbps
		Uplink	10 Gbps
	Experimentada pelo usuário	Downlink	100 Mbps – 1Gbps
		Uplink	50 Mbps
Eficiência Espectral	Melhor, em comparação ao 4G (IMT-Advanced), 3 vezes		
Capacidade de Tráfego por Área	10 Mbps/m^2		
Latência	1 ms		
Densidade de Conexão	10^6 dispositivos/km^2		
Eficiência Energética	Melhor, em comparação ao 4G (IMT-Advanced), 100 vezes (proporcional ao tráfego de dados)		
Mobilidade	500 Km/h		

Fonte: Mendes (2019), adaptado de Kim e Zarri (2018) e Series (2015).

2.1.2 Casos de Uso

Segundo a União Internacional de Telecomunicações (ITU), os três principais grupos de caso de uso do 5G são (Series, 2015):

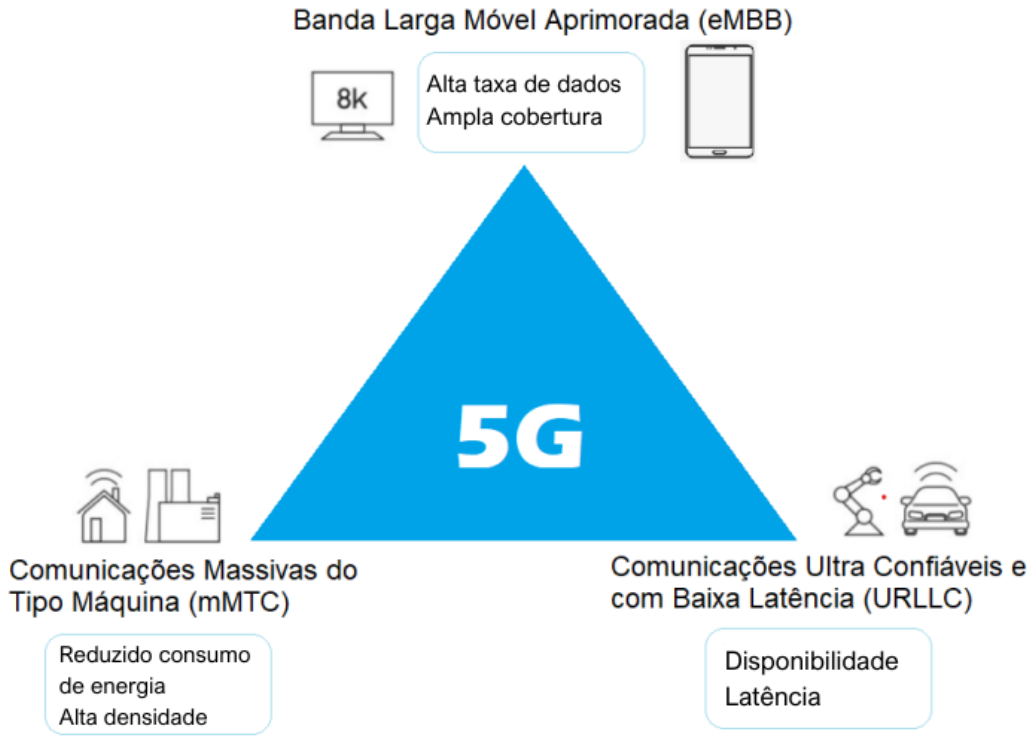
– **Banda Larga Móvel Aprimorada (EMBB):** apresenta uma integração com as tecnologias existentes no 4G, tem como foco aplicações que requerem alta velocidade de dados e uma extensa cobertura (Lima, 2022). Essa integração permite que o 5G complemente as redes 4G, oferecendo maior capacidade em áreas densamente povoadas e suporte a serviços que necessitam de transmissão em alta resolução, como *streaming* em 4K/8K, realidade

aumentada e jogos na nuvem.

- **Comunicações Ultra Confiáveis e com Baixa Latência (URLLC):** com o objetivo de atender às necessidades de aplicações que demandam baixa latência e alta disponibilidade, essa banda foi projetada para suportar aplicações críticas, como intervenções de medicina remota, veículos com direção autônoma ou assistida, além de processos de automação industrial (Lima, 2022).
- **Comunicações Massivas do Tipo Máquina (MMTC):** com objetivo de atender a dispositivos de baixo custo e baixo consumo de energia, dando prioridade, principalmente, à conexão de um grande número de dispositivos ao mesmo tempo. Essa tecnologia é projetada para operar utilizando a mesma infraestrutura de rede física, garantindo que diferentes dispositivos e aplicações coexistam sem causar conflitos (Lima, 2022).

Assim, cada cenário de uso apresenta exigências críticas distintas para garantir a garantia de Qualidade de Serviço (QoS - *Quality of Service*). A Figura 2 apresenta os requisitos fundamentais para cada cenário de aplicação do 5G.

Figura 2 – Requisitos dos Casos de Uso do 5G.



Fonte: Lima (2022).

2.1.3 Arquitetura do 5G

Segundo Oliveira *et al.* (2018), a arquitetura do 5G foi projetada para suportar uma ampla gama de aplicações e demandas de rede. Os principais componentes da arquitetura incluem:

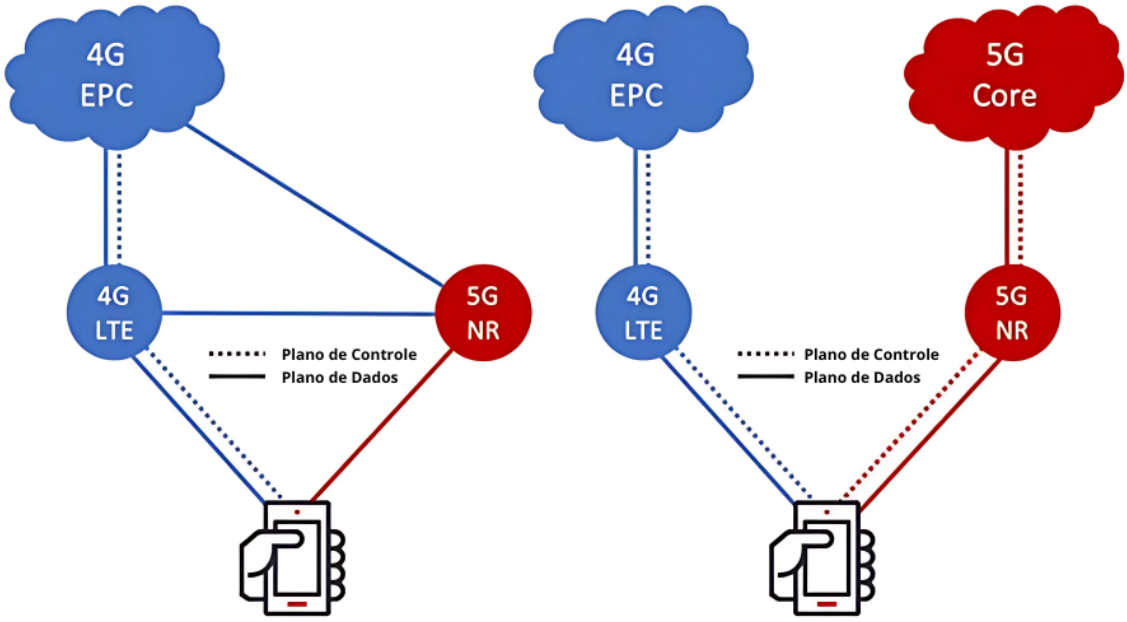
- **Rádio de Nova Geração (NR):** Substitui as tecnologias *Long Term Evolution* (LTE) e a quarta geração de redes móveis (4G), utilizando frequências em bandas baixas (sub-1 GHz), médias (1-6 GHz) e altas (ondas milimétricas acima de 24 GHz), o que permite maior flexibilidade de cobertura e capacidade.
- ***Core Network Baseado em Software*:** O core do 5G é baseado em tecnologias como virtualização de funções de rede (NFV) e redes definidas por software (SDN), que oferecem maior flexibilidade e capacidade de personalização.
- ***Network Slicing*:** Permite a criação de "fatias" virtuais de rede para atender diferentes necessidades, como alta largura de banda para *streaming* e baixa latência para aplicações críticas.
- ***Edge Computing*:** Reduz a latência ao processar dados próximos à origem, em vez de enviar para servidores distantes.

Os primeiros modelos de arquitetura da rede de 5G são o 5G *StandAlone* (SA) e o 5G *Non-StandAlone* (NSA). Na arquitetura NSA, também conhecida como rede não autônoma, as redes de acesso 5G e LTE operam em conjunto, possibilitando que os aparelhos usem as duas tecnologias ao mesmo tempo. Enquanto o plano de controle opera no LTE, o plano de usuário utiliza o 5G. Esta estratégia permite que as operadoras melhorem suas redes 4G progressivamente, convertendo-as em redes 5G. Dessa forma, é possível aumentar a taxa de transmissão de dados e reduzir a latência, aproveitando a infraestrutura já existente (Oliveira *et al.*, 2018).

A rede SA (*Standalone*), também conhecida como rede autônoma, é uma infraestrutura independente que possibilita a operação conjunta das redes 4G e 5G, sem a necessidade de interconexão entre elas. Nesta estrutura, cada tecnologia de acesso por rádio, como 5G e LTE, opera com seu próprio núcleo de rede, proporcionando maior independência e adaptabilidade na administração das conexões (Oliveira *et al.*, 2018).

A Figura 3 mostra simplificadamente os modos de funcionamento do 5G NSA e 5G SA.

Figura 3 – Modos 5G NSA e 5G SA.



Fonte: Adaptado de Lima (2022).

Diferentemente das gerações passadas, o 5G possibilita a combinação de tecnologias de várias gerações em várias configurações. Essa flexibilidade arquitetural permite que as operadoras ajustem a configuração da rede de acordo com o perfil dos clientes e as demandas específicas de cada local. Assim, o 5G não substituirá imediatamente as redes 4G, mas funcionará de forma integrada com elas, favorecendo uma transição gradual (Oliveira *et al.*, 2018).

2.2 Protocolo IPv6

O IPv6 utiliza endereços expressos em notação hexadecimal, um sistema numérico de base 16 que combina dígitos de 0 a 9 e letras de A a F. Diferente do IPv4, que adota a notação decimal pontuada (por exemplo, 192.168.1.10), o IPv6 emprega essa representação para oferecer um espaço de endereçamento imensamente maior, atendendo à crescente demanda da internet.

O Protocolo IPv4 tem sido a espinha dorsal da internet por décadas, funcionando de maneira robusta e eficaz com poucas alterações desde sua criação. Esse sucesso é evidenciado pelo crescimento exponencial da internet e pela ampla adoção do IPv4. No entanto, com o esgotamento dos endereços IPv4 e o aumento contínuo no número de dispositivos conectados à

rede mundial, tornou-se importante adotar um protocolo que suporte um número muito maior de endereços. O IPv6 surge como a solução para esse desafio, oferecendo um espaço de endereçamento significativamente maior e introduzindo uma série de melhorias em relação ao IPv4, incluindo aprimoramentos em segurança e eficiência no roteamento (Tanenbaum; Wetherall, 2011).

Segundo Tanenbaum e Wetherall (2011), o "IPv6 usa endereços de 128 bits, uma escassez desses endereços provavelmente não ocorrerá no futuro previsível". Os endereços IPv6 são representados utilizando uma sequência hexadecimal, onde cada dígito hexadecimal corresponde a 4 bits, totalizando 16 bits por bloco de 4 dígitos. Um endereço IPv6 completo é composto por 8 blocos de 16 bits, separados por dois pontos. Cada bloco é expresso como um valor hexadecimal, resultando em uma notação que oferece uma ampla capacidade de endereçamento. Por exemplo, um endereço IPv6 pode ser escrito como:

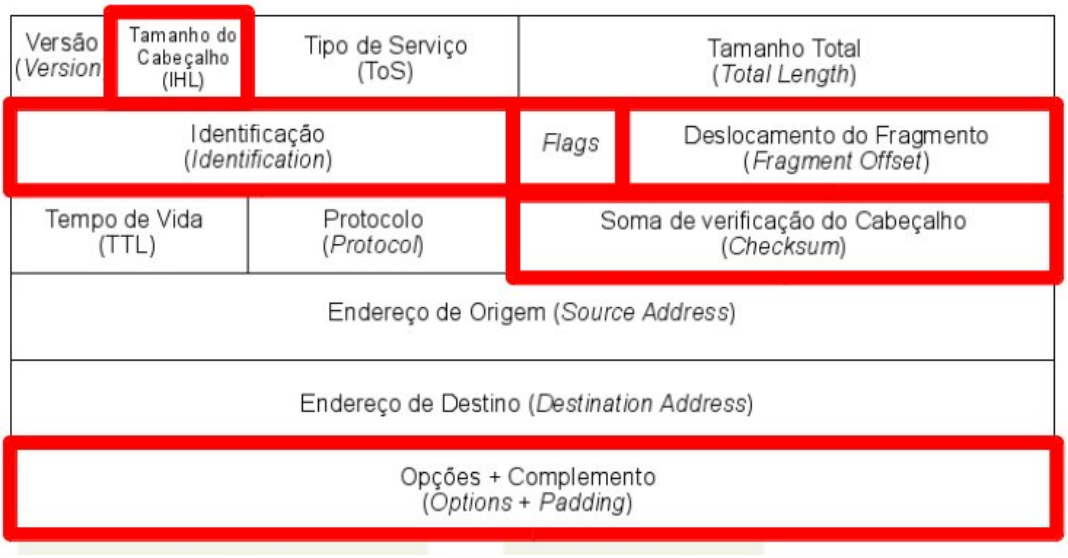
`2001:0DB8:AD1F:25E2:CADE:CAFE:F0CA:84C1`

Os campos do cabeçalho do IPv6 passaram por mudanças significativas em comparação com o IPv4, resultando em um cabeçalho mais simples e eficiente. O número de campos foi reduzido para apenas oito e o tamanho fixado de 40 bytes, proporcionando uma estrutura mais enxuta. Essa simplificação incluiu a eliminação de diversos campos presentes no IPv4. Por exemplo, o campo "Tamanho do Cabeçalho" (IHL) foi removido, uma vez que o tamanho do cabeçalho do IPv6 é fixo. Outros campos, como "Identificação", "Deslocamento de Fragmento", *"Flags"*, "Opções" e "Complementos", também foram suprimidos. Em vez disso, essas informações foram realocadas para cabeçalhos de extensão, que são utilizados para fornecer funcionalidades adicionais e manipular o tráfego de forma mais flexível (Deering; Hinden, 2017).

Deering e Hinden (2017) concluiu que, o cabeçalho do IPv6 ficou mais compacto e eficiente, com um design que melhora a performance e a simplicidade do protocolo, facilitando o processamento dos pacotes na rede.

O campo "Limite de Encaminhamento" no IPv6 substitui o antigo campo "Tempo de Vida" do IPv4. Essa mudança reflete uma evolução no controle da vida útil dos pacotes na rede. Além disso, o campo "Tipo de Serviço" foi desmembrado em dois novos campos: "Classe de Tráfego" e "Identificador de Fluxo". Esses campos fornecem uma abordagem mais granular para a gestão da qualidade e do tratamento dos pacotes. Essas e outras alterações são representadas nas Figuras 4 e 5, que ilustram os cabeçalhos do IPv4 e IPv6, respectivamente (Deering; Hinden, 2017).

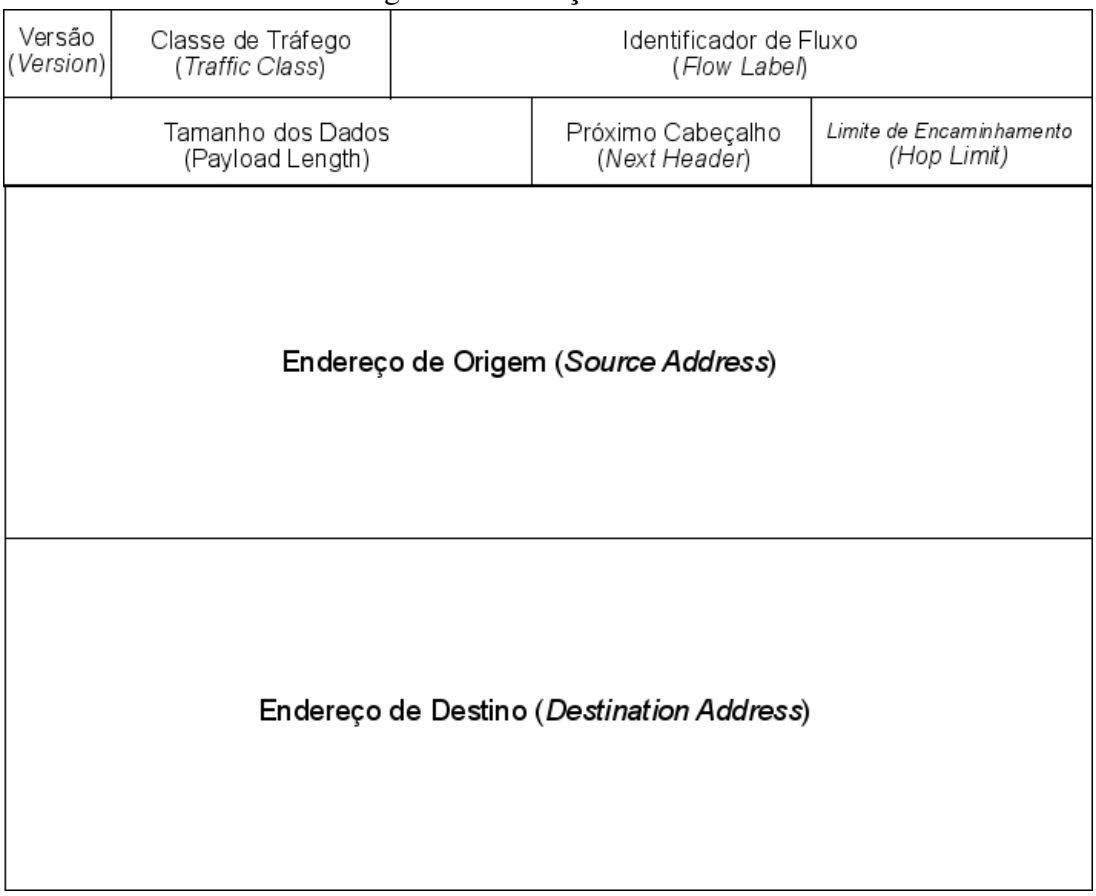
Figura 4 – Cabeçalho do IPv4, Campos que Perderam o Valor no Cabeçalho IPv6.



Fonte: IPV6.BR (2012a).

A Figura 5 é referente ao cabeçalho IPv6, após todos as alterações dos campos que perderam valor.

Figura 5 – Cabeçalho do IPv6.



Fonte: IPV6.BR (2012a).

O campo "Tipo de Serviço" foi substituído pelos campos "Classe de Tráfego" e "Identificador de Fluxo". O campo "Tamanho dos Dados" substitui o antigo campo "Tamanho Total". Os campos "Versão", "Endereço de Origem" e "Endereço de Destino", sofreram alteração apenas em seus tamanhos. O campo "Tamanho dos Dados" no IPv6 substitui o campo "Tamanho Total" do IPv4, refletindo uma abordagem mais direta e específica para a definição do tamanho dos dados transportados. Por outro lado, os campos "Versão", "Endereço de Origem" e "Endereço de Destino" mantêm suas funções básicas, mas com ajustes em seus tamanhos para acomodar as novas demandas do IPv6.

Para Comer (2016), as mudanças introduzidas pelo IPv6 podem ser agrupadas em 7 categorias:

- **Endereços Maiores**: o novo protocolo conta com 128 bits contra os 32 bits do IPv4;
- **Hierarquia de endereços estendida**: usa espaço de endereço maior para criar níveis adicionais de hierarquia de endereçamento, para um ISP alocar blocos de endereços para um cliente, por exemplo;
- **Formato de Cabeçalho Flexível**: uso de um datagrama totalmente novo que inclui um conjunto de cabeçalhos opcionais;
- **Opções Avançadas**: o IPv6 permite que um datagrama inclua informações de controle opcionais, não disponíveis no IPv4;
- **Provisão para Extensão de Protocolo**: em vez de especificar todos os detalhes, a capacidade de extensão do IPv6 permite que o IETF adapte o protocolo ao novo hardware de rede e novas aplicações;
- **Suporte para Autoconfiguração**: o IPv6 permite que os computadores em uma rede isolada atribuam endereços locais automaticamente.;
- **Suporte para Alocação de Recursos**: o novo protocolo inclui uma abstração de fluxos e bits para a especificação de diferenciação de serviço (*Diff Serv*). O último é idêntico ao *Diff Serv* do IPv4.

2.3 Endereçamento IPv6

Segundo IPV6.BR (2012b), o IPv6 define três categorias principais de endereçamento: *unicast*, *multicast* e *anycast*. Cada uma dessas categorias possui propósitos distintos no encaminhamento de pacotes e na comunicação entre dispositivos na rede, sendo eles:

- **Endereços *Unicast***: Destinados a uma única interface de rede, permitindo a comunicação

ponto a ponto. Cada endereço *Unicast* identifica exclusivamente um único dispositivo na rede, e os pacotes enviados para um endereço *Unicast* são recebidos por esse único destino;

- **Endereços *Anycast***: Associados a múltiplas interfaces, mas os pacotes enviados a um endereço *Anycast* são entregues apenas à interface mais próxima (ou à menos carregada, dependendo da configuração) em termos de roteamento. Este tipo de endereço é útil para serviços que precisam ser acessíveis de vários locais, como servidores de conteúdo distribuído
- **Endereços *Multicast***: Utilizados para enviar pacotes para um grupo específico de interfaces. Diferentemente do *unicast*, onde os pacotes são entregues a um único destinatário, os endereços *Multicast* permitem a distribuição de dados a vários dispositivos simultaneamente, que são parte de um grupo *Multicast*.

O endereçamento *unicast* é utilizado para identificar um único dispositivo na rede, sendo o tipo mais comum em comunicações ponto a ponto. Dentro dessa categoria, existem diferentes subtipos com funções específicas:

- ***Global Unicast*:** São endereços roteáveis globalmente na Internet, equivalentes aos endereços públicos no IPv4. Geralmente pertencem ao prefixo `2000::/3` e são atribuídos de forma hierárquica por registradores.
- ***Link-Local*:** Utilizados para comunicação entre dispositivos no mesmo enlace (ou segmento de rede), sem necessidade de roteadores. Possuem o prefixo `FE80::/10` e são essenciais para protocolos como *Neighbor Discovery Protocol* (NDP).
- ***Unique Local Address (ULA):*** Endereços utilizados em redes privadas, com escopo local semelhante ao IPv4 privado. Possuem o prefixo `FC00::/7` e não são roteáveis na Internet pública.

A compreensão desses tipos de endereçamento é essencial para o desenho seguro de redes IPv6, pois cada tipo possui implicações específicas para o controle de acesso, visibilidade externa e exposição a ataques.

Um plano de endereçamento deve formalizar a alocação de endereços IP para servidores, *gateways* e demais dispositivos da rede, além de definir as VLANs e os dispositivos associados a cada VLAN. A ausência de um plano de endereçamento pode levar a confusão e problemas de gerenciamento na rede. Como prática recomendada, mesmo na falta de um plano formalizado, é aconselhável adotar uma estratégia de nomeação para os dispositivos da rede. Isso

inclui configurar uma resolução *Domain Name System* (DNS) interna para a LAN, garantindo que servidores, impressoras e dispositivos que prestam serviços para a rede tenham endereços IP estáticos. Isso facilita a administração e a resolução de problemas, além de assegurar que os dispositivos possam ser facilmente localizados e identificados na rede.

Para todos os outros *hosts* conectados à rede, é recomendável definir um *pool* de endereços IP para alocação dinâmica. Esse *pool* deve abranger os IPs disponíveis para atribuição a cada *host*, bem como definir o período pelo qual um endereço IP é concedido a um *host* antes de ser liberado para outro ou renovado. Esse processo é gerenciado pelo servidor *Dynamic Host Configuration Protocol* (DHCP), que é um protocolo projetado especificamente para automatizar a configuração de endereços IP e outras informações de rede para dispositivos em uma rede. O DHCP simplifica a administração de endereços IP, garantindo uma alocação eficiente e evitando conflitos de endereços (Sousa, 2018).

No caso do IPv6, o protocolo equivalente é o DHCPv6. Segundo Sousa (2018), o DHCPv6 oferece diversas maneiras de atribuir endereços IPv6 aos dispositivos na rede:

- **Autoconfiguração *Stateless* (SLAAC)**: permite a aquisição de endereços globais sem o uso de DHCP;
- **Configuração Estática**: Modo de configuração manual de forma que o host tenha um endereço fixo, servidores em geral utilizam esse tipo de configuração.
- **Configuração Estática EUI-64**: modalidade de configuração estática que automaticamente gera o sufixo identificador do *host* utilizando 48 bits do MAC (*Media Access Control*) da placa de rede e mais 16 bits de uma função de expansão específica para fornecer os 64 bits necessários para o sufixo.
- **Opções Avançadas**: O IPv6 permite que um datagrama inclua informações de controle opcionais, não disponíveis no IPv4.
- **DHCPv6 *Stateful***: o servidor DHCPv6 mantém uma tabela com o estado dos clientes (endereço físico com os endereços lógicos atribuídos).
- **DHCPv6 *Stateless***: modalidade onde o servidor DHCP utiliza as funcionalidades da autoconfiguração para fornecer apenas algumas informações como o endereço de um servidor DNS, ou *Network Time Protocol* (NTP) para algumas aplicações, *Trivial File Transfer Protocol* (TFTP), etc.

2.3.1 SLAAC

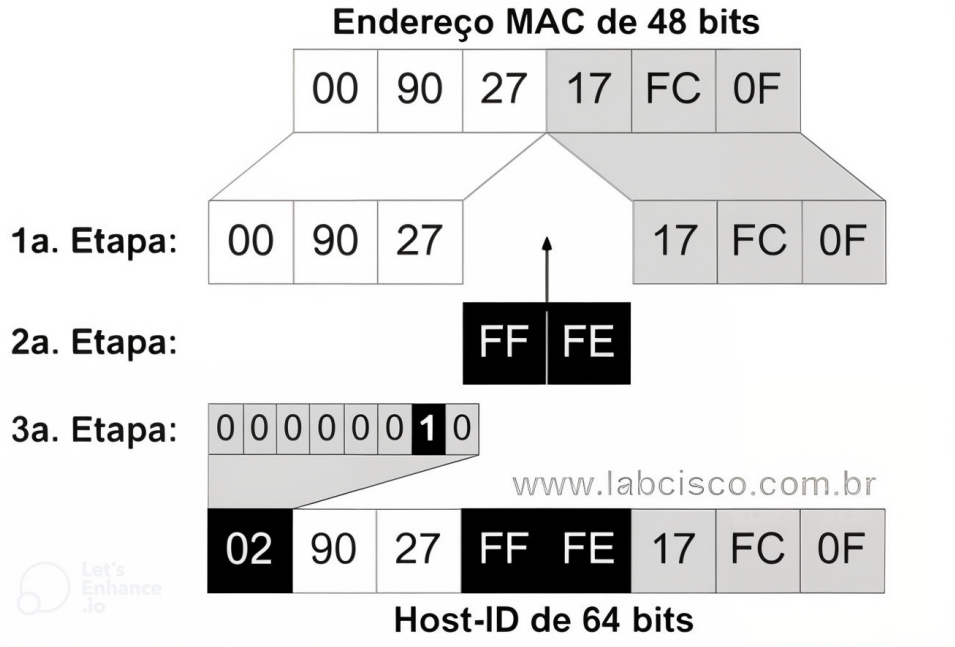
A autoconfiguração é uma das principais características do IPv6, permitindo a configuração automática de uma rede de computadores sem a necessidade de um servidor DHCP. Esse processo é conhecido como *Stateless Address Autoconfiguration* (SLAAC). O SLAAC é um método que não mantém registros dos endereços atribuídos (*stateless*), sendo a atribuição de endereços realizada automaticamente nos *hosts* (*autoconfiguration*), conforme descrito por (Brito, 2013).

Brito (2013) explica que "o processo de autoconfiguração dos endereços em redes baseadas no IPv6 consiste basicamente em duas etapas: (i) configuração do prefixo e (ii) configuração do sufixo de *host*".

Na configuração do prefixo, os *host* obtêm seu prefixo de rede através de mensagens *Internet Control Message Protocol Version 6* (ICMPv6) enviadas pelo roteador. Na segunda etapa, referente ao sufixo, os últimos 64 bits do endereço IPv6 são gerados a partir do endereço físico (MAC) da interface de rede, utilizando uma função de expansão conhecida como EUI-64. Dado que o endereço físico possui 48 bits, a EUI-64 adiciona os 16 bits restantes para completar o *Host-ID* de 64 bits, conforme descrito por Sousa (2018).

A Figura 6 apresenta uma explicação detalhada sobre o funcionamento do algoritmo EUI-64:

Figura 6 – Aplicação da Função EUI-64 na Identificação do Host.



Fonte: Brito (2013).

1. Recebe o endereço 48 bits e separá-o em duas porções iguais; sem o uso de DHCP;
2. Adiciona os algarismos hexadecimais “FFFE” (16 bits) entre as duas porções;
3. Inverte o 7º bit do primeiro byte para 1 (destacado em preto), indicando que o endereço é administrado localmente.

Após a conclusão do algoritmo, as porções do endereço são combinadas para gerar automaticamente um endereço global *unicast* atribuído à interface, possibilitando a conexão tanto no contexto local quanto na Internet. Embora as empresas possam optar por métodos alternativos de atribuição de endereços, o SLAAC se revela extremamente útil para simplificar o processo de atribuição, especialmente no contexto da IoT (Brito, 2013).

2.3.2 DHCPv6

O *Dynamic Host Configuration Protocol versão 6* (DHCPv6) é um protocolo que permite a configuração automatizada de endereços IP e parâmetros de rede em dispositivos conectados. Diferente de sua versão no IPv4, o DHCPv6 pode operar de duas formas:

- ***Stateful:*** O servidor DHCPv6 mantém um registro dos endereços atribuídos, gerenciando a alocação e o tempo de aluguel (*lease*) de cada IP.
- ***Stateless:*** O servidor não armazena informações sobre os endereços, apenas fornece configurações adicionais, como servidores DNS e *gateways*.

O DHCPv6 é amplamente utilizado em redes empresariais e de operadoras para garantir uma gestão centralizada de endereços e a aplicação eficiente de políticas de rede (Sousa, 2018).

2.4 Segurança em Redes 5G com IPv6

A adoção do 5G e do IPv6 traz avanços significativos para a conectividade, mas também impõe desafios de segurança que precisam ser analisados. Esta seção discute as principais ameaças e vulnerabilidades associadas a essas tecnologias.

2.4.1 Características do IPv6 para Segurança em Redes 5G

O IPv6 foi projetado com recursos que aprimoram a segurança das redes 5G. Um dos principais avanços é a eliminação da necessidade do *Network Address Translation* (NAT), permitindo que dispositivos tenham endereços públicos únicos. Isso reduz a complexidade da

rede e minimiza vulnerabilidades associadas ao mascaramento de IPs, comuns no IPv4 (IPV6.BR, 2012b).

- **Evita o NAT:** o IPv6 elimina a necessidade de NAT, permitindo que dispositivos se conectem diretamente à internet sem precisar compartilhar endereços IP. Essa conexão direta reduz a complexidade de redes e elimina alguns dos pontos de vulnerabilidade associados ao NAT (IPV6.BR, 2012b).
- **Isolamento de Dispositivos:** como cada dispositivo pode ter um endereço global único, é mais fácil rastrear atividades maliciosas ou identificar dispositivos comprometidos, aumentando a transparência e a segurança da rede (IPV6.BR, 2012b).

O amplo espaço de endereços do IPv6 também possibilita a implementação de tecnologias como a segmentação de rede (*network slicing*), que permite que diversas aplicações ou usuários funcionem em segmentos de rede separados, cada um com seus próprios blocos de endereços exclusivos. Isso garante maior segurança e eficiência.

Além disso, o IPv6 possui suporte nativo ao IPsec, embora o IPv4 também possa utilizar IPsec, essa funcionalidade não é nativa e requer configuração manual. No IPv6, o IPsec é um componente integrado do protocolo, garantindo mecanismos de autenticação de origem, criptografia de pacotes e integridade dos dados, tornando as comunicações mais seguras (Júnior *et al.*, 2005).

Esse suporte ao IPsec proporciona três pilares fundamentais para a segurança das redes:

- **Autenticação de Origem:** Verifica a identidade do emissor dos pacotes de dados, impedindo ataques de falsificação.
- **Confidencialidade:** Utiliza o *Encapsulating Security Payload* (ESP) para criptografar os dados transmitidos, garantindo que apenas o destinatário autorizado possa acessá-los.
- **Gerenciamento de Chaves:** Emprega mecanismos avançados para troca e renovação de chaves criptográficas, assegurando comunicações protegidas contra interceptações.

Além disso, o IPsec facilita a criação de túneis seguros na infraestrutura do 5G, contribuindo para redes mais resilientes e menos vulneráveis a ataques

Embora o IPv6 tenha sido projetado com suporte nativo ao IPsec, o que representa um avanço significativo em relação ao IPv4, essa característica por si só não é suficiente para garantir a segurança das comunicações em redes modernas. Primeiramente, o uso de IPsec, apesar de recomendado, não é necessariamente obrigatório em todas as implementações de

IPv6. Muitos sistemas e aplicações não ativam ou não configuram corretamente o IPsec por padrão, devido à sua complexidade de gerenciamento e à sobrecarga computacional envolvida, especialmente em dispositivos com recursos limitados, como os encontrados em ambientes IoT (Jankiewicz *et al.*, 2011).

Além disso, o IPsec atua na camada de rede e não fornece proteção contra vulnerabilidades que ocorrem em camadas superiores, como ataques a aplicações, falhas na autenticação de serviços, ou exploração de interfaces abertas comuns em arquiteturas 5G. Outro ponto crítico é que a gestão de chaves e a definição de políticas de segurança entre os nós ainda dependem de configurações manuais ou de soluções externas, como *Internet Key Exchange* (IKEv2), que podem apresentar falhas de configuração ou interoperabilidade (Arkko; Nikander, 2003).

Na prática, portanto, o IPsec oferece um conjunto importante de mecanismos de segurança - como confidencialidade, integridade e autenticação -, mas sua eficácia depende de uma implementação correta, da integração com outras medidas de segurança e da atualização constante frente às novas formas de ataque. Em redes 5G com funções virtualizadas e múltiplas interfaces, a segurança precisa ser tratada de forma mais abrangente, indo além do escopo do IPsec.

Outro benefício do IPv6 é a redução de erros humanos na configuração de endereços, pois ele permite a autoconfiguração dos dispositivos de maneira mais eficiente. Isso diminui a possibilidade de falhas manuais e melhora a segurança ao evitar configurações incorretas que poderiam ser exploradas por invasores (IPV6.BR, 2012b).

– **Redução de Erros Humanos:** a automação reduz os riscos de configurações manuais incorretas, que podem criar vulnerabilidades na rede.

Nas redes 5G, com uma alta densidade de dispositivos, a configuração automática facilita a expansão da rede. Essa capacidade é especialmente vantajosa em grandes ambientes corporativos e centros de dados, onde a rápida alocação e reconfiguração de endereços IP são essenciais para garantir a continuidade dos serviços sem intervenção manual.

Embora o IPv6 traga melhorias significativas para a segurança das redes 5G, algumas ameaças ainda precisam ser mitigadas. Entre os ataques mais preocupantes estão:

– ***Spoofing* de *Neighbor Discovery Protocol Spoofing* (NDP):** o invasor responde a solicitações de descoberta de vizinhança (*Neighbor Solicitation*) com informações falsas, fazendo com que os pacotes sejam enviados para ele em vez do destino legítimo. No IPv6, o espaço de endereços é vasto, tornando essa técnica menos eficaz. No entanto, é essencial

adotar medidas como filtros de pacotes e configurações adequadas de *firewall* para evitar exploração de sub-redes específicas (Liu *et al.*, 2022).

- **Sequestro de DNS (DNS *Hijacking*):** o atacante intercepta e altera consultas DNS, redirecionando os usuários para sites maliciosos. Isso pode ser mitigado com mecanismos como *Secure Neighbor Discovery* (SEND) e políticas rigorosas de roteamento (Sermpezis *et al.*, 2021).

Por fim, a integração do 5G com IPv6 representa um avanço na segurança das redes modernas, mas sua implementação segura exige o uso de boas práticas de configuração e monitoramento contínuo para mitigar riscos emergentes.

3 TRABALHOS RELACIONADOS

Neste capítulo, serão apresentados alguns trabalhos relacionados destacando as semelhanças e diferenças com o desenvolvido neste trabalho.

3.1 *5G Network Security Issues, Challenges, Opportunities and Future Directions: A Survey*

Para Humayun *et al.* (2021), o 5G representa um avanço significativo na tecnologia de redes celulares sem fio, trazendo benefícios como velocidades mais rápidas, maior capacidade e latência reduzida. O estudo aponta que essa tecnologia tem potencial para revolucionar diversas indústrias e economias, mas também destaca que questões de segurança permanecem como um desafio crítico. Apesar das promessas dos provedores de serviços 5G quanto à integridade, confidencialidade e disponibilidade de dados, ainda existem ameaças importantes que precisam ser abordadas. Dessa forma, o artigo oferece uma pesquisa detalhada sobre segurança no contexto do 5G, explorando ameaças, oportunidades e estratégias de mitigação.

No trabalho de Humayun *et al.* (2021), os autores apresentam uma análise abrangente das principais questões de segurança que envolvem as redes 5G. Eles discutem as ameaças mais comuns, como ataques direcionados à infraestrutura crítica e dispositivos conectados, e propõem estratégias de mitigação para aumentar a resiliência do sistema. Além disso, o estudo aborda os serviços de segurança oferecidos por redes 5G, como a proteção da confidencialidade e integridade dos dados, e explora os desafios de implementar esses serviços em larga escala.

O artigo se destaca por incluir um estudo de caso que ilustra as possibilidades do 5G em usos práticos, oferecendo uma visão tangível dos benefícios e restrições dessa tecnologia. Esta estratégia auxilia prestadores de serviços e pesquisadores a reconhecer áreas críticas e apontar caminhos para aprimoramentos futuros.

O estudo de Humayun *et al.* (2021) se concentra principalmente nas questões de segurança do 5G. O presente trabalho amplia a discussão ao integrar o papel do IPv6, destacando como essa tecnologia é essencial para atender às crescentes demandas de conectividade e segurança em redes de próxima geração. O presente trabalho tem um caráter integrador, conectando o 5G a outras tecnologias emergentes, enquanto o estudo de Humayun *et al.* (2021) tem um enfoque mais específico na segurança do 5G. Assim, este trabalho não apenas complementa os esforços existentes, mas também propõe uma visão mais ampla e aplicada, voltada para a construção de redes seguras e eficientes.

3.2 *A Systematic Analysis of 5G Networks With a Focus on 5G Core Security*

O trabalho de Tang *et al.* (2022) destaca que, mesmo após anos de desenvolvimento, os padrões do 5G continuam evoluindo, com especificações técnicas sendo ajustadas em tempo real. Nesse contexto, vários países já começaram a implementar redes 5G, principalmente por meio da abordagem *Non-Standalone* (NSA), que combina a infraestrutura 5G com redes 4G tradicionais. Contudo, muitas pessoas ainda têm dificuldades em compreender como o 5G pode sustentar aplicações críticas de maneira segura. Para abordar essa lacuna, o estudo oferece uma revisão detalhada de funcionalidades do 5G, como a arquitetura baseada em serviços (SBA), funções de rede chave (NFs), novos recursos de segurança no equipamento de usuário (UE) e na rede de acesso via rádio (RAN). Além disso, explora o modelo de confiança e mecanismos de segurança, como o protocolo 5G AKA (*5G Authentication and Key Agreement*) e o *Common API Framework* (CAPIF), além de levantar preocupações de segurança e propor direções para futuras pesquisas.

No artigo de Tang *et al.* (2022), os autores exploram a segurança no núcleo das redes 5G, analisando suas inovações tecnológicas. Eles detalham como a SBA reorganiza a entrega e gestão de serviços, ao mesmo tempo que introduz novas funções de rede projetadas para lidar com as demandas de conectividade e segurança. O trabalho também destaca avanços nos mecanismos de autenticação, como o protocolo 5G AKA, que melhora a proteção contra ataques de *spoofing* e *man-in-the-middle*.

Outro aspecto relevante é o *framework* CAPIF, que unifica a interação entre APIs, promovendo segurança e interoperabilidade em um ambiente de múltiplos fornecedores. Além de revisar essas características, os autores apontam potenciais vulnerabilidades associadas a essas inovações, como brechas em redes híbridas que combinam infraestruturas 4G e 5G, sugerindo que melhorias são necessárias para fortalecer o modelo de confiança e a resiliência da rede.

Enquanto o estudo de Tang *et al.* (2022) foca na segurança do núcleo das redes 5G, analisando suas inovações tecnológicas, o presente trabalho amplia o escopo ao integrar o IPv6 como um elemento fundamental para a evolução das redes 5G. Embora Tang *et al.* (2022) detalhem aspectos técnicos como a Arquitetura Baseada em Serviços (SBA), novas Funções de Rede (NFs) e melhorias nos protocolos de autenticação e segurança, eles não abordam a transição para o IPv6 nem seu impacto na conectividade e proteção das redes de próxima geração. Assim, este trabalho complementa a análise ao explorar a interdependência entre 5G e IPv6, destacando como essa integração afeta a segurança e o desempenho das comunicações.

3.3 *A Survey on Security Aspects for 3GPP 5G Networks*

O trabalho de Cao *et al.* (2019) aborda os aspectos de segurança das redes 5G propostas pelo *Third Generation Partnership Project* (3GPP), que define os padrões para a evolução do sistema *Long Term Evolution* (LTE) para o sistema de comunicação móvel de próxima geração (5G). O artigo apresenta uma visão geral da arquitetura e das funcionalidades de segurança das redes 3GPP 5G, explorando as inovações e os desafios associados. Em especial, os autores destacam novos recursos como o suporte massivo à Internet das Coisas (IoT), comunicação de Dispositivo para Dispositivo (D2D), comunicação Veículo para Tudo (V2X) e "fatias" de rede (*network slicing*). Esses avanços, embora promissores, trazem grandes desafios relacionados à segurança, como vulnerabilidades emergentes, requisitos críticos de proteção e questões de pesquisa ainda não resolvidas.

O estudo de Cao *et al.* (2019) apresenta contribuições significativas para o entendimento da segurança nas redes 5G, com uma abordagem detalhada das inovações propostas pelo 3GPP. Os autores discutem a arquitetura da rede 5G e as funcionalidades de segurança, evidenciando os mecanismos implementados para proteger os dados e garantir a confiabilidade do sistema.

O artigo destaca como novos recursos analisados o suporte em massa à IoT, que requer soluções dimensionáveis para administrar dispositivos diversificados; a comunicação D2D, que requer segurança direta entre dispositivos sem a necessidade de intermediários convencionais; e a comunicação V2X, que apresenta desafios únicos em contextos de mobilidade elevada. Além disso, as "fatias" de rede são caracterizadas como uma inovação crucial para possibilitar a execução de vários serviços em uma infraestrutura compartilhada, contudo, adicionam uma complexidade extra na aplicação de medidas de segurança.

O artigo também discute vulnerabilidades e desafios em cada uma dessas áreas, além de propor soluções existentes e destacar lacunas que necessitam de mais pesquisas. Por exemplo, os autores indicam que os protocolos atuais podem ser insuficientes para lidar com ataques em grande escala ou com a alta heterogeneidade dos dispositivos IoT.

Enquanto o estudo de Cao *et al.* (2019) é amplamente focado nos aspectos de segurança das redes 3GPP 5G e nos desafios específicos de novos recursos como IoT, D2D e V2X, o presente trabalho adota uma abordagem diferente, incluindo a análise do papel do IPv6 como facilitador da segurança e escalabilidade das redes 5G.

Um outro aspecto que difere é a abordagem das "fatias" de rede. Embora Cao *et al.*

(2019) apresentem vulnerabilidades específicas desta técnica, o objetivo deste estudo é entender como as soluções de segurança podem ser aprimoradas através da integração com o IPv6 e outras tecnologias emergentes. Portanto, este estudo complementa o de Cao *et al.* (2019), ao ampliar o escopo e propor uma visão mais ampla sobre a interação entre tecnologias e segurança nas redes modernas.

3.4 *A Comprehensive Survey on Core Technologies and Services for 5G Security: Taxonomies, Issues, and Solutions*

O trabalho de Park *et al.* (2021) apresenta um levantamento abrangente sobre as tecnologias e serviços centrais relacionados à segurança do 5G, destacando como essa geração de redes móveis surge para oferecer maior velocidade, menor latência e conectividade massiva a diversos dispositivos. Essa evolução do 4G, reforçada por novas tecnologias como arquitetura baseada em serviços (SBA), infraestrutura em nuvem e novas tecnologias de rádio, também traz desafios inéditos em termos de segurança e privacidade.

O artigo organiza e analisa ameaças à segurança no 5G, bem como soluções propostas, abordando aspectos como autenticação, disponibilidade, confidencialidade de dados, integridade e não-repúdio. O conceito de não-repúdio refere-se à garantia de que uma determinada ação ou comunicação não pode ser negada posteriormente por seu autor.

Adicionalmente, discute tecnologias emergentes associadas ao 5G, como *Blockchain*, redes definidas por software (SDN), inteligência artificial (IA), sistemas ciberfísicos, computação de borda móvel, comunicação dispositivo-a-dispositivo (D2D) e a Indústria 4.0. O estudo finaliza com aplicações e serviços baseados no 5G, ao mesmo tempo que apresenta os desafios e direções futuras para a segurança nessas redes.

O trabalho de Park *et al.* (2021) organiza os desafios e soluções de segurança no 5G em diferentes categorias, permitindo uma visão sistemática sobre os problemas enfrentados e as tecnologias aplicadas. Entre os principais serviços de segurança abordados estão:

- **Autenticação:** mecanismos avançados para verificar usuários e dispositivos conectados.
- **Disponibilidade:** estratégias para manter a rede funcional, mesmo sob ataque.
- **Confidencialidade e Integridade de Dados:** Proteção contra acessos não autorizados e modificações indevidas.
- **Não-repúdio:** garantia de que as ações realizadas na rede sejam atribuíveis aos respectivos agentes.

O estudo também analisa o impacto de tecnologias emergentes no 5G, como o *Blockchain*, que oferece novos modelos de confiança e descentralização, e a inteligência artificial (IA), utilizada para prever ataques e adaptar a infraestrutura de segurança em tempo real. A inclusão da computação de borda móvel e dos sistemas ciberfísicos demonstra como o 5G está preparado para suportar aplicações críticas em áreas como automação industrial e saúde conectada.

Por outro lado, o artigo destaca os desafios de integrar essas tecnologias em um ambiente 5G, como a escalabilidade, a interoperabilidade entre dispositivos heterogêneos e a necessidade de novas normas e protocolos. Os autores propõem direções futuras, como o aprimoramento de algoritmos de IA e a adaptação dos sistemas para lidar com ataques sofisticados.

Enquanto o estudo de Park *et al.* (2021) focam em uma abordagem ampla das tecnologias e serviços de segurança no 5G, o presente estudo se diferencia ao direcionar a análise para a integração do IPv6 no ecossistema 5G. O foco está na capacidade do IPv6 de atender às demandas crescentes de conectividade e escalabilidade, fundamentais para o avanço das redes de próxima geração.

Além disso, enquanto Park *et al.* (2021) exploram majoritariamente tecnologias emergentes, este trabalho enfatiza como essas inovações podem ser combinadas com padrões já consolidados, como o IPv6, para oferecer soluções práticas e integradas aos desafios de segurança. Assim, este estudo complementa a análise de Park *et al.* (2021), aprofundando-se na convergência tecnológica necessária para a implementação eficiente das redes de próxima geração.

3.5 *IPv6 Security Issues - A Systematic Review*

O trabalho de Shiranzaei e Khan (2018), apresenta uma revisão sistemática das principais questões de segurança relacionadas ao IPv6. Este estudo busca mapear e classificar vulnerabilidades, ameaças e desafios que surgem com a adoção do IPv6, fornecendo uma visão abrangente sobre o estado da segurança no contexto de redes que utilizam esse protocolo. Os autores se concentram em apontar lacunas na pesquisa atual e propor direções futuras para a mitigação de riscos associados.

O artigo destaca que, embora o IPv6 tenha sido projetado para superar as limitações do IPv4, como o esgotamento de endereços, sua introdução trouxe novos vetores de ataque

devido à complexidade adicional e à falta de maturidade em sua implementação. Entre as vulnerabilidades exploradas, os autores mencionam:

- **Problemas de Autoconfiguração de Endereços:** falhas na configuração automática de dispositivos podem ser exploradas por agentes mal-intencionados.
- **Ataques Baseados em *Multicast*:** o suporte expandido para *multicast* no IPv6 introduz desafios de segurança únicos, especialmente em redes de grande escala.
- **Adoção de Cabeçalhos Estendidos:** o uso de cabeçalhos adicionais oferece flexibilidade, mas também amplia a superfície de ataque ao permitir manipulações não previstas.
- **Transição de IPv4 para IPv6:** Técnicas como túneis e pilha dupla, embora úteis, criam cenários híbridos que aumentam as vulnerabilidades.

Shiranzaei e Khan (2018) analisam as práticas de segurança em uso atualmente, que incluem filtros de tráfego, *firewalls* dedicados ao IPv6 e protocolos como o IPsec. Contudo, a pesquisa destaca que a implementação desigual dessas soluções prejudica a proteção global do IPv6, indicando a necessidade de normas e regulamentos uniformes.

O trabalho de Shiranzaei e Khan (2018) foca no levantamento de vulnerabilidades do IPv6, sem organizar essas ameaças de forma estruturada. Já este estudo propõe uma taxonomia única, facilitando a análise das ameaças e das estratégias de mitigação no contexto do 5G. Além disso, enquanto Shiranzaei e Khan (2018) abordam soluções de segurança de forma dispersa, este trabalho as classifica em um modelo padronizado, oferecendo uma visão mais clara e aplicável às redes de próxima geração.

3.6 Analise Comparativa

Nesta seção é realizada uma análise comparativa de forma ampla entre os trabalhos relacionados e o trabalho proposto.

Um dos critérios mais marcantes que diferencia este trabalho dos estudos analisados, é o escopo abrangente na integração entre 5G, IPv6 e segurança em redes de próxima geração. Enquanto muitos dos estudos analisados, como Cao *et al.* (2019) e Park *et al.* (2021), abordam a segurança no contexto do 5G e seu impacto na IoT, eles não consideram de maneira detalhada a integração do IPv6 nas redes de próxima geração. No entanto, a transição para o IPv6 é importante para o desenvolvimento das redes 5G, especialmente devido à crescente demanda por endereçamento global e conectividade massiva.

O trabalho de Humayun *et al.* (2021) foca na análise de ameaças e estratégias de miti-

gação na rede 5G, com uma abordagem voltada para os desafios operacionais da segurança. Outro aspecto relevante é que alguns trabalhos, como Shiranzaei e Khan (2018), focam principalmente na segurança do IPv6, discutindo vulnerabilidades, desafios e soluções associadas ao protocolo. Embora esse estudo seja fundamental para compreender as ameaças no IPv6, ele não explora sua aplicação no contexto do 5G, deixando lacunas importantes sobre como esse protocolo pode ser implementado e protegido em redes móveis avançadas. Diferentemente disso, o presente trabalho conecta diretamente essas três frentes: 5G, IPv6 e segurança. Analisando como a evolução dos protocolos impacta a cibersegurança e a comunicação em ambientes heterogêneos.

Além disso, enquanto trabalhos como Tang *et al.* (2022) e Park *et al.* (2021) exploram diferentes camadas de segurança e a mitigação de ataques em redes 5G, eles não fornecem uma visão detalhada das taxonomias existentes, algo que o presente trabalho propõe ao realizar uma revisão das abordagens, classificações e soluções presentes na literatura. Dessa forma, esta pesquisa discute os desafios e ameaças existentes, e também organiza e classifica as estratégias utilizadas para enfrentá-los, servindo como um referencial consolidado para futuros estudos.

Outro fator diferenciador é a abordagem comparativa entre segurança no 5G e a adoção do IPv6. Enquanto alguns trabalhos, como Park *et al.* (2021), discutem a segurança no 5G de forma ampla, esta pesquisa foca especificamente no impacto do IPv6 nesse contexto, analisando os desafios de segurança que surgem dessa integração. Esse nível de detalhamento é essencial para compreender as vulnerabilidades e estabelecer diretrizes que fortaleçam a cibersegurança das redes de próxima geração.

Por fim, enquanto os estudos analisados contribuem significativamente para a compreensão de aspectos isolados, como segurança no 5G ou no IPv6, este trabalho se diferencia por oferecer uma análise estruturada e aprofundada da segurança no 5G em relação ao IPv6. Ao revisar taxonomias e explorar desafios específicos dessa integração, ele proporciona um referencial técnico que pode auxiliar pesquisadores e profissionais na tomada de decisões e no desenvolvimento de soluções mais seguras para redes de próxima geração.

Para consolidar a comparação entre os trabalhos relacionados e o presente estudo, o Quadro 1 apresenta uma análise comparativa baseada em critérios essenciais para a compreensão da segurança em redes 5G e IPv6. Os critérios selecionados refletem aspectos como a presença de mapeamentos sistemáticos de ameaças, a proposição de uma taxonomia e a consideração de estratégias de mitigação. Essa comparação permite evidenciar como cada estudo contribui para a literatura e destacar as lacunas que o trabalho proposto busca preencher.

Quadro 1 – Comparativo Entre os Trabalhos Relacionados e o Proposto.

Critério	**Humayun *et al.* (2021)**	**Tang *et al.* (2022)**	**Cao *et al.* (2019)**	**Park *et al.* (2021)**	**Shiranzaei e Khan (2018)**	**Trabalho Proposto**
Foco na Segurança do IPv6					✓	✓
Foco na Segurança do 5G	✓	✓		✓		✓
Análise da Integração entre 5G e IPv6		✓				✓
Mapeamento de Ameaças e Vulnerabilidades	✓	✓	✓	✓	✓	✓
Abordagem Sistematizada (Survey)	✓	✓	✓	✓	✓	✓
Proposição de Taxonomia				✓		✓
Discussão sobre Estratégias de Mitigação	✓	✓	✓	✓		✓

Fonte: Elaborado pelo autor.

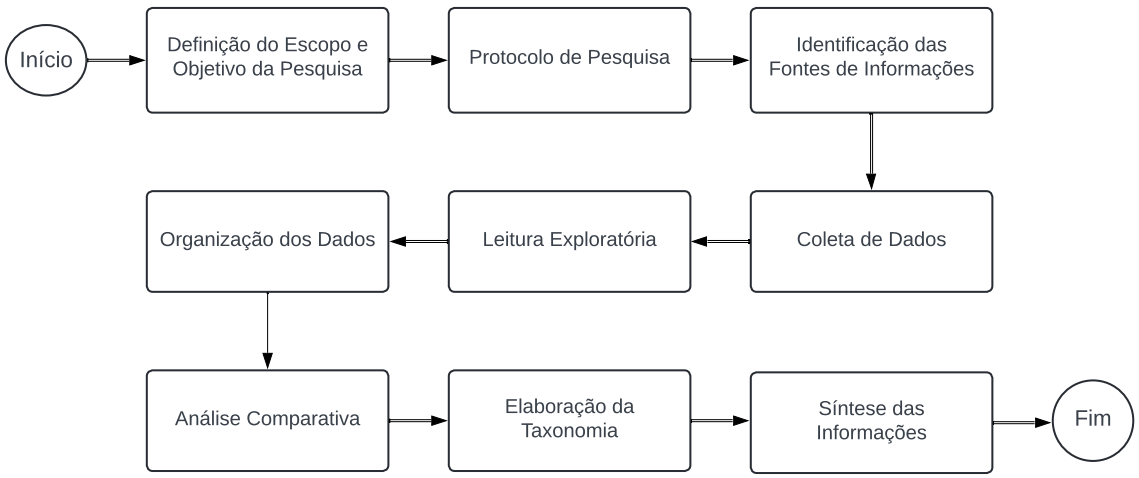
A partir do Quadro 1, observa-se que, embora diversos trabalhos abordem aspectos importantes da segurança no 5G e no IPv6, o presente estudo se diferencia por oferecer uma análise conjunta e interconectada desses temas. Diferentemente dos estudos analisados, ele se destaca por explorar a integração entre 5G e IPv6 no contexto da segurança, além de propor uma taxonomia específica para sistematizar as ameaças e desafios existentes. Além disso, ao abordar tanto vulnerabilidades quanto estratégias de mitigação, o trabalho proposto visa fornecer um referencial técnico, capaz de auxiliar pesquisadores e profissionais no desenvolvimento de soluções mais seguras para redes de próxima geração.

4 METODOLOGIA

Neste capítulo serão apresentados os passos necessários para a execução deste trabalho. A Figura 7 apresenta os seguintes passos para a execução do trabalho: (i) Definição do escopo e objetivo da pesquisa; (ii) Protocolo de pesquisa; (iii) Identificação das fontes de informações; (iv) Coleta de dados; (v) Leitura exploratória; (vi) Organização dos dados; (vii) Análise comparativa; (viii) Elaboração da taxonomia; (ix) Síntese das informações.

A execução desta pesquisa seguiu um conjunto estruturado de etapas organizadas de forma sequencial. A Figura 7 apresenta o fluxograma metodológico adotado, destacando todas as fases da revisão sistemática, desde a definição do escopo até a síntese das informações obtidas. Cada uma dessas etapas será detalhada nas subseções seguintes, permitindo a rastreabilidade e replicabilidade do processo de investigação.

Figura 7 – Fluxograma de Execução da Metodologia.



Fonte: Elaborado pelo autor.

4.1 Definição do Escopo e Objetivo da Pesquisa

O primeiro passo na execução deste trabalho foi a definição clara do escopo e dos objetivos da pesquisa, uma etapa fundamental para guiar todo o processo investigativo e garantir que a pesquisa se mantenha focada e alinhada com os propósitos definidos. O escopo da pesquisa foi estabelecido com base na necessidade de compreender as tecnologias emergentes que estão transformando o cenário das redes de comunicação, com um enfoque especial no 5G e no

protocolo IPv6 e sua relação com a segurança das redes.

O progresso das redes 5G e a mudança para o IPv6 apresentam novos desafios para a segurança, pois ambos aumentam consideravelmente a quantidade de aparelhos conectados e a complexidade das redes. A pesquisa buscou identificar e comparar as principais ameaças associadas a essas tecnologias, destacando como os protocolos de segurança atuais podem ser modificados ou melhorados para atender às necessidades das redes de próxima geração.

A presente revisão sistemática buscou responder às seguintes questões:

- Quais são as principais vulnerabilidades de segurança relacionadas à integração entre as tecnologias 5G e IPv6?
- Quais soluções têm sido propostas na literatura para mitigar os riscos de segurança em redes que utilizam 5G e IPv6?
- Existem lacunas ou desafios ainda não resolvidos que demandam novos estudos ou abordagens no contexto de 5G e IPv6?

4.2 Protocolo de Pesquisa

A fim de garantir transparência e reprodutibilidade na realização desta revisão sistemática, foi elaborado um protocolo de pesquisa com base nas diretrizes propostas por Kitchenham (2004) e Kitchenham *et al.* (2009), amplamente reconhecidas na condução de revisões sistemáticas na área de Engenharia de Software e correlatas. A metodologia adotada contempla três fases principais, conforme o Quadro 2.

Quadro 2 – Etapas da Revisão Sistemática segundo Kitchenham.

Fase	**Descrição das Atividades**
Planejamento da Revisão	Definir o objetivo geral, formular as questões de pesquisa, selecionar bases de dados (Google Scholar, IEEE Xplore), elaborar strings de busca e estabelecer critérios de inclusão e exclusão.
Condução da Revisão	Executar as buscas com base nas strings definidas, aplicar filtros de inclusão/exclusão, ler os artigos (título, resumo e texto completo), e organizar os dados em planilhas.
Análise e Apresentação dos Resultados	Analisar os dados coletados, categorizar os estudos por tipo de vulnerabilidade ou solução, elaborar uma taxonomia e sintetizar os achados, identificando lacunas na literatura.

Fonte: Adaptado de Kitchenham (2004) e Kitchenham *et al.* (2009).

Para operacionalizar essas etapas de forma sistemática, foi elaborado um protocolo detalhado que define os elementos-chave da pesquisa, conforme apresentado no Quadro 3.

Quadro 3 – Protocolo da Revisão Sistemática.

Elemento	**Descrição**
Objetivo da Revisão	Investigar as principais vulnerabilidades e soluções de segurança em redes que integram tecnologias 5G e IPv6.
Questões de Pesquisa	1. Quais são as principais vulnerabilidades de segurança associadas à integração entre 5G e IPv6? 2. Quais são as soluções mais eficazes propostas na literatura para mitigar as vulnerabilidades de segurança em redes que integram 5G e IPv6? 3. Quais lacunas de pesquisa e problemas em aberto ainda persistem na segurança de redes que integram 5G e IPv6?
Bases de Dados	*Google Scholar*, *IEEE Xplore*, *ACM Digital Library*, *Elsevier*.
Strings de Busca	*"5G" AND "IPv6" AND "Security"*, *"5G" AND "IPv6" AND ("Vulnerabilities" OR "Threats")*, *("IPv6" OR "5G") AND ("Cybersecurity" OR "Security" OR "Threats" OR "Vulnerabilities")*.
Critérios de Inclusão	Artigos entre 2018 e 2025; texto completo disponível; que abordem 5G, IPv6 e segurança.
Critérios de Exclusão	Trabalhos duplicados; artigos sem foco em segurança; estudos sem proposta ou avaliação clara.
Procedimento de Seleção	Leitura do título, resumo e conclusões; seguida de leitura completa para os artigos selecionados.
Procedimento de Análise	Extração das contribuições, categorização dos temas, agrupamento em taxonomias e comparação entre abordagens.
Ferramentas Utilizadas	*Parsifal* (elaboração do protocolo e triagem), *Zotero* (referências), *Google Sheets* (análise de dados).
Período de Busca	Publicações entre 2018 e 2025.

Fonte: Elaborado pelo autor, com base em Kitchenham (2004) e Kitchenham *et al.* (2009).

4.2.1 Construção das Strings de Busca

As *strings* de busca foram construídas com base nos três eixos centrais do tema: a tecnologia de redes móveis de quinta geração (5G), o protocolo de endereçamento IPv6, e os aspectos relacionados à segurança e ameaças cibernéticas. As expressões foram elaboradas de forma a capturar variações terminológicas e semânticas presentes na literatura científica, buscando maximizar a sensibilidade da busca inicial.

Foram utilizadas as seguintes combinações:

– *“5G” AND “IPv6” AND “Security”*

Essa *string* representa a formulação mais direta e objetiva, focada em recuperar artigos que abordam explicitamente os três temas centrais do estudo. Foi empregada como base para avaliar a interseção direta entre 5G, IPv6 e segurança em redes.

– *“5G” AND “IPv6” AND (“Vulnerabilities” OR “Threats”)*

Essa variação tem como objetivo capturar estudos que tratam de riscos e ameaças, mesmo quando não utilizam o termo genérico *"security"*. Os termos *“vulnerabilities”* e *“threats”* permitem incluir publicações com foco mais específico em falhas ou ataques, ampliando a cobertura temática.

– *(“IPv6” OR “5G”) AND (“Cybersecurity” OR “Security” OR “Threats” OR “Vulnerabilities”)*

Essa *string* mais ampla foi utilizada para recuperar estudos que mencionam pelo menos uma das tecnologias (5G ou IPv6) associada a termos ligados à segurança, mesmo que não abordem explicitamente a integração entre ambas. Foi empregada como forma de garantir cobertura máxima e permitir posterior refinamento pelos critérios de inclusão e exclusão.

A escolha por múltiplas *strings* buscou equilibrar abrangência e precisão, conforme metodologia descrita por Kitchenham (2004). Todas as strings foram testadas previamente nas bases selecionadas para verificar sua efetividade e relevância dos resultados obtidos. Os termos foram definidos com base em leituras preliminares, glossários técnicos e estudos similares, garantindo consistência com a terminologia empregada na área de redes e segurança.

Além disso, foi registrada a quantidade de artigos retornados por cada *string* de busca em cada base utilizada, conforme mostrado no Quadro 4.

Quadro 4 – Quantidade de Artigos Retornados por *String* e Por Base de Dados.

String de Busca	**IEEE Xplore**	**Google Scholar**	**Total**
“5G” AND “IPv6” AND “Security”	29	1.350	1.379
“5G” AND “IPv6” AND (“Vulnerabilities” OR “Threats”)	8	912	920
(“IPv6” OR “5G”) AND (“Cybersecurity” OR “Security” OR “Threats” OR “Vulnerabilities”)	971	16.500	17.471
Total de artigos brutos (sem remoção de duplicatas)	**1.008**	**18.762**	**19.770**

Os dados do Quadro 4 representam a quantidade total de artigos retornados em cada busca, antes da aplicação dos critérios de exclusão, filtragem de duplicatas e avaliação da qualidade metodológica. As buscas foram realizadas manualmente nas interfaces das plataformas,

respeitando os mesmos critérios temporais (2018–2025) e usando filtros automáticos disponíveis para seleção por título, resumo e palavras-chave.

Diante do grande volume de resultados, especialmente no *Google Scholar*, foi necessário adotar uma estratégia de triagem inicial para tornar o processo de seleção viável. Assim, optou-se por analisar manualmente os resultados contidos nas primeiras dez páginas de cada combinação de *string* por base. Essa decisão considerou a relevância decrescente dos resultados conforme o ranqueamento dos algoritmos de busca, conforme discutido por Kitchenham (2004) e Kitchenham *et al.* (2009). Essa abordagem resultou em aproximadamente 600 artigos analisados por título e resumo, dos quais 60 foram inicialmente selecionados por apresentarem aderência mínima ao escopo da pesquisa (cobertura de pelo menos dois dos três eixos centrais: 5G, IPv6 ou segurança). Esses 60 compuseram o conjunto inicial antes da aplicação dos critérios formais de inclusão e exclusão.

Tal medida buscou equilibrar viabilidade prática e rigor metodológico, permitindo que a revisão sistemática mantivesse sua abrangência temática sem comprometer a exequibilidade do processo de análise.

4.2.2 Identificação das Fontes de Informações

Após a definição do escopo da pesquisa, o passo seguinte consistiu na identificação das fontes de informação relevantes para sustentar teoricamente e metodologicamente a revisão sistemática. Considerando a ampla disponibilidade de materiais na internet, optou-se por restringir a busca a bases de dados acadêmicas reconhecidas, que garantem a qualidade e a confiabilidade dos artigos incluídos.

Foram selecionadas quatro bases principais: *IEEE Xplore*, *Google Scholar*, *ACM Digital Library* e *Elsevier (ScienceDirect)*. A base *IEEE Xplore* foi escolhida por seu alto rigor editorial e pela relevância dos periódicos nas áreas de redes de computadores, segurança da informação e comunicações. O *Google Scholar*, por sua vez, foi utilizado por sua ampla cobertura multidisciplinar e facilidade de acesso, permitindo recuperar trabalhos relevantes publicados em diferentes fontes.

A *ACM Digital Library* foi incorporada por sua tradição em pesquisas da área de computação, especialmente nos campos de arquitetura de redes e segurança aplicada. Já a *Elsevier*, por meio da plataforma *ScienceDirect*, ofereceu contribuições relevantes com artigos voltados a abordagens práticas e experimentais em contextos avançados de redes.

A escolha dessas bases se justifica pela complementaridade de suas coleções, garantindo amplitude temática, diversidade metodológica e rigor acadêmico. Tal seleção permitiu reunir um conjunto expressivo de estudos pertinentes à interseção entre segurança, redes 5G e IPv6, fornecendo alicerces robustos para a formulação da taxonomia e das análises subsequentes.

4.3 Coleta e Análise dos Dados

Esta etapa corresponde à execução prática do protocolo de pesquisa definido anteriormente. A coleta e a análise dos dados foram conduzidas por meio de buscas sistemáticas nas bases selecionadas, seguidas da aplicação de critérios rigorosos de inclusão, exclusão e avaliação qualitativa. As subseções a seguir detalham os procedimentos metodológicos adotados.

4.3.1 Definição das Strings de Busca

Para garantir a precisão na recuperação dos estudos, foram definidas previamente as *strings* de busca com base nos principais termos relacionados ao tema da pesquisa, como *"5G"*, *"IPv6"* e *"Security"*. Essas strings foram aplicadas nas bases acadêmicas *Google Scholar* e *IEEE Xplore*, conforme apresentado no Quadro 5. O período de 2018 a 2025 foi escolhido por abranger a fase de adoção acelerada das redes 5G em escala global, bem como os esforços crescentes de transição do IPv4 para o IPv6 em diversos setores. A partir de 2018, observa-se uma intensificação nas publicações técnicas sobre segurança em redes móveis de quinta geração, impulsionadas por lançamentos comerciais e padronizações importantes realizadas pelo 3GPP. Simultaneamente, o esgotamento dos endereços IPv4 e a integração massiva de dispositivos IoT exigiram maior atenção ao IPv6 como solução escalável. Desse modo, o recorte adotado visa capturar tanto os desafios emergentes quanto as soluções mais recentes no cruzamento entre essas duas tecnologias e seus impactos em segurança.

Quadro 5 – Strings de Busca Aplicadas nas Bases de Dados.

String de Busca	**Bases Utilizadas**	**Filtros Aplicados**
"5G" AND "IPv6" AND "Security"	*Google Scholar, IEEE Xplore*	Artigos publicados entre 2018 e 2025
"5G" AND "IPv6" AND ("Vulnerabilities" OR "Threats")	*Google Scholar, IEEE Xplore*	Artigos com foco em redes 5G e IPv6
("IPv6" OR "5G") AND ("Cybersecurity" OR "Security" OR "Threats" OR "Vulnerabilities")	*Google Scholar, IEEE Xplore*	Artigos completos disponíveis

Fonte: Elaborado pelo autor.

A utilização de diferentes *strings* de busca se justifica pela necessidade de ampliar a cobertura dos estudos relevantes, garantindo maior abrangência e refinamento na seleção dos artigos. A primeira *string*, *"5G" AND "IPv6" AND "Security"*, foi formulada para capturar trabalhos diretamente focados na interseção entre essas três tecnologias, atuando como filtro principal e mais restritivo. Já a segunda string, *"5G" AND "IPv6" AND ("Vulnerabilities"OR "Threats")*, teve como objetivo identificar pesquisas que abordassem especificamente aspectos de segurança sob a ótica das vulnerabilidades e ameaças, permitindo mapear problemas recorrentes na literatura. Por fim, a terceira *string*, mais ampla, combinando *("IPv6" OR "5G")* com *("Cybersecurity" OR "Security" OR "Threats" OR "Vulnerabilities")*, foi empregada para garantir a recuperação de estudos que, mesmo não focando exclusivamente na integração entre 5G e IPv6, pudessem trazer contribuições relevantes sobre segurança em pelo menos um desses domínios. Essa abordagem estratégica permite mitigar perdas de artigos importantes devido a variações terminológicas, ao mesmo tempo em que favorece a diversidade e representatividade da amostra analisada.

4.3.2 Critérios de Inclusão e Exclusão dos Estudos

Com base nas práticas recomendadas para revisões sistemáticas, foram estabelecidos critérios objetivos com o intuito de selecionar os estudos mais relevantes, confiáveis e alinhados ao escopo desta pesquisa. O Quadro 6 apresenta os critérios de inclusão e exclusão adotados.

Quadro 6 – Critérios de Inclusão e Exclusão dos Estudos.

Tipo de Critério	**Descrição**
Inclusão	– Publicações entre 2018 e 2025; – Disponibilidade em texto completo; – Abordagem conjunta das tecnologias 5G e IPv6; – Foco em segurança, vulnerabilidades ou soluções; – Estudos publicados em periódicos ou conferências com revisão por pares.
Exclusão	– Artigos duplicados; – Documentos sem revisão por pares; – Trabalhos sem foco direto em segurança de redes; – Publicações com menos de quatro páginas.

Fonte: Elaborado pelo autor.

4.3.3 Critérios de Qualidade dos Estudos

Além dos critérios de inclusão e exclusão, foi aplicada uma avaliação qualitativa para garantir a consistência metodológica dos estudos. Para isso, foi elaborado um conjunto de critérios objetivos, permitindo atribuir uma pontuação binária (0 ou 1) a cada aspecto avaliado. Apenas os estudos com pontuação total igual ou superior a 3 (de um máximo de 5) serão mantidos na análise final. O Quadro 7 apresenta os critérios escolhidos.

Quadro 7 – Critérios de Qualidade para Seleção dos Estudos.

Critério Avaliado	**Pontuação (0 ou 1)**
O artigo está escrito em inglês?	0 ou 1
O artigo apresenta claramente os objetivos da pesquisa?	0 ou 1
O artigo propõe uma solução para vulnerabilidades ou ameaças de segurança?	0 ou 1
O artigo descreve uma metodologia de análise, simulação ou experimento?	0 ou 1
O artigo menciona 5G e IPv6 no resumo e/ou conclusão?	0 ou 1

Fonte: Elaborado pelo autor.

A aplicação dos critérios de qualidade permitiu refinar a seleção dos estudos com base em sua aderência metodológica e relevância temática. Observou-se que os critérios mais frequentemente atendidos foram: (i) o uso do idioma inglês e (ii) a presença explícita dos objetivos da pesquisa. Esses dois critérios apresentaram pontuação positiva na maioria dos artigos inicialmente elegíveis.

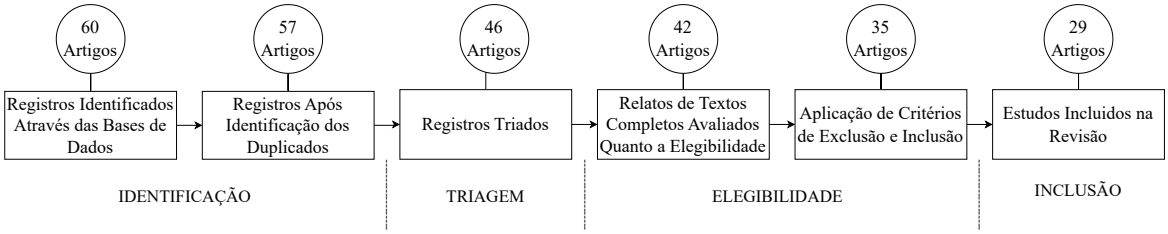
Por outro lado, os critérios que mais contribuíram para a exclusão de estudos foram: (i) a ausência de proposição de solução concreta para ameaças de segurança e (ii) a falta de uma metodologia claramente descrita (como análise estruturada, simulação ou experimento). Tais ausências indicam que parte da literatura revisada, embora relevante ao contexto geral de redes, não oferecia contribuições práticas ou avaliativas suficientemente robustas para os objetivos desta revisão sistemática.

O quinto critério — a menção simultânea a 5G e IPv6 no resumo ou conclusão — também teve papel relevante para o corte, já que diversos estudos abordavam apenas uma das tecnologias de forma isolada, sem considerar a integração entre elas. Com isso, a pontuação total de muitos artigos ficou abaixo do limiar mínimo (3 pontos), resultando em sua exclusão do conjunto final.

Essa avaliação assegurou a manutenção de estudos mais completos, consistentes e alinhados ao escopo proposto, ao mesmo tempo em que permitiu documentar de forma transparente os motivos para descarte dos demais.

A Figura 8 apresenta um fluxograma que resume o processo de seleção dos artigos, detalhando a quantidade de registros em cada fase, desde a busca inicial até a definição final do corpus analisado.

Figura 8 – Fluxograma da Seleção de Estudos.



Fonte: Elaborado pelo autor.

4.3.4 Ferramentas de Apoio à Organização dos Dados

Com o objetivo de garantir rastreabilidade, padronização e eficiência durante o processo de revisão sistemática, foram utilizadas ferramentas específicas para apoiar a organização, o gerenciamento e a análise dos estudos selecionados.

O *Parsifal* foi utilizado na etapa inicial para a construção do protocolo de pesquisa e para a triagem dos artigos, permitindo o registro dos critérios aplicados e o rastreamento das decisões de inclusão e exclusão. Para o gerenciamento das referências bibliográficas, utilizou-se o *Zotero*, que possibilita o armazenamento, a categorização e a exportação das citações conforme os estilos acadêmicos requeridos.

Além disso, uma planilha foi elaborada no *Google Sheets* para organizar de forma estruturada as informações extraídas dos artigos selecionados, incluindo: título, autores, ano, base de dados, objetivos, métodos, contribuições e classificação conforme os eixos definidos na taxonomia. Essa sistematização facilitou a análise comparativa entre os estudos e a identificação de padrões recorrentes.

As ferramentas citadas também contribuíram na aplicação dos critérios de exclusão e na elaboração das sínteses da pesquisa.

4.4 Leitura Exploratória

Após a filtragem inicial dos materiais, a etapa seguinte consistiu em uma leitura exploratória dos artigos selecionados, com o objetivo de proporcionar familiarização com os conteúdos, conceitos e abordagens relevantes nas áreas de 5G, IPv6 e segurança de redes. Essa leitura permitiu compreender as principais tendências, terminologias recorrentes, e estratégias empregadas pelos autores, além de refinar a delimitação do escopo analítico da pesquisa.

Durante essa fase, foram registradas anotações detalhadas a respeito de definições, dados relevantes, contribuições técnicas, análises e demais elementos considerados essenciais para o desenvolvimento do estudo. Essas anotações serviram não apenas para consolidar o entendimento teórico, mas também como base estruturante para as etapas seguintes da revisão sistemática.

A partir desse processo, foi possível identificar lacunas de pesquisa, convergências e divergências entre os estudos, bem como tópicos emergentes que merecem aprofundamento. Tais percepções orientaram a organização dos dados e a construção da taxonomia, garantindo que o trabalho se apoiasse em uma base sólida de conhecimento teórico e prático.

4.5 Organização dos Dados

Nesta etapa, foi realizada uma sistematização criteriosa das informações extraídas dos artigos selecionados, com o objetivo de construir uma base de dados abrangente e estruturada. Esse processo incluiu a elaboração de fichamentos detalhados, nos quais cada estudo foi documentado com base em critérios específicos, como tema abordado, autores, ano de publicação, objetivos e contribuições.

A categorização desses dados permitiu uma organização clara do material, facilitando consultas posteriores e apoiando diretamente as fases de análise comparativa e construção da taxonomia. Essa organização foi essencial para assegurar que o desenvolvimento da pesquisa ocorresse de forma coerente, metódica e alinhada aos objetivos definidos.

Além de sustentar o progresso da pesquisa, essa base organizada serviu como referência contínua para decisões sobre inclusão, relevância e ênfase dos conteúdos incorporados ao texto final, contribuindo para a consistência teórica e o rigor acadêmico do trabalho.

4.6 Análise Comparativa

Após a organização dos dados, foi realizada uma análise comparativa com o intuito de compreender as relações entre as informações coletadas e extrair conclusões relevantes sobre o impacto das tecnologias 5G e IPv6 na segurança de redes de comunicação. Essa etapa permitiu comparar diferentes perspectivas, identificar padrões recorrentes e destacar divergências entre os estudos analisados, proporcionando uma visão crítica e aprofundada dos temas abordados.

A análise foi conduzida de forma criteriosa, levando em consideração não apenas os pontos fortes, mas também as limitações das abordagens investigadas. Buscou-se, com isso, identificar tanto as soluções já propostas quanto as lacunas ainda existentes nas estratégias de segurança, evidenciando áreas que demandam maior atenção por parte da comunidade científica e tecnológica.

4.7 Elaboração da Taxonomia

A etapa de elaboração da taxonomia foi essencial para organizar e estruturar o conhecimento obtido nas fases anteriores da pesquisa. A taxonomia consistiu na classificação e ordenação de conceitos, ameaças, vulnerabilidades, tecnologias e soluções de segurança identificados ao longo do estudo, com o objetivo de construir uma estrutura lógica que facilitasse a compreensão das interações entre os diversos elementos analisados.

A construção teve início com a definição das categorias e subcategorias principais, resultantes da análise comparativa. Cada categoria foi associada a um conjunto de termos e conceitos específicos, representando aspectos distintos das tecnologias 5G, IPv6 e suas implicações para a segurança das redes. A estrutura resultante permitiu uma visualização sistematizada dos temas tratados, contribuindo para a identificação de áreas críticas que demandam aprofundamento e inovação.

4.8 Síntese das Informações

A última etapa da metodologia consistiu na síntese das informações, um processo essencial para consolidar o conhecimento obtido e apresentar, de forma coesa e estruturada, os principais resultados da pesquisa. Essa síntese envolveu a integração dos dados organizados e analisados ao longo de todo o estudo, com o objetivo de extrair conclusões claras e fundamentadas sobre as implicações das tecnologias 5G e IPv6 para a segurança das redes de comunicação.

A estrutura da síntese foi construída com base em diversos elementos: as categorias definidas na taxonomia, os resultados da análise comparativa, as boas práticas identificadas e as lacunas evidenciadas na literatura. Nessa etapa, buscou-se conectar os diferentes tópicos abordados, destacando como os recursos e limitações do 5G e do IPv6 se articulam com os desafios contemporâneos de segurança em redes.

Por fim, foram discutidos os desafios ainda não superados para a implementação segura dessas tecnologias, bem como possíveis direções para mitigar os riscos associados. Questões em aberto, como a adaptação de protocolos de segurança a ambientes altamente dinâmicos, a transição do IPv4 para o IPv6 e a necessidade de regulamentações específicas, também foram abordadas, apontando oportunidades concretas para pesquisas futuras e avanços na área.

5 RESULTADOS

Este capítulo apresenta e analisa os principais achados da revisão sistemática realizada sobre segurança em redes que integram IPv6 e 5G. Com base nos 29 artigos selecionados, buscou-se identificar padrões, tendências, lacunas e contribuições recorrentes na literatura recente.

Inicialmente, foi elaborada uma taxonomia funcional (ou descritiva) que organiza os trabalhos segundo três eixos principais: Tecnologia, Problemas de Segurança e Soluções. Essa estrutura permite uma visão abrangente dos componentes técnicos, desafios enfrentados e mecanismos de mitigação propostos nos estudos revisados.

Em seguida, é apresentada uma taxonomia analítica, construída a partir da correlação entre os eixos identificados. Essa abordagem relacional visa sintetizar as informações, cruzando tecnologias com ameaças associadas e respectivas soluções, além de revelar lacunas na literatura.

Por fim, os resultados são discutidos de forma crítica, destacando frequências e ausências significativas, bem como a maturidade e limitações das abordagens existentes. Essa análise tem o objetivo de apoiar futuras investigações na área, promovendo uma compreensão mais aprofundada sobre os rumos atuais da pesquisa em segurança para redes 5G e IPv6.

5.1 Taxonomia Descritiva

A fim de organizar e categorizar os estudos selecionados nesta revisão sistemática, foi desenvolvida uma taxonomia descritiva que representa os principais eixos temáticos abordados nos artigos. A estrutura está dividida em três blocos principais: Tecnologia, Problemas de Segurança e Soluções.

O eixo Tecnologia contempla elementos de infraestrutura e suporte utilizados nos trabalhos analisados. São incluídas tecnologias de acesso e aplicação como *5th Generation Standalone* (5G SA), *5th Generation Non-Standalone* (5G NSA), *Internet Protocol version 6* (IPv6), *Mobile Edge Computing* (MEC), *Internet of Things* (IoT) Integrado e *Network Slicing*. Complementando essas tecnologias, são abordadas também ferramentas e arquiteturas de suporte, como *Software-Defined Networking* (SDN), *Network Function Virtualization* (NFV), *Dual Stack Protocols*, e métodos de avaliação como Simulador Específico, Ambiente Real e Avaliação Teórica/Descritiva.

O eixo Problemas de Segurança está subdividido em três categorias: Ameaças

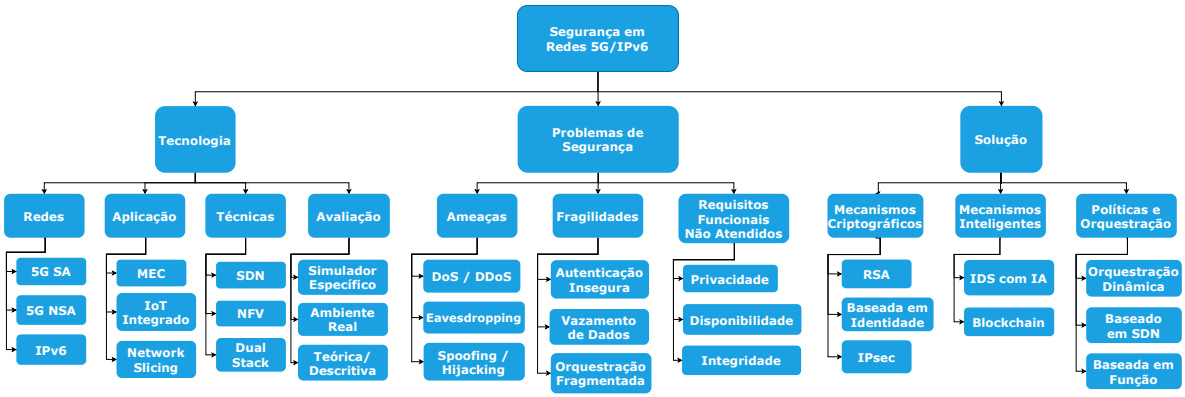
Diretas, Fragilidades Sistêmicas e Requisitos Funcionais Não Atendidos. Em Ameaças Diretas, destacam-se ataques como *Denial of Service* (DoS) e *Distributed Denial of Service* (DDoS), bem como técnicas como *Eavesdropping*, *Spoofing* e *Hijacking*. Em Fragilidades Sistêmicas, são abordados problemas como Autenticação Insegura, Vazamento de Dados e Orquestração Fragmentada. Por fim, os Requisitos Não Atendidos incluem questões relacionadas à Privacidade, Disponibilidade e Integridade.

O eixo Soluções compreende as estratégias técnicas e políticas adotadas para mitigar os problemas identificados. Em Mecanismos Inteligentes, estão presentes abordagens como *Intrusion Detection Systems* com Inteligência Artificial (IDS com IA) e *Blockchain*. Em Criptografia, destacam-se métodos como *Rivest-Shamir-Adleman* (RSA), Baseada em Identidade e Protocolo de Segurança IP (IPsec). Já no grupo de Políticas e Orquestração, são apresentadas abordagens como Orquestração Dinâmica, orquestração Baseada em SDN e Baseada em Função.

A estrutura proposta permite não apenas descrever os tópicos mais recorrentes na literatura, como também estabelecer relações entre os três eixos da taxonomia, evidenciando padrões e lacunas. Esses aspectos serão aprofundados na Seção 5.8, onde se discute criticamente a taxonomia descritiva e a taxonomia analítica, correlacionando Tecnologias, Ameaças e Soluções com base nos achados da revisão sistemática.

A Figura 9 apresenta visualmente essa taxonomia, servindo como guia para a subsequente revisão e comparação dos estudos.

Figura 9 – Taxonomia Proposta para Segurança em Redes 5G/IPv6.



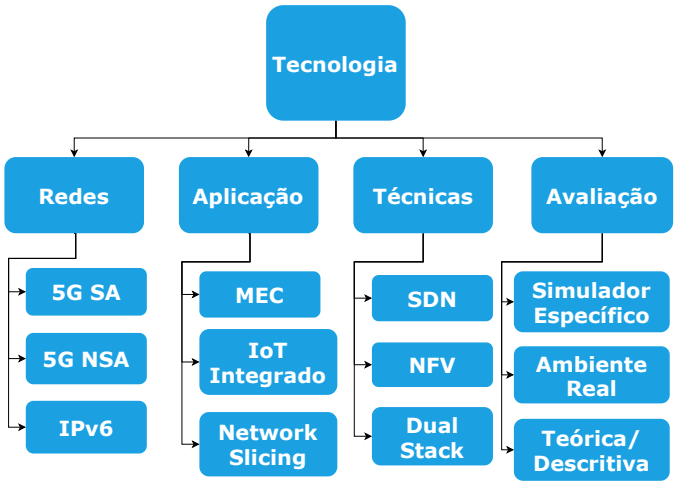
Fonte: Elaborado pelo Autor.

5.2 Tecnologia

As tecnologias analisadas compõem a base arquitetural e funcional das soluções propostas para segurança em redes 5G e IPv6. Elas abrangem protocolos, arquiteturas, mecanismos de virtualização e componentes de apoio como IoT, *slicing* e computação de borda.

A Figura 10 ilustra as categorias que compõem o eixo "Tecnologia", subdividido em quatro ramos: Redes, Aplicação, Técnicas e Avaliação. Cada uma dessas categorias será explorada nas subseções a seguir, destacando os elementos identificados na literatura revisada.

Figura 10 – Categorias que Compõem o Eixo Tecnologia.



Fonte: Elaborado pelo Autor.

A subseção a seguir aborda a categoria Redes, englobando os elementos nucleares relacionados ao 5G (SA e NSA) e IPv6.

5.2.1 Redes

A categoria Redes reúne as tecnologias centrais de conectividade presentes nas soluções para segurança em ambientes 5G com IPv6. Os artigos analisados abordam tanto os modos de operação do 5G (SA e NSA) quanto o uso do protocolo IPv6 e suas extensões, como o *Dual Stack*.

O modo SA adota um núcleo 5G nativo, enquanto o NSA utiliza o *core* LTE como base, o que afeta diretamente as estratégias de segurança adotadas (Tang *et al.*, 2022). Já o IPv6, ao eliminar o NAT e suportar nativamente IPsec, oferece uma infraestrutura mais transparente e segura para ambientes 5G, embora exija medidas específicas de proteção em sua configuração inicial e em mecanismos como SLAAC e DHCPv6 (Olimid; Nencioni, 2020; Saleem *et al.*,

2020).

Alguns trabalhos também destacam a operação simultânea de IPv4 e IPv6 em configurações *Dual Stack*, identificando que esse modelo amplia a superfície de ataque ao herdar vulnerabilidades de ambas as pilhas (Batewela *et al.*, 2025a). Por outro lado, essa abordagem tem sido necessária para garantir compatibilidade com infraestruturas legadas durante o processo de migração.

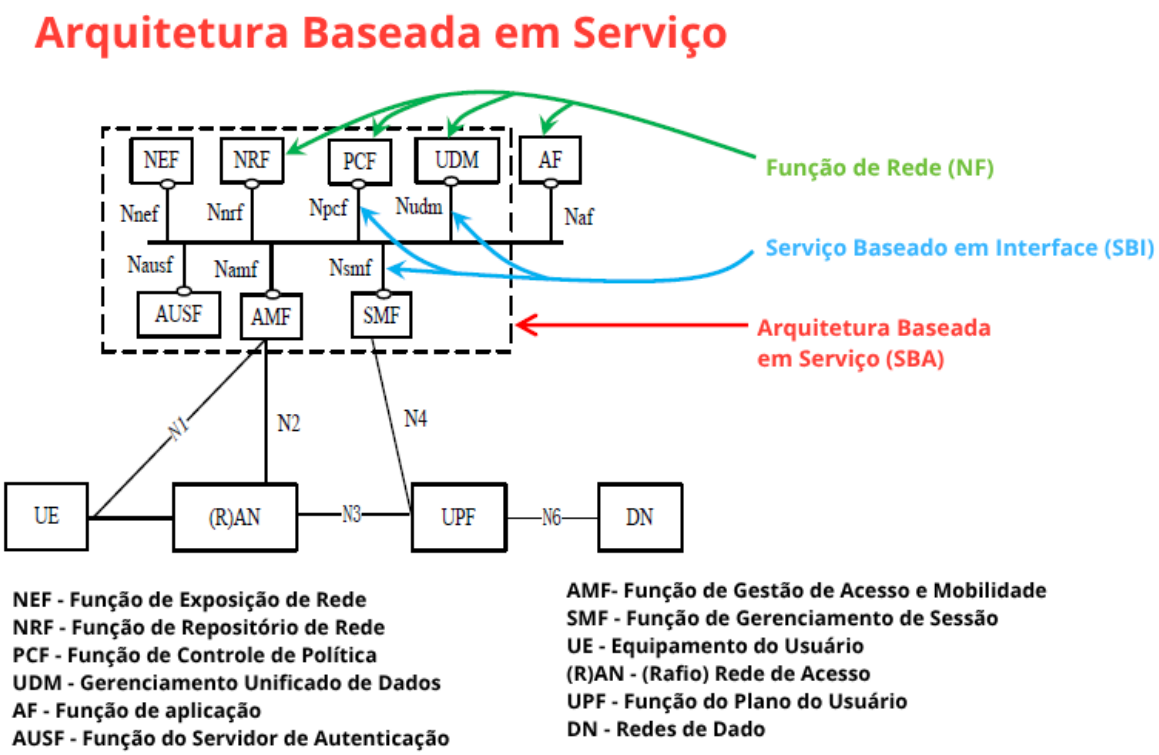
A seguir, cada tecnologia será detalhada individualmente.

5.2.1.1 5G SA

O 5G *Standalone* (SA) adota um núcleo de rede próprio, o 5G *Core* (5GC), estruturado sobre uma Arquitetura Orientada a Serviços (SBA), o que permite maior flexibilidade na utilização de técnicas como *network slicing*, *edge computing* e virtualização de funções (Dutta; Hammad, 2020; Tang *et al.*, 2022; Bjerre *et al.*, 2022). Essa arquitetura separa os planos de controle e de usuário e utiliza funções como *Access and Mobility Management Function* (AMF), *Session Management Function* (SMF), *User Plane Function* (UPF) e *Authentication Server Function* (AUSF), oferecendo ganhos operacionais, mas ampliando a superfície de ataque, especialmente via APIs abertas e interfaces expostas (Sullivan *et al.*, 2021; Bánáti, 2025). Vulnerabilidades em hipervisores, falhas de segmentação entre *slices* e riscos na orquestração dinâmica são recorrentes (Tang *et al.*, 2022). Como medidas mitigadoras, destacam-se o uso de Sistemas de Detecção de Intrusão (IDS), *firewalls* virtualizados e isolamento lógico (Arfaoui *et al.*, 2018; Gao *et al.*, 2024). O modelo SA é preferido em aplicações que exigem latência ultrabaixa e alta confiabilidade, como veículos autônomos e telemedicina, além de mitigar riscos herdados de redes legadas, ao contrário da arquitetura *Non-Standalone* (NSA) (Tang *et al.*, 2022; Bánáti, 2025; Oruma; Petrovic, 2023).

A Figura 11 representa a arquitetura SBA adotada nas redes 5G, em que funções como AMF, SMF, e AUSF interagem por meio de interfaces padronizadas (SBI). Essa organização modular facilita a orquestração e a flexibilidade, mas também introduz novos vetores de ataque, como dependência de autenticação entre funções, excesso de exposição via API e segmentação lógica passível de exploração. Diversos estudos analisados apontam fragilidades ou propõem soluções baseadas em reforço de segurança nesse modelo.

Figura 11 – Arquitetura Baseada em Serviço.



Fonte: Adaptado de Teleco (2024).

Embora o 5G SA represente um avanço arquitetural significativo, a maioria dos estudos revisados limita-se à descrição de vulnerabilidades hipotéticas ou análises conceituais das funções do 5GC, sem explorar em profundidade testes empíricos ou estudos de caso concretos. Isso dificulta a compreensão do impacto real das falhas na segmentação de *slices*, das dependências entre funções lógicas e da exposição via APIs abertas. Além disso, soluções frequentemente citadas, como IDS e *firewalls* virtualizados, muitas vezes são apresentadas de forma genérica, sem considerar a complexidade de sua integração em ambientes distribuídos com múltiplos *vendors*. Falta, portanto, uma abordagem crítica sobre os desafios operacionais da segurança em 5G SA, especialmente em aplicações de missão crítica como saúde e transporte autônomo. A literatura tende a subestimar os custos e a maturidade tecnológica necessários para alcançar o nível de segurança proposto.

5.2.1.2 5G NSA

O 5G *Non-Standalone* (NSA) utiliza o núcleo do 4G LTE, conhecido como *Evolved Packet Core* (EPC), em conjunto com o rádio de nova geração, oferecendo uma solução transitória para a adoção do 5G (Tang *et al.*, 2022; Ahmad *et al.*, 2019). Apesar de facilitar a implantação, essa arquitetura herda vulnerabilidades da geração anterior, principalmente pela dependência do *GPRS Tunneling Protocol* (GTP), alvo de críticas por não validar a localização do usuário e permitir ataques como *spoofing*, DoS e interceptações (Bjerre *et al.*, 2022; Tang *et al.*, 2022; Bánáti, 2025). Tais ataques podem manipular o plano de usuário, redirecionar tráfego e até causar fraudes financeiras (Tang *et al.*, 2022; Bánáti, 2025). Adicionalmente, o ataque do tipo *bidding down* força o uso de protocolos menos seguros, reduzindo a proteção da conexão (Bjerre *et al.*, 2022). A presença de autenticação fraca e interfaces abertas no EPC favorece *spoofing* de identidade e acesso indevido a sessões (Bánáti, 2025; Sullivan *et al.*, 2021). Como contramedidas, destacam-se o uso de *Security Edge Protection Proxy* (SEPP), autenticação mútua e criptografia ponta a ponta, embora sua aplicação plena ainda enfrente limitações no modelo NSA (Bjerre *et al.*, 2022; Tang *et al.*, 2022).

Apesar de amplamente adotada por operadoras em estágios iniciais de migração, a arquitetura NSA é frequentemente criticada por comprometer os avanços de segurança prometidos pelo 5G. O reaproveitamento do EPC do 4G, embora economicamente viável, perpetua fragilidades conhecidas, além de tornar a segmentação da rede e o isolamento entre *slices* menos eficazes. Alguns estudos apontam que a continuidade no uso do GTP, mesmo com mitigadores como o SEPP, representa um gargalo difícil de contornar sem transição completa para o modelo SA. Além disso, a literatura revisada raramente menciona casos concretos de mitigação bem-sucedida em ambientes NSA, o que levanta questionamentos sobre sua real efetividade em cenários críticos. Diante disso, observa-se uma tendência de recomendação do modelo SA como única alternativa viável para aplicações que exigem segurança avançada, como saúde digital, veículos autônomos e ambientes industriais.

5.2.1.3 IPv6

O *Internet Protocol version 6* (IPv6) substitui o IPv4 ao oferecer um espaço de endereçamento significativamente maior, suporte nativo ao IPsec e mecanismos avançados de atribuição, como SLAAC e DHCPv6, fundamentais para ambientes densos como redes 5G e

aplicações em IoT (Khan *et al.*, 2019b; Ahmed *et al.*, 2024; Olimid; Nencioni, 2020). Apesar de projetado com foco em segurança, o IPv6 introduz novos vetores de ataque, como *spoofing* no *Neighbor Discovery Protocol* (NDP), *DNS hijacking* e abusos de cabeçalhos estendidos (Olimid; Nencioni, 2020; Khan *et al.*, 2019b). A ausência de NAT e a comunicação direta entre dispositivos aumentam a transparência, mas demandam filtros e *firewalls* otimizados (Gao *et al.*, 2024; Arfaoui *et al.*, 2018). O IPsec fortalece a confidencialidade e integridade das comunicações, sendo especialmente relevante em aplicações sensíveis (Ahmed *et al.*, 2024). Contudo, a transição para o IPv6 ainda enfrenta desafios relacionados à compatibilidade, maturidade de ferramentas e riscos introduzidos por abordagens híbridas como *Dual Stack*, exigindo práticas de configuração seguras (Khan *et al.*, 2019b; Ahmed *et al.*, 2024).

Apesar de amplamente promovido como solução para os desafios de endereçamento e segurança em redes modernas, o IPv6 ainda carece de validações práticas mais abrangentes em ambientes críticos e distribuídos. Muitos estudos analisados assumem benefícios do IPv6 de forma teórica, sem avaliar seu impacto real em arquiteturas complexas ou sob ataques coordenados. A pouca atenção à implementação segura do NDP e à configuração de políticas IPsec revela uma lacuna entre o potencial do protocolo e sua aplicação efetiva. Além disso, a adoção de transições híbridas, como o Dual Stack, quando mal configuradas, podem introduzir inconsistências que anulam os ganhos esperados de segurança e desempenho. Portanto, embora o IPv6 seja recorrente na literatura, é necessário um olhar mais crítico sobre seus riscos operacionais e a efetividade das práticas recomendadas nos estudos.

5.2.2 Aplicação

As aplicações viabilizadas pelas redes 5G, especialmente quando combinadas ao IPv6, abrangem uma ampla gama de cenários que demandam elevada largura de banda, baixa latência e alta confiabilidade. Entre os domínios mais destacados nos artigos analisados estão: cidades inteligentes, saúde digital, automação industrial, transporte inteligente e IoT.

A integração entre 5G e IoT permite a conexão massiva de dispositivos com comunicação eficiente, mesmo em ambientes dinâmicos e com limitação energética. Essa característica facilita aplicações críticas como monitoramento ambiental, iluminação inteligente e controle de tráfego urbano (Ahmed *et al.*, 2024).

Na área da saúde, o uso de 5G em monitoramento remoto e cirurgia assistida tem sido amplamente explorado. A baixa latência e a elevada confiabilidade da rede são essenciais

para garantir a segurança e a eficácia dessas aplicações. Soluções como o *framework 5GSS*, voltado ao monitoramento inteligente de pacientes, ilustram esse potencial (Hu *et al.*, 2022).

Outro domínio em destaque é o das cidades inteligentes, onde o 5G habilita a operação coordenada de sensores distribuídos, veículos autônomos e sistemas de resposta a emergências. A combinação com computação em borda (MEC) melhora a eficiência energética e a capacidade de decisão em tempo real, reduzindo a sobrecarga da rede central (Oruma; Petrovic, 2023).

A segmentação lógica da rede através de *network slicing* permite customizar recursos para diferentes tipos de serviços, garantindo desempenho adequado a cada aplicação - de entretenimento em alta resolução até sistemas críticos de missão (Gao *et al.*, 2024).

Esses cenários reforçam o papel do 5G e do IPv6 como catalisadores da transformação digital em setores estratégicos, impondo também novas exigências de segurança, interoperabilidade e governança.

A classificação proposta nesta taxonomia organiza essa categoria em três subáreas: MEC, IoT Integrado e *Network Slicing*, cada uma com características, desafios e estratégias de segurança específicas. A seguir, cada uma dessas aplicações será explorada em maior profundidade.

5.2.2.1 Mobile Edge Computing

O *Mobile Edge Computing* (MEC) aproxima recursos computacionais da borda da rede, reduzindo latência e tráfego no núcleo, sendo essencial em redes 5G para aplicações sensíveis ao tempo, como cidades inteligentes, transporte autônomo e segurança pública (Oruma; Petrovic, 2023; Tang *et al.*, 2022). Ao permitir processamento local e descentralizado, o MEC melhora a escalabilidade e o consumo de recursos, tornando-se promissor também para aplicações em IoT e realidade aumentada. No entanto, sua arquitetura expande a superfície de ataque ao introduzir APIs abertas, expor instâncias virtuais e descentralizar o controle, facilitando ataques como *Man-in-the-Middle* (MitM), DoS e manipulação de máquinas virtuais (Ahmad *et al.*, 2018; Oruma; Petrovic, 2023; Saleem *et al.*, 2020). Para mitigar esses riscos, são propostas autenticação robusta, isolamento de instâncias e uso de criptografia local, além da integração com *Blockchain* e IDS distribuídos em cenários críticos (Gao *et al.*, 2024).

Apesar dos benefícios técnicos amplamente documentados, a adoção segura do MEC ainda é um desafio prático. A descentralização proposta, embora vantajosa para latência e

autonomia, dificulta o controle centralizado de políticas de segurança e dificulta a padronização de proteções entre diferentes zonas da rede. A literatura também sugere que o nível de maturidade das implementações de MEC varia significativamente entre operadoras e fornecedores, o que pode acarretar vulnerabilidades não previstas ou brechas de configuração. Além disso, soluções como *Blockchain* e IDS distribuídos, embora promissoras, apresentam elevado custo computacional e complexidade de integração em ambientes heterogêneos. Nesse cenário, é fundamental que a adoção do MEC seja acompanhada de diretrizes técnicas consolidadas e abordagens dinâmicas de mitigação, o que ainda está em estágio incipiente nos estudos revisados.

5.2.2.2 IoT Integrado

A integração da *Internet of Things* (IoT) com redes 5G viabiliza comunicações massivas e em tempo real entre dispositivos inteligentes, essenciais em aplicações como saúde digital, transporte autônomo e robótica social (Ahmed *et al.*, 2024; Khan *et al.*, 2019b; Hu *et al.*, 2022; Oruma; Petrovic, 2023). Recursos como conexões massivas (mMTC), baixa latência (URLLC) e uso nativo de IPv6 favorecem escalabilidade e identificação direta de dispositivos. No entanto, a expansão da IoT amplia os riscos de falsificação de dispositivos, exposição de dados e sobrecarga da rede. Como contramedidas, os estudos propõem segmentação de rede, protocolos de autenticação específicos e políticas baseadas em comportamento (Ahmed *et al.*, 2024; Khan *et al.*, 2019b). A segurança desse ecossistema depende da integração com arquiteturas como MEC, SDN e mecanismos de orquestração inteligente, embora persistam desafios relacionados à interoperabilidade, maturidade dos protocolos e governança distribuída.

Apesar do consenso sobre o potencial da IoT integrada ao 5G, os estudos analisados frequentemente limitam-se à proposição de contramedidas genéricas, sem validar sua aplicabilidade em ambientes reais de alta densidade. Por exemplo, estratégias como segmentação e autenticação comportamental são mencionadas, mas carecem de testes de escalabilidade sob restrições típicas de dispositivos IoT, como energia e processamento limitados. Além disso, a dependência de arquiteturas complementares como MEC e SDN torna a segurança da IoT fortemente acoplada a elementos externos cuja própria robustez ainda é debatida. Faltam estudos que tratem da coordenação efetiva entre múltiplos domínios administrativos, especialmente em redes públicas e ambientes urbanos inteligentes, onde a governança distribuída e a interoperabilidade entre fabricantes são críticas. Assim, embora as propostas ofereçam direções promissoras, muitas ainda se mantêm no nível conceitual, sem enfrentar os entraves operacionais de sua adoção

prática.

5.2.2.3 Network Slicing

O conceito de *network slicing* permite a criação de redes lógicas independentes sobre uma infraestrutura física compartilhada, utilizando SDN e Network Function Virtualization (NFV) para segmentar recursos de ponta-a-ponta (Olimid; Nencioni, 2020; Gao *et al.*, 2024). Cada *slice* atende a requisitos específicos de desempenho, como latência, banda e confiabilidade, sendo aplicada em contextos como saúde digital, veículos autônomos e entretenimento (Tang *et al.*, 2022; Singh *et al.*, 2024). No entanto, essa flexibilidade expande a superfície de ataque: falhas de isolamento entre *slices*, vulnerabilidades nas interfaces de orquestração e ameaças internas comprometem a confidencialidade e a disponibilidade dos serviços (Khan *et al.*, 2019b; Bjerre *et al.*, 2022; Gao *et al.*, 2024). Entre as contramedidas estão autenticação por *slice*, criptografia ponta-a-ponta, detecção de intrusos e segmentação baseada em atributos (Tang *et al.*, 2022; Khan *et al.*, 2019b). Abordagens recentes propõem o uso de IA para reforçar a segurança durante a operação dinâmica das *slices* (Gao *et al.*, 2024).

Apesar de ser amplamente considerada uma das inovações mais promissoras do 5G, a aplicação prática do *network slicing* enfrenta limitações importantes. A ausência de padronização robusta para mecanismos de isolamento entre *slices* aumenta a complexidade de garantir segurança em ambientes *multitenant*. Além disso, poucos estudos tratam da responsabilidade compartilhada entre provedores de infraestrutura e operadores de *slices*, o que levanta questões quanto à governança e resposta a incidentes. Soluções com IA ainda se encontram em estágio experimental e carecem de validação em ambientes reais, principalmente quanto à capacidade de detectar comportamentos anômalos em tempo real sem gerar falsos positivos. A eficácia das estratégias propostas depende fortemente da maturidade da orquestração e do alinhamento entre os domínios SDN, NFV e segurança, o que raramente é alcançado de forma integrada.

5.2.3 Técnicas

Esta subseção reúne técnicas fundamentais utilizadas para viabilizar arquiteturas 5G seguras, escaláveis e programáveis. Dentre elas, destacam-se a virtualização de funções, o controle programável da rede e a operação simultânea de múltiplos protocolos de rede. Tais abordagens são essenciais para atender aos requisitos de latência, isolamento, flexibilidade e compatibilidade que caracterizam ambientes heterogêneos e de alta demanda.

As tecnologias agrupadas aqui - SDN, NFV e *Dual Stack* - são amplamente empregadas nos cenários analisados. SDN permite a separação entre controle e encaminhamento, simplificando a aplicação de políticas de segurança e roteamento dinâmico (Khan *et al.*, 2019b). NFV, por sua vez, substitui funções tradicionais de hardware por instâncias virtualizadas, reduzindo custos operacionais e acelerando a resposta a ameaças (Tang *et al.*, 2022). Já o modelo *Dual Stack* garante interoperabilidade entre IPv4 e IPv6, sendo crucial durante a fase de transição e adaptação das redes legadas (Olimid; Nencioni, 2020).

As seções a seguir exploram essas técnicas individualmente, detalhando sua arquitetura, benefícios e vulnerabilidades no contexto da segurança em redes 5G.

5.2.3.1 SDN

O *Software Defined Networking* (SDN) é um pilar da arquitetura 5G, permitindo redes programáveis com separação entre os planos de controle e dados. A centralização do controle via controlador SDN viabiliza orquestração dinâmica de serviços, automação de políticas e gerenciamento de *slices* (Olimid; Nencioni, 2020; Khan *et al.*, 2019b; Gao *et al.*, 2024). Essa flexibilidade permite reconfiguração em tempo real de tráfego, controle granular e provisionamento ágil de funções virtualizadas, especialmente quando combinado ao NFV (Tang *et al.*, 2022; Singh *et al.*, 2024). No entanto, a centralização representa um ponto único de falha e vetor para ataques DoS, além de riscos em interfaces *northbound* e *southbound* mal protegidas (Sullivan *et al.*, 2021; Gao *et al.*, 2024). Como contramedidas, destacam-se autenticação mútua, isolamento de instâncias críticas, uso de *Trusted Execution Environments* (TEE) e monitoramento com detecção de anomalias baseada em Aprendizado de Máquina (ML) (Khan *et al.*, 2019b; Suomalainen *et al.*, 2020).

Apesar da recorrência de propostas baseadas em SDN na literatura, observa-se uma carência de estudos que validem suas soluções em ambientes heterogêneos ou em escala real. A maioria dos trabalhos limita-se a simulações ou arquiteturas idealizadas, sem considerar os desafios operacionais de implantar controladores redundantes, sincronizados e tolerantes a falhas em redes 5G distribuídas. Além disso, os riscos associados à centralização do controle são frequentemente subestimados: a literatura propõe contramedidas como TEE ou ML, mas não discute suas limitações quanto ao desempenho, custo de implementação e compatibilidade com equipamentos de múltiplos fornecedores. Essa lacuna reforça a necessidade de mais estudos práticos e padronizados que testem a resiliência da arquitetura SDN sob cenários realistas de

mobilidade, latência crítica e ataques coordenados.

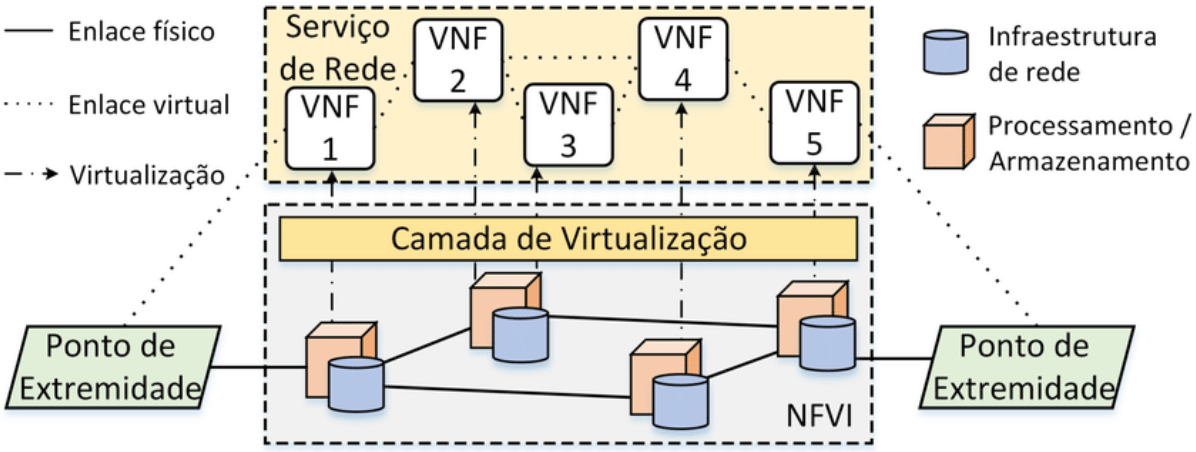
5.2.3.2 NFV

A *Network Function Virtualization* (NFV) permite a execução de funções de rede, como *firewalls* e roteadores, em ambientes virtualizados sobre infraestrutura genérica, promovendo flexibilidade, escalabilidade e redução de custos operacionais em redes 5G (Dutta; Hammad, 2020; Gao *et al.*, 2024). Integrada ao SDN, a NFV viabiliza *slicing*, computação em borda e controle dinâmico de políticas (Khan *et al.*, 2019b; Singh *et al.*, 2024). No entanto, a abstração introduzida por APIs abertas e o uso de ambientes *multitenant* ampliam a superfície de ataque, expondo vulnerabilidades em hipervisores e canais de comunicação entre *Virtual Network Functions* (VNFs) (Tang *et al.*, 2022; Sullivan *et al.*, 2021). Os principais riscos envolvem *hijacking* de funções, interceptação de tráfego interno e exaustão de recursos. Como contramedidas, são recomendados o uso de TEE, autenticação mútua, monitoramento contínuo e validação de imagens das VNFs (Bánáti, 2025; Arfaoui *et al.*, 2018). Em aplicações críticas como IoT massiva, automação industrial e telemedicina, a adoção segura da NFV é essencial para garantir confiabilidade e desempenho em cenários distribuídos (Oruma; Petrovic, 2023; Hu *et al.*, 2022).

Apesar das promessas de flexibilidade e redução de custos associadas à NFV, poucos trabalhos discutem de forma aprofundada os entraves operacionais em sua adoção prática. Muitos estudos propõem soluções idealizadas para ambientes virtualizados, mas negligenciam aspectos como o overhead introduzido pela virtualização, a interoperabilidade entre VNFs de diferentes fornecedores e os riscos de isolamento ineficaz entre inquilinos em ambientes multitenant. Além disso, embora seja recorrente a sugestão de autenticação mútua e uso de TEE como contramedidas, raramente se avaliam os impactos de desempenho e escalabilidade dessas abordagens em redes densas e dinâmicas. Essa ausência de validações empíricas indica uma lacuna na literatura quanto à viabilidade da NFV em ambientes críticos como telemedicina e IoT massiva, nos quais a latência e a confiabilidade não podem ser comprometidas.

A Figura 12 ilustra o conceito central da virtualização de funções de rede (NFV), na qual os serviços de rede são compostos por VNFs executadas sobre uma infraestrutura física comum. Essa abordagem é fundamental para a flexibilidade, escalabilidade e automação exigidas pelas arquiteturas modernas do 5G, e está fortemente associada à adoção de soluções dinâmicas de segurança baseadas em software.

Figura 12 – Infraestrutura da Virtualização de Funções de Rede.



Fonte: Adaptado de Teleco (2024).

5.2.3.3 Dual Stack

A abordagem *Dual Stack*, que permite a operação simultânea dos protocolos IPv4 e IPv6, é amplamente adotada em redes 5G como estratégia de transição, garantindo compatibilidade com sistemas legados e habilitando funcionalidades avançadas do IPv6, como o IPsec e autoconfiguração (Olimid; Nencioni, 2020; Khan *et al.*, 2019b). Apesar de sua praticidade, a coexistência de pilhas distintas aumenta a complexidade da rede e a superfície de ataque. Os principais riscos envolvem *spoofing* de pacotes IPv6, manipulação maliciosa de autoconfiguração e inconsistências de roteamento (Tang *et al.*, 2022; Gao *et al.*, 2024). Como medidas de mitigação, os estudos recomendam filtros de tráfego específicos para ambas as pilhas, desativação de túneis automáticos e uso do *Secure Neighbor Discovery* (SEND) para reforço da integridade das comunicações (Khan *et al.*, 2019b; Gao *et al.*, 2024; Oruma; Petrovic, 2023). Embora essencial no estágio atual de evolução das redes, a implementação segura do *Dual Stack* exige políticas de configuração e monitoramento contínuo.

Apesar de consolidada como solução de transição, a abordagem *Dual Stack* é criticada por perpetuar a dependência do IPv4 e dificultar o avanço pleno para o IPv6. A duplicidade de protocolos introduz desafios operacionais que nem sempre são devidamente tratados, especialmente em redes de grande escala, como operadoras e provedores de conteúdo. Além disso, a ausência de suporte nativo a IPv6 em muitos dispositivos legados e sistemas industriais obriga a manutenção da pilha dupla por períodos indefinidos, o que implica maior esforço de segurança e gestão. A literatura revisada pouco discute o impacto de ataques combinados explorando vulnerabilidades simultâneas nas duas pilhas, um ponto relevante considerando o

contexto 5G/IoT. A adoção de mecanismos como SEND e filtros específicos é recomendada, mas raramente implementada de forma padronizada e consistente, o que evidencia a necessidade de diretrizes mais claras e auditorias contínuas para redes *Dual Stack*.

5.2.4 Avaliação

Esta subseção trata dos métodos utilizados para validar, testar ou explorar soluções de segurança e comunicação em redes que integram 5G e IPv6. A forma como a avaliação é conduzida influencia diretamente a confiabilidade dos resultados apresentados nos estudos, impactando sua aplicabilidade prática.

Os artigos analisados foram classificados em três categorias distintas: Simulador Específico, para estudos que utilizam plataformas como NS-3; Ambiente Real, para testes implementados em protótipos físicos ou bancos de ensaio; e Teórica/Descritiva, quando a avaliação é baseada em análise conceitual, comparação de arquitetura ou levantamento bibliográfico.

A seguir, cada uma dessas abordagens será detalhada, destacando seus objetivos, limitações e relevância no contexto de redes 5G seguras e baseadas em IPv6.

5.2.4.1 Simulador Específico

A simulação é amplamente utilizada na avaliação de soluções de segurança em redes 5G com IPv6, por permitir testes controlados de ataques e defesas com baixo custo e sem riscos operacionais. Ferramentas como NS-3 e OMNeT++ são recorrentes nos estudos, permitindo simulações com *slicing*, mobilidade e detecção de ataques como *spoofing* e DoS (Tang *et al.*, 2022; Bánáti, 2025; Khan *et al.*, 2019b). O NS-3 se destaca por testar métricas de latência e resposta sob diferentes políticas de segurança, enquanto o OMNeT++ viabiliza testes com orquestração MEC e algoritmos baseados em ML (Gao *et al.*, 2024). Alguns trabalhos ainda utilizam simuladores próprios para explorar tópicos específicos, como roteamento seguro e desempenho criptográfico em topologias 5G (Suomalainen *et al.*, 2020). As principais limitações relatadas incluem a ausência de modelos realistas de canal, pouca integração com dispositivos físicos e restrições na modelagem de interferência (Olimid; Nencioni, 2020; Arfaoui *et al.*, 2018). Para maior confiabilidade, recomenda-se complementar as simulações com experimentação física ou análise teórica detalhada.

Apesar de serem amplamente empregadas, as simulações carecem de padronização em relação aos cenários utilizados, o que dificulta a reprodutibilidade e comparação entre os

estudos. A ausência de parâmetros uniformes, como topologias, cargas de tráfego e configurações de ataque, compromete a avaliação objetiva da eficácia das soluções propostas. Outro ponto crítico é a escassez de estudos que validem seus resultados em ambiente híbrido (simulação + testes físicos), o que levanta dúvidas sobre sua aplicabilidade prática em redes 5G reais. Poucos simuladores oferecem suporte nativo à pilha IPv6 completa, especialmente com extensões de segurança como IPsec ou SEND, o que limita a fidelidade dos testes. Esses fatores indicam a necessidade de desenvolvimento de bibliotecas especializadas e de uma metodologia unificada para testes de segurança em simulações voltadas à arquitetura 5G/IPv6.

5.2.4.2 Ambiente Real

A avaliação de soluções de segurança em ambientes reais é fundamental para validar seu comportamento sob tráfego genuíno e dispositivos comerciais, permitindo observar a eficácia frente a ataques como DoS, *spoofing* e falhas de autenticação. Estudos em ambientes reais no 5G *Core* (5GC) demonstraram vulnerabilidades em APIs *RESTful* em tempo de execução (Tang *et al.*, 2022), enquanto projetos como *5G-MiEdge* e *5G Champion* exploraram a resiliência de soluções em cenários industriais e urbanos (Khan *et al.*, 2019b; Bánáti, 2025). Outros trabalhos utilizaram redes privadas e dispositivos reais para testar *firewalls* virtualizados, segmentação por atributos e controle adaptativo de acesso, com destaque para aplicações em cidades inteligentes e saúde digital (Hu *et al.*, 2022; Oruma; Petrovic, 2023; Ahmed *et al.*, 2024). A presença de ambientes *multitenant* e a heterogeneidade de dispositivos demandam integração com ferramentas de monitoramento, *honeypots* e orquestradores com resposta em tempo real (Dutta; Hammad, 2020; Khan *et al.*, 2019b; Arfaoui *et al.*, 2018). Quando a experimentação prática é inviável, os estudos recorrem à modelagem conceitual e análises teóricas, como discutido na próxima seção.

Apesar de fornecerem resultados mais próximos da realidade, os testes em ambiente real ainda são escassos na literatura, principalmente devido a barreiras logísticas, custos operacionais e restrições de segurança. A maioria dos estudos revisados limita-se a protótipos com poucos nós e aplicações específicas, o que dificulta a generalização dos resultados. Poucos artigos exploram redes 5G públicas ou infraestruturas em larga escala, o que limita a compreensão do impacto real de soluções de segurança sob múltiplas condições de carga, mobilidade e interferência. Há também uma lacuna quanto à integração de métricas quantitativas padronizadas nesses testes, o que dificulta a comparação com simulações e análises teóricas. Esses fatores reforçam a importância de iniciativas que promovam *testbeds* abertos, reprodutíveis

e com suporte ao ecossistema IPv6 e tecnologias emergentes como MEC, SDN e NFV.

5.2.4.3 Teórica/Descritiva

Avaliações teóricas ou descritivas são comuns em estudos exploratórios e revisões sistemáticas sobre segurança em redes 5G/IPv6. Essa abordagem, sem validação prática direta, é usada para mapear o estado da arte, estruturar taxonomias e discutir requisitos de segurança relacionados a tecnologias como SDN, NFV, MEC, *Blockchain* e criptografia (Dutta; Hammad, 2020; Bjerre *et al.*, 2022; Khan *et al.*, 2019b; Tang *et al.*, 2022; Al-Shareeda; Manickam, 2022; Gao *et al.*, 2024). Os artigos abordam desafios como novos vetores introduzidos pela SBA, falhas em APIs *RESTful* e problemas de isolamento em ambientes *multitenant* (Khan *et al.*, 2019b; Tang *et al.*, 2022; Bánáti, 2025). Também são frequentes comparações conceituais entre estratégias de mitigação, avaliando atributos como escalabilidade, *overhead* e compatibilidade com padrões (Hu *et al.*, 2022; Sullivan *et al.*, 2021; Gupta *et al.*, 2018; Singh *et al.*, 2024). Por fim, muitos trabalhos propõem arquiteturas seguras baseadas em orquestração inteligente e autenticação por identidade ou comportamento, contribuindo para a consolidação teórica do campo e orientando estudos experimentais futuros (Bánáti, 2025; Al-Shareeda; Manickam, 2022; Batewela *et al.*, 2025a).

Apesar de seu valor estrutural, a predominância de análises puramente conceituais na literatura limita a comprovação empírica das soluções propostas. Muitos trabalhos carecem de métricas quantitativas, dados reais de desempenho ou validações comparativas que evidenciem a eficácia dos mecanismos frente a ataques reais. Essa lacuna prejudica a replicabilidade e a aplicabilidade prática dos resultados, especialmente em contextos operacionais mais complexos. Além disso, a ausência de padronização metodológica entre os estudos dificulta a comparação entre abordagens distintas. Torna-se, portanto, necessário o avanço para avaliações híbridas que aliem a profundidade teórica à experimentação controlada ou em *testbeds* reais, promovendo maior robustez e aplicabilidade das contribuições.

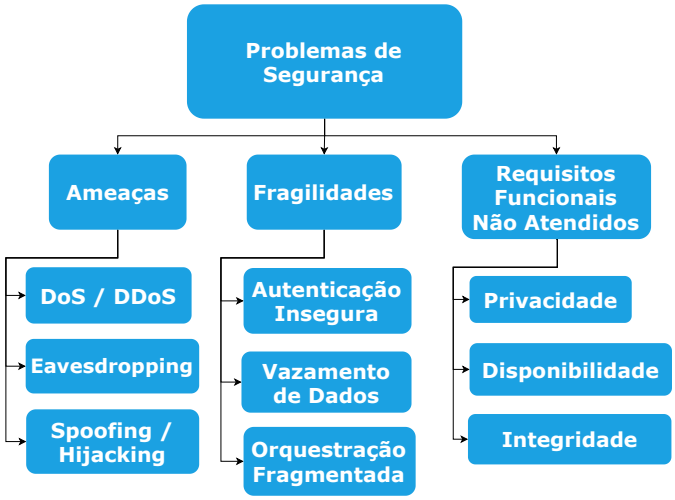
5.3 Problemas de Segurança

A consolidação das redes 5G combinadas com o protocolo IPv6 não representa apenas avanços em desempenho, flexibilidade e escalabilidade, mas também a ampliação significativa da superfície de ataque. Esse cenário decorre de fatores como a adoção de arquiteturas

orientadas a serviços, o uso intensivo de virtualização de funções de rede e a fragmentação lógica da infraestrutura por meio do *slicing*. Como evidenciado nos estudos analisados, tais inovações, embora essenciais para a evolução das redes móveis, introduzem vulnerabilidades técnicas e operacionais que demandam reavaliações criteriosas dos mecanismos de proteção tradicionais.

A Figura 13 ilustra os principais desafios de segurança foram organizados em três categorias funcionais que serão detalhados na subseções a seguir: (i) Ameaças Diretas, que representam os ataques mais frequentes observados nos sistemas; (ii) Fragilidades Sistêmicas, decorrentes de deficiências na arquitetura ou na implementação de boas práticas; e (iii) Requisitos Funcionais Não Atendidos, que evidenciam falhas em assegurar os princípios fundamentais de segurança, como privacidade, disponibilidade e integridade.

Figura 13 – Categorias que Compõem o Eixo Problemas de Segurança.



Fonte: Elaborado pelo Autor.

5.3.1 Ameaças

As redes 5G, ao incorporarem tecnologias como *slicing*, virtualização, *edge computing* e arquitetura orientada a serviços, ampliam significativamente a superfície de ataque em comparação às gerações anteriores. A comunicação distribuída entre funções de rede virtualizadas, o uso de APIs abertas e a integração com dispositivos heterogêneos – incluindo elementos do IoT – contribuem para um cenário de ameaças mais dinâmico, complexo e fragmentado.

Nos artigos analisados, é recorrente a identificação de ataques clássicos adaptados ao novo contexto, além da emergência de vetores inéditos, facilitados pela natureza programável e modular do 5G. A ausência de isolamento completo entre *slices*, a utilização de canais de

sinalização inseguros e a exposição de funções centrais, como o AMF e o UPF, elevam o risco de comprometimento de grandes porções da infraestrutura em eventos de ataque bem sucedido (Sullivan *et al.*, 2021; Tang *et al.*, 2022; Bánáti, 2025).

Entre as ameaças mais recorrentes estão os ataques de negação de serviço (DoS/DDoS), interceptação de tráfego (*eavesdropping*) e ataques de *spoofing* e *hijacking*, que afetam tanto o plano de controle quanto o de usuário. Tais ameaças são citadas em diversos contextos, desde redes core até interfaces de acesso em ambientes críticos, como saúde, transporte e cidades inteligentes (Bjerre *et al.*, 2022; Khan *et al.*, 2019b; Ahmad *et al.*, 2018; Gao *et al.*, 2024; Ahmed *et al.*, 2024).

Além disso, foram observadas variações mais sofisticadas desses ataques, como DoS por esgotamento de recursos em funções virtualizadas, sequestro de *slices* para redirecionamento malicioso de tráfego, e técnicas avançadas de falsificação de identidade e sessão (Al-Shareeda; Manickam, 2022; Ahmad *et al.*, 2019; Batewela *et al.*, 2025a). Essas ameaças frequentemente exploram falhas em autenticação, ausência de criptografia ponta-a-ponta e interfaces de gerenciamento mal protegidas.

A seguir, são detalhadas as principais ameaças identificadas: DoS/DDoS, *Eavesdropping* e *Spoofing/Hijacking*, suas causas, impactos e abordagens sugeridas para mitigação.

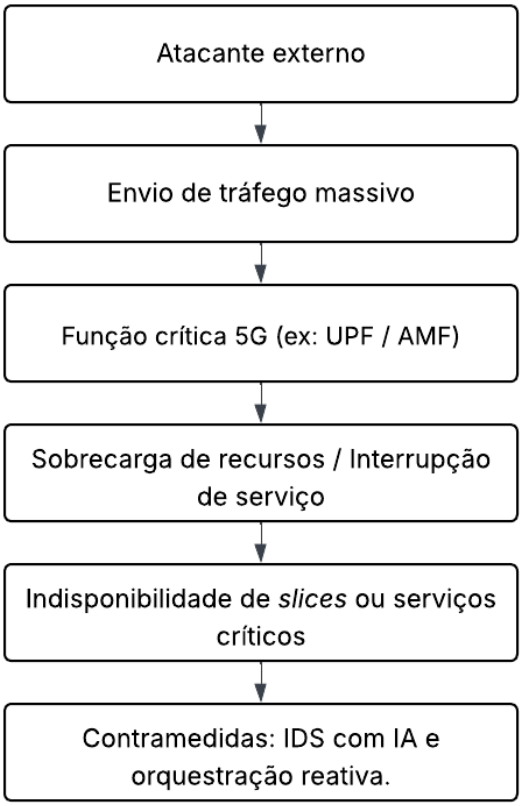
5.3.1.1 DoS/DDoS

Ataques de negação de serviço (DoS) e negação de serviço distribuída (DDoS) estão entre as ameaças mais críticas em redes 5G, ampliadas pela introdução do *network slicing*, da SBA e da NFV (Khan *et al.*, 2019b; Gao *et al.*, 2024). Funções de controle como AMF e SMF são alvos frequentes por sobrecarga de sinalização, enquanto a *User Plane Function* (UPF) pode ser explorada por saturação via GTP-U (Tang *et al.*, 2022; Hamroun *et al.*, 2025; Singh *et al.*, 2024). Dispositivos IoT inseguros alimentam *botnets* utilizadas em ataques contra *slices* críticos como saúde e transporte autônomo (Hu *et al.*, 2022; Oruma; Petrovic, 2023). Além dos ataques volumétricos, destacam-se técnicas furtivas como *slow-rate attacks* e degradação intencional da Qualidade de Serviço (QoS) por manipulação de *handovers* (Khan *et al.*, 2019b; Alwis *et al.*, 2024). Contramedidas incluem detecção por ML, uso de *honeypots*, orquestração resiliente e segmentação contextual, embora apresentem limitações de escalabilidade e custo computacional (Hamroun *et al.*, 2025; Gao *et al.*, 2024; Salahdine *et al.*, 2023). O enfrentamento eficaz exige arquiteturas autoadaptativas, com monitoramento em tempo real e isolamento dinâmico entre

funções e serviços.

A Figura 14 ilustra de forma simplificada a progressão típica de um ataque DoS/DDoS e suas contramedidas.

Figura 14 – Fluxo de Ataque Por Negação de Serviço (DoS/DDoS) e Contramedidas Associadas.



Fonte: Elaborado pelo Autor.

Esse tipo de ataque é especialmente preocupante em arquiteturas *multitenant*, onde a falha de um *slice* pode afetar outros que compartilham a mesma infraestrutura. Como contramedidas, os estudos analisados sugerem a adoção de sistemas de detecção de intrusão baseados em IA (IDS com IA), orquestração reativa e balanceamento de carga adaptativo. Essas estratégias permitem identificar padrões anômalos, redistribuir o tráfego e restaurar a resiliência da rede sem intervenção manual.

Apesar da ampla cobertura do tema na literatura, muitos trabalhos sobre DoS/DDoS ainda se concentram em descrições de ataques ou arquiteturas de defesa idealizadas, sem validação prática ou avaliação de desempenho em ambientes reais. A complexidade crescente dos ataques distribuídos, sobretudo quando originados por *botnets* IoT, exige soluções que vão além de modelos teóricos e simulações simplificadas. Além disso, algumas propostas

negligenciam o impacto de ataques furtivos e de baixo volume, que exploram o comportamento normalizado da rede para permanecerem indetectáveis. A ausência de *benchmarks* padronizados e métricas comparativas limita a avaliação da efetividade das contramedidas. Assim, observa-se a necessidade de estudos que combinem avaliação empírica com análise de custo-benefício, especialmente em contextos críticos como saúde e transporte autônomo, onde a indisponibilidade pode ter consequências graves.

5.3.1.2 Eavesdropping

Ataques de escuta (*eavesdropping*) exploram a natureza aberta dos canais sem fio no 5G para interceptar dados e sinais de controle, sendo agravados pela densidade de dispositivos, presença de antenas distribuídas e integração com redes legadas (Sullivan *et al.*, 2021; Hamroun *et al.*, 2025). Mensagens como *paging* continuam desprotegidas, permitindo inferência de localização, enquanto técnicas como *International Mobile Subscriber Identity catching* (IMSI *catching*) ainda são viáveis em situações de *fallback* para redes 4G/2G (Tang *et al.*, 2022; Bánáti, 2025). Dispositivos também podem ser induzidos a se conectar a estações base falsas, especialmente durante eventos de *handover* (Bánáti, 2025). Contramedidas incluem criptografia ponta-a-ponta, técnicas de segurança na camada física como *beamforming*, geração de ruído, *Physical Layer Security* (PLS) e uso de MIMO massivo com pré codificação seletiva (Sullivan *et al.*, 2021; Ahmad *et al.*, 2019). Ataques passivos também atuam como preparação para ameaças mais invasivas, como *spoofing* e *hijacking* (Tang *et al.*, 2022)

Embora a literatura identifique com precisão os vetores de escuta em redes 5G, há uma lacuna entre o reconhecimento dos riscos e a efetiva avaliação da eficácia das contramedidas em ambientes reais. Muitas propostas de defesa baseiam-se em pressupostos ideais, como a disponibilidade universal de MIMO massivo ou o uso irrestrito de criptografia ponta-a-ponta, o que nem sempre se reflete em cenários práticos, especialmente em contextos IoT ou de transição tecnológica (*fallback*). A persistência de mensagens de *paging* não criptografadas e a viabilidade de ataques IMSI *catching* mesmo em 2025 evidenciam falhas na aplicação de políticas de proteção básica. Ademais, os ataques passivos são frequentemente subestimados por não causarem impacto imediato, embora sirvam como base para ações mais danosas. Estudos futuros devem investigar a viabilidade e o custo das técnicas de segurança física em implementações reais, bem como propor diretrizes para mitigação progressiva durante a coexistência de múltiplas gerações de rede.

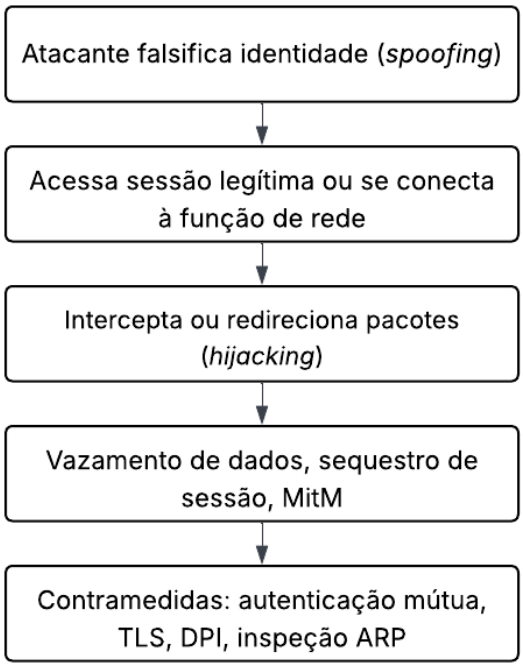
5.3.1.3 Spoofing/Hijacking

Ataques de *spoofing* e *hijacking* representam ameaças críticas à integridade, confidencialidade e disponibilidade em redes 5G. O *spoofing* envolve falsificação de identidade de dispositivos, explorando falhas em protocolos como *Address Resolution Protocol* (ARP), GTP e *Packet Data Convergence Protoco* (PDCP), permitindo redirecionamento de tráfego e manipulação de sessões (Bjerre *et al.*, 2022; Bánáti, 2025; Ahmad *et al.*, 2019). Em ambientes com SDN e APIs abertas, a ausência de autenticação forte viabiliza ataques *Man-in-the-Middle* (Bánáti, 2025). Já o *hijacking* compromete sessões legítimas por meio de falhas em protocolos como Protocolo de Iniciação de Sessão (SIP), *Diameter* e HTTP/2, especialmente em redes SBA (Bánáti, 2025; Hamroun *et al.*, 2025). A coexistência com redes legadas 4G agrava essas vulnerabilidades. Contramedidas incluem autenticação mútua via TLS, inspeção ARP reforçada com *Dynamic ARP Inspection* (DAI), correlação de eventos por *Security Information and Event Management* (SIEM) e isolamento de instâncias SDN (Bjerre *et al.*, 2022; Bánáti, 2025). Estudos recentes propõem autenticação de caminhos *Segment Routing over IPv6* (SRv6) para prevenir redirecionamento indevido em redes SD-WAN 5G, com validação criptográfica e compatibilidade com dispositivos de baixa capacidade computacional (Filsfils; Camarillo, 2020).

Apesar da diversidade de contramedidas propostas contra *spoofing* e *hijacking*, a literatura revela uma lacuna entre as soluções teóricas e sua aplicação prática em ambientes heterogêneos e legados. Muitos mecanismos, como inspeção ARP reforçada e autenticação via TLS, pressupõem configurações padronizadas e capacidades computacionais compatíveis, o que nem sempre se verifica em dispositivos IoT ou redes com múltiplos fornecedores. Além disso, o uso crescente de SDN e APIs abertas amplia a superfície de ataque e exige políticas de controle granular, que ainda carecem de padronização em nível internacional. O ataque por *hijacking* de sessões HTTP/2 ou SIP evidencia a urgência de revisões nos protocolos de controle de sessões nas redes SBA. A proposta de autenticação via SRv6 surge como alternativa viável, mas sua adoção depende de compatibilidade ampla com infraestrutura e dispositivos de baixo desempenho. A mitigação eficaz desses ataques demanda abordagens coordenadas entre os níveis físico, lógico e de aplicação, além de monitoramento contínuo em tempo real.

A Figura 15 representa os estágios envolvidos em ataques de *spoofing* e *hijacking*, incluindo os vetores e as principais formas de mitigação.

Figura 15 – Fluxo de Ataque por Falsificação de Identidade (*Spoofing*) e Sequestro de Sessão (*Hijacking*).



Fonte: Elaborado pelo Autor.

A Figura 15 ilustra as principais etapas envolvidas em um ataque combinado de *spoofing* e *hijacking* em redes 5G. O atacante inicia falsificando sua identidade, por exemplo, via *spoofing* de ARP ou IMSI, com o intuito de se passar por um nó ou usuário legítimo. Isso lhe permite acessar sessões ou se conectar a funções de rede sem a devida autenticação.

Uma vez estabelecido esse acesso indevido, o invasor pode interceptar ou redirecionar pacotes legítimos, configurando um ataque do tipo *hijacking*. As consequências incluem vazamento de dados, sequestro de sessões, perda de integridade e ataques *Man-in-the-Middle*. Para mitigar esses riscos, as abordagens identificadas na literatura propõem o uso de autenticação mútua entre funções, criptografia com TLS, Inspeção de Pacotes (DPI) e protocolos reforçados de controle de ARP como S-ARP e DAI.

5.3.2 Fragilidades

As redes 5G introduzem uma arquitetura distribuída e orientada a serviços, composta por múltiplas interfaces expostas, funções virtualizadas e gerenciamento por orquestração. Embora tais características ofereçam ganhos substanciais de desempenho e flexibilidade, elas também criam pontos críticos de vulnerabilidade interna, que podem ser explorados mesmo na

ausência de ataques externos diretos.

Neste contexto, fragilidades são entendidas como debilidades estruturais ou lacunas nos mecanismos de segurança, autenticação ou controle, que podem comprometer a confiabilidade da rede e facilitar a ação de ameaças externas. Diferente de ataques propriamente ditos, essas fragilidades frequentemente se originam de decisões de projeto, configurações inadequadas ou limitações em protocolos herdados.

Nos artigos analisados, três fragilidades destacam-se de forma recorrente: a presença de mecanismos de autenticação insegura, falhas que levam ao vazamento de dados entre domínios ou *slices*, e a ausência de uma orquestração unificada e coerente entre as funções de segurança distribuídas da rede. Essas debilidades não apenas expõem funções críticas a comprometimento, mas também dificultam a implementação de políticas de mitigação eficientes e coordenadas.

As subseções a seguir detalham essas três categorias de fragilidade, com base nos artigos analisados, destacando suas causas, impactos e propostas de mitigação identificadas na literatura especializada.

5.3.2.1 Autenticação Insegura

Apesar da introdução dos protocolos 5G-AKA e EAP-AKA', a autenticação em redes 5G ainda apresenta vulnerabilidades críticas, como exposição do identificador permanente do assinante (SUPI), ataques *Man-in-the-Middle* e comprometimento de chaves em sessões de pré-autenticação (Sullivan *et al.*, 2021; Jover; Marojevic, 2019). O envio de mensagens em texto claro, especialmente em sessões de emergência, permite a exploração de funções como *AttachReject* e *TAU-Reject*, agravado pela ausência de um modelo global de gerenciamento de chaves públicas (Jover; Marojevic, 2019). O 5G-AKA sofre de falhas estruturais, enquanto o EAP-AKA', embora mais robusto, apresenta elevado *overhead*, o que pode levar à adoção de alternativas menos seguras (Sullivan *et al.*, 2021). Durante eventos de *handover*, a complexidade do processo e a falta de sincronização expõem a rede a ataques como *false base station* e uso indevido de *Password Authentication Protocol* (PAP) (Gupta *et al.*, 2018). Propostas como autenticação com IA, delegação dinâmica de credenciais e uso de *honeypots* têm sido sugeridas, mas ainda carecem de ampla padronização.

Apesar da diversidade de propostas para mitigar falhas de autenticação, a maioria dos artigos analisados concentra-se em soluções conceituais ou simuladas, com escassa validação em ambientes reais ou protótipos de rede operacionais. Faltam estudos que confrontem direta-

mente os trade-offs entre segurança e desempenho, especialmente em contextos com restrições computacionais, como dispositivos IoT. Além disso, a ausência de um modelo unificado de gerenciamento de identidades e chaves entre operadoras e regiões revela um desalinhamento entre a evolução técnica do 5G e sua infraestrutura de confiança global. Soluções baseadas em IA e delegação de credenciais são promissoras, mas a carência de padronização, interoperabilidade e análise de custo-eficácia compromete sua adoção prática em escala.

5.3.2.2 Vazamento de Dados

A confidencialidade em redes 5G é ameaçada pelo compartilhamento de funções entre *slices*, onde instâncias maliciosas podem falsificar identidade e acessar dados de outros domínios por meio da *Network Repository Function* (NRF) (Alwis *et al.*, 2024; Gao *et al.*, 2024). Identificadores como o *Single Network Slice Selection Assistance Information* (S-NSSAI) também podem ser interceptados durante o estabelecimento de conexão, favorecendo ataques *Man-in-the-Middle* e negação de serviço seletiva (Gao *et al.*, 2024). Em ambientes *multi-slice* e *multitenant*, a ausência de isolamento adequado permite o cruzamento de dados entre aplicações de criticidade distinta, agravado por terminais conectados a múltiplos *slices* simultaneamente (Alwis *et al.*, 2024; Suomalainen *et al.*, 2020). Atacantes também podem manipular relatórios de operação de *slices* para induzir ajustes maliciosos ou replicar topologias legítimas (Gao *et al.*, 2024). Interfaces expostas da arquitetura *cloud-native*, como a *Network Exposure Function* (NEF), representam vetores adicionais para vazamento, sobretudo quando mal autenticadas (Tang *et al.*, 2022; Ahmad *et al.*, 2019). Ainda, durante a mobilidade entre *slices*, falhas na separação de chaves podem gerar acessos indevidos a dados sensíveis (Gao *et al.*, 2024).

Embora diversos estudos identifiquem vetores de vazamento de dados em redes 5G, observa-se uma lacuna na validação empírica das técnicas de mitigação propostas, sobretudo em cenários *multitenant* complexos. A literatura destaca riscos associados à exposição de interfaces como NEF e NRF, mas são escassas as análises sobre mecanismos eficazes de autenticação mútua e segmentação de acesso baseados em atributos (ABAC) nesses contextos. Além disso, poucos trabalhos investigam a eficácia de controles de segregação em terminais com múltiplos *slices* simultâneos — realidade crescente com o avanço da convergência entre redes públicas e privadas. A ausência de normativas claras sobre segurança *inter-slice* agrava a dificuldade de padronização, tornando a proteção da confidencialidade altamente dependente de políticas locais e soluções proprietárias. Essa heterogeneidade compromete a interoperabilidade segura entre

domínios, demandando abordagens mais sistemáticas e intersetoriais para isolamento de dados e autenticação federada entre funções de rede.

5.3.2.3 Orquestração Fragmentada

A fragmentação da orquestração em redes 5G compromete a aplicação coerente de políticas de segurança entre nuvem, borda e acesso rádio, permitindo que atacantes explorem falhas de coordenação para manipular tráfego ou induzir indisponibilidade (Bánáti, 2025; Batewela *et al.*, 2025a; Singh *et al.*, 2024). Arquiteturas como ETSI NFV MANO são apontadas como insuficientes por não oferecerem monitoramento em tempo real nem ciclos automatizados de resposta a ameaças emergentes (Batewela *et al.*, 2025a). A situação se agrava em ambientes *multitenant* com *slicing*, onde inconsistências entre *slices* facilitam ataques cruzados e vazamentos laterais (Bánáti, 2025). A ausência de padronização nas interfaces de orquestração, uso de APIs abertas e presença de múltiplos *vendors* dificultam a integração entre controladores SDN, orquestradores NFV e componentes MEC (Bánáti, 2025; Batewela *et al.*, 2025a). Como solução, propõe-se o uso de *frameworks* com ML, orquestração adaptativa e resposta autônoma, capazes de operar em cenários dinâmicos com mobilidade de funções (Batewela *et al.*, 2025a; Singh *et al.*, 2024).

Um cenário típico de exploração dessa fragilidade ocorre quando diferentes domínios da rede - como o núcleo, a borda e o plano de controle - são orquestrados por soluções independentes, sem sincronização segura entre si. Nesse contexto, um atacante pode executar ações de interceptação entre domínios, redirecionar fluxos sensíveis ou desativar funções virtualizadas por meio de comandos falsificados. A ausência de autenticação mútua entre os orquestradores, combinada à inexistência de uma política centralizada de detecção de anomalias, agrava a exposição da rede. Essa lacuna mostra que a falta de padronização na orquestração não é apenas um desafio de interoperabilidade, mas um vetor real para ataques complexos em redes de próxima geração.

Embora a literatura aponte a ausência de padronizações consolidadas para a orquestração segura em redes 5G com IPv6, é importante destacar que existem iniciativas em andamento. O *3rd Generation Partnership Project* (3GPP) tem publicado especificações técnicas como a série TS 33.501 voltadas à segurança de redes 5G, enquanto o *Internet Engineering Task Force* (IETF) contribui com *Request for Comments* (RFCs) e *drafts* que tratam da segurança em redes baseadas em IPv6, SDN e NFV. No entanto, ainda não há consenso nem diretrizes

unificadas que definam como esses componentes devem interagir de forma segura em arquiteturas heterogêneas. Essa lacuna de padronização prática e interoperável continua sendo um desafio para a aplicação coerente de políticas de segurança, especialmente em ambientes *multitenant* com *slicing* e componentes de múltiplos fornecedores.

5.3.3 Requisitos Funcionais Não Atendidos

As redes 5G, por sua complexidade arquitetural e dinamicidade operacional, enfrentam dificuldades recorrentes em garantir os requisitos fundamentais da segurança da informação: privacidade, disponibilidade e integridade. Esses princípios, muitas vezes tratados de forma transversal nas camadas da rede, são comprometidos quando não há implementação efetiva de controles em cada ponto do ciclo de vida dos dados, desde a origem até a borda e o núcleo da rede.

Em SBAs, o uso extensivo de APIs abertas e o compartilhamento de funções virtualizadas entre diferentes *slices* e domínios operacionais ampliam significativamente os pontos de exposição da rede. Em diversos cenários analisados, a ausência de autenticação robusta, a configuração inadequada de políticas de acesso e a falta de monitoramento contínuo resultam na violação de requisitos fundamentais de segurança, mesmo na ausência de ataques ativos (Sullivan *et al.*, 2021; Tang *et al.*, 2022; Batewela *et al.*, 2025a).

A privacidade é comprometida especialmente em cenários onde a identidade do usuário não é devidamente protegida, como em mensagens de controle não criptografadas, ou quando *slices* distintos compartilham funções sem isolamento lógico rigoroso (Alwis *et al.*, 2024; Jover; Marojevic, 2019). Já a disponibilidade sofre com falhas de planejamento de resiliência e ataques que exploram a elasticidade da rede virtualizada, como DoS/DDoS direcionados a funções específicas ou sobrecarga de *slices* sensíveis (Khan *et al.*, 2019b; Gao *et al.*, 2024). Por fim, a integridade dos dados e comandos pode ser comprometida por falhas em canais de sinalização, ausência de validação de pacotes e injeções de comandos em interfaces abertas (Singh *et al.*, 2024).

As subseções seguintes detalham essas três categorias de requisitos funcionais frequentemente comprometidos, com base nos artigos analisados, apontando causas, impactos e propostas de mitigação.

5.3.3.1 Privacidade

A privacidade em redes 5G enfrenta riscos crescentes devido à integração com IoT, computação em nuvem e *edge computing*. Três dimensões principais são afetadas: identidade, localização e dados. A exposição da identidade ocorre por ataques como IMSI *catching*, especialmente em cenários com ausência de chaves públicas ou sessões de emergência, mesmo com o uso do identificador criptografado *Subscription Concealed Identifier* (SUCI) (Ahmad *et al.*, 2019; Salahdine *et al.*, 2023; Jover; Marojevic, 2019). A privacidade de localização é comprometida por serviços baseados em geolocalização (LBS), que coletam dados continuamente, permitindo inferência de rotinas sem o consentimento explícito do usuário (Khan *et al.*, 2019b; Ahmad *et al.*, 2018). Técnicas como *cloaking*, obfuscação e anonimização são estratégias mitigadoras (Khan *et al.*, 2019b; Ahmad *et al.*, 2019). Já a privacidade de dados sofre com a exposição em ambientes *multitenant*, uso de *cloud* e transferência entre fronteiras, onde faltam políticas padronizadas de retenção e acesso (Khan *et al.*, 2019b; Suomalainen *et al.*, 2020; Salahdine *et al.*, 2023). A literatura recomenda princípios como *accountability*, minimização de dados e criptografia fim-a-fim como fundamentos essenciais para garantir a proteção da privacidade em redes 5G

Apesar da ampla discussão sobre estratégias de preservação da privacidade, nota-se que muitas soluções permanecem no campo conceitual ou apresentam aplicabilidade restrita a contextos altamente controlados. A obfuscação de localização, por exemplo, tende a degradar a precisão de serviços legítimos, como navegação ou entrega, gerando um dilema entre funcionalidade e privacidade. Além disso, a literatura raramente aborda os desafios regulatórios e operacionais de aplicar criptografia fim-a-fim em ambientes heterogêneos, como sistemas legados, dispositivos IoT com baixa capacidade computacional ou redes com múltiplos provedores. A ausência de um consenso global sobre políticas de retenção e consentimento agrava a exposição do usuário em sistemas distribuídos, especialmente em transferências transfronteiriças. Essas lacunas indicam a necessidade urgente de abordagens que aliem viabilidade técnica, proteção legal e adaptação ao cenário real de redes móveis.

5.3.3.2 Disponibilidade

A garantia de disponibilidade em redes 5G é desafiada por sua arquitetura distribuída, natureza *multitenant* e uso intensivo de NFV e *slicing*, que ampliam o risco de esgotamento de recursos e falhas em cascata. Ataques de DoS/DDoS contra funções como AMF e UPF, ou

sobrecarga deliberada de *slices*, são destacados como vetores recorrentes (Tang *et al.*, 2022; Hamroun *et al.*, 2025; Singh *et al.*, 2024). A presença de MEC, com recursos limitados e baixa redundância, agrava a vulnerabilidade à interrupção de serviços (Khan *et al.*, 2019b; Suomalainen *et al.*, 2020; Ahmad *et al.*, 2018). Falhas de isolamento entre slices permitem propagação lateral de ataques, afetando serviços críticos como saúde e transporte (Gao *et al.*, 2024; Salahdine *et al.*, 2023). Além disso, a ausência de mecanismos eficazes de *failover*, controle de sobrecarga e balanceamento adaptativo aumenta o risco de *downtime* (Khan *et al.*, 2019b; Salahdine *et al.*, 2023; Singh *et al.*, 2024). Estudos propõem o uso de orquestração inteligente, redundância física e lógica, e estratégias baseadas em ML. Em cenários com requisitos de tempo estrito, como automação industrial, a integração com *Time-Sensitive Networking* (TSN) exige latência ultrabaixa e resiliência a falhas temporais (Sethi *et al.*, 2022).

Embora os estudos identifiquem corretamente os riscos à disponibilidade em redes 5G, nota-se uma carência de consenso sobre como assegurar resiliência frente à crescente complexidade da arquitetura distribuída. A dependência de recursos virtualizados, a fragmentação da rede por meio de *slicing* e a presença de funções críticas como AMF expostas a ataques volumétricos, sugerem que abordagens tradicionais de disponibilidade, como redundância estática ou *failover* simples, tornam-se insuficientes. A literatura menciona orquestração inteligente e uso de *Machine Learning* para predição de falhas, porém tais soluções ainda carecem de validação ampla em ambientes reais e padronização formal. A interoperabilidade entre mecanismos de alta disponibilidade e tecnologias como TSN, essencial para garantir QoS em aplicações críticas, também se encontra em estágio inicial de desenvolvimento. Torna-se evidente a necessidade de estratégias mais integradas entre detecção, isolamento dinâmico e recuperação proativa, alinhadas a um *framework* de confiabilidade adaptável ao contexto de operação de cada *slice*.

5.3.3.3 Integridade

A integridade dos dados em redes 5G é essencial para garantir que as informações não sejam alteradas durante a transmissão, especialmente em aplicações críticas como saúde e controle industrial. Embora mecanismos como a verificação no *Radio Resource Control* (RRC) e *Non-Access Stratum* (NAS) existam no plano de controle, a proteção no plano de usuário não é mandatória e depende de medidas adicionais dos operadores (Oruma; Petrovic, 2023; Jover; Marojevic, 2019). A integridade pode ser comprometida por ataques de injeção, *replay* e *Man-in-the-Middle*, além de falhas físicas e operacionais, como sabotagem de estações

e vulnerabilidades em servidores (Bánáti, 2025; Oruma; Petrovic, 2023). As contramedidas incluem criptografia robusta, protocolos como TLS, monitoramento contínuo, autenticação forte, segmentação e auditorias regulares. Também são exploradas soluções com *blockchains* permissionadas para garantir consistência e rastreabilidade em ambientes distribuídos (Oruma; Petrovic, 2023). Entretanto, desafios persistem em cenários de *edge computing* e IoT, onde dispositivos limitados dificultam a aplicação de proteções avançadas.

Apesar da existência de soluções como uso de *blockchains* permissionadas e protocolos criptográficos robustos, a efetiva garantia de integridade ainda enfrenta barreiras significativas na prática. Em especial, a não obrigatoriedade de proteção no plano de usuário cria zonas de vulnerabilidade exploráveis por atacantes, sobretudo em serviços que trafegam dados sensíveis sem camadas adicionais de proteção. Além disso, a literatura tende a superestimar a viabilidade do uso de *blockchains* em redes 5G, ignorando os altos custos computacionais e o impacto na latência - fatores críticos em aplicações em tempo real. Em dispositivos IoT com baixa capacidade de processamento, a aplicação de técnicas como TLS ou verificação em cadeia se torna impraticável, o que abre margem para adulterações silenciosas. O cenário é agravado pela ausência de mecanismos padronizados de verificação de integridade no nível de borda e pela dificuldade de auditoria em ambientes altamente distribuídos. Esses aspectos indicam que, embora bem documentadas, as soluções propostas ainda carecem de maturidade e aplicabilidade em larga escala.

5.4 Solução

A análise dos problemas de segurança evidenciou tanto vulnerabilidades técnicas específicas quanto fragilidades estruturais presentes nas arquiteturas que compõem o ecossistema 5G. Diante desse panorama, diversos estudos propõem soluções orientadas à mitigação desses riscos, com foco em mecanismos criptográficos, estratégias de orquestração inteligente, controle de acesso robusto e monitoramento contínuo. Esta seção apresenta essas abordagens de forma sistematizada, agrupando-as conforme suas características técnicas e objetivos de segurança.

A fim de mitigar os diversos desafios de segurança identificados em redes 5G e IPv6, os estudos revisados propõem um conjunto diversificado de soluções técnicas. Essas soluções podem ser classificadas em três categorias principais: técnicas de criptografia, mecanismos inteligentes e abordagens de políticas e orquestração. Cada uma delas responde a vulnerabilidades específicas, seja no plano de controle, de usuário ou nas interfaces entre dispositivos e a

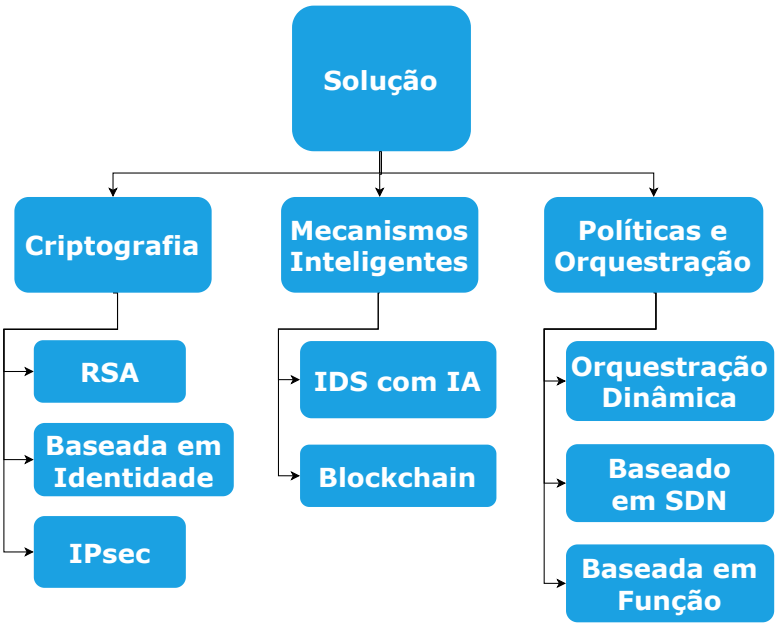
infraestrutura de rede.

As propostas variam desde a adoção de algoritmos criptográficos tradicionais, como RSA e IPsec, até técnicas mais modernas e adaptativas, como criptografia baseada em identidade. Além disso, observa-se um crescimento significativo no uso de IA para a detecção e mitigação de ataques, por meio de sistemas de detecção de intrusão (IDS) aprimorados com ML. Complementarmente, soluções baseadas em *Blockchain* têm ganhado espaço como alternativas descentralizadas para assegurar a integridade e a confiabilidade de transações e dados críticos.

Do ponto de vista organizacional da rede, a orquestração eficiente de recursos e serviços de segurança é outro aspecto essencial. Nesse contexto, surgem abordagens como a orquestração dinâmica, baseada em SDN ou em funções específicas de rede, que oferecem flexibilidade, escalabilidade e resposta rápida a ameaças emergentes.

A Figura 16 apresenta uma síntese visual das soluções analisadas na literatura, organizadas em três categorias principais: criptografia, mecanismos inteligentes e abordagens baseadas em políticas e orquestração. Essa estrutura orienta a organização desta seção e será detalhada nas subseções a seguir.

Figura 16 – Categorias que Compõem o Eixo Solução.



Fonte: Elaborado pelo Autor.

Nas subseções a seguir, cada um desses conjuntos é explorado tecnicamente com base nos artigos analisados nesta revisão sistemática, com o objetivo de apresentar um panorama das soluções mais recorrentes, suas vantagens, limitações e perspectivas de aplicação em ambientes

5G/IPv6.

5.4.1 Mecanismos Criptográficos

A criptografia continua sendo uma das principais ferramentas para garantir a segurança de dados e comunicações em ambientes 5G e IPv6. Com o aumento da superfície de ataque e a crescente heterogeneidade dos dispositivos conectados, a proteção da confidencialidade, autenticidade e integridade das informações torna-se ainda mais crítica.

Nos artigos analisados, observa-se uma predominância de três abordagens criptográficas no contexto de redes 5G: o uso do algoritmo RSA, a criptografia baseada em identidade (IBC) e o protocolo IPsec. Cada uma dessas soluções busca responder a requisitos específicos do ambiente de rede - como mobilidade, latência reduzida e compatibilidade com IPv6 - e está alinhada aos diferentes domínios de segurança definidos pelo 3GPP, como segurança de acesso, de domínio e de aplicação.

A seguir, cada uma dessas técnicas é detalhada quanto ao seu funcionamento, aplicações no contexto de 5G/IPv6 e evidências extraídas da literatura.

5.4.1.1 RSA

A criptografia RSA é utilizada pontualmente em redes 5G, principalmente para autenticação inicial e estabelecimento seguro de chaves, especialmente na camada de controle. Na arquitetura MES-FPMIPv6, por exemplo, o RSA garante a integridade da comunicação antes do *handover* (Degefa *et al.*, 2022). No entanto, estudos apontam suas limitações em cenários com dispositivos IoT, devido ao alto custo computacional, e seu impacto negativo na latência em aplicações críticas (Saleem *et al.*, 2020; Ahmad *et al.*, 2018). Apesar de robusto, o RSA tende a ser substituído por algoritmos mais leves ou híbridos, e sua integração com protocolos como IPsec em IPv6 exige configuração cuidadosa. Seu uso permanece restrito a casos onde a segurança assimétrica é indispensável e os recursos da rede o permitem.

A análise do uso de RSA em redes 5G revela um dilema recorrente entre robustez criptográfica e viabilidade prática. Embora sua aplicação em camadas de controle e autenticação inicial seja bem documentada, a literatura aponta para uma crescente incompatibilidade entre os requisitos de desempenho das redes 5G e o custo computacional elevado do RSA, especialmente em cenários com dispositivos IoT de baixa capacidade. A ausência de aceleração criptográfica nativa nesses dispositivos limita sua adoção ampla. Além disso, mesmo quando utilizado em

conjunto com protocolos como IPsec sobre IPv6, o RSA pode introduzir latências inaceitáveis para aplicações de tempo sensível, como saúde e automação industrial. Esses fatores explicam a tendência observada em alguns estudos de migrar para esquemas mais leves, como Criptografia de Curva Elíptica (ECC), ou híbridos, que combinem o RSA apenas na fase inicial de troca de chaves. A falta de diretrizes padronizadas sobre onde e como aplicar o RSA com segurança e eficiência reforça a necessidade de estudos comparativos mais aprofundados sobre algoritmos assimétricos em ambientes 5G.

5.4.1.2 Baseado em Identidade

A *Identity-Based Cryptography* (IBC) é investigada como solução promissora para autenticação e privacidade em redes 5G, principalmente em cenários com dispositivos IoT de recursos limitados. Ao eliminar certificados digitais tradicionais, a IBC reduz a complexidade da infraestrutura de chaves públicas. O esquema FC-PA, proposto para redes veiculares 5G, utiliza pseudônimos com IBC para garantir anonimato e resistência a ataques de repetição com baixa latência (Mohammed *et al.*, 2023). Em contextos de IoT, a IBC facilita conexões seguras sem armazenamento de certificados, mas enfrenta desafios de escalabilidade e dependência de autoridades confiáveis (Ahmed *et al.*, 2024). Embora ofereça proteção contra *spoofing* e interceptação, sua adoção é limitada por barreiras de padronização e compatibilidade com sistemas legados (Khan *et al.*, 2019b).

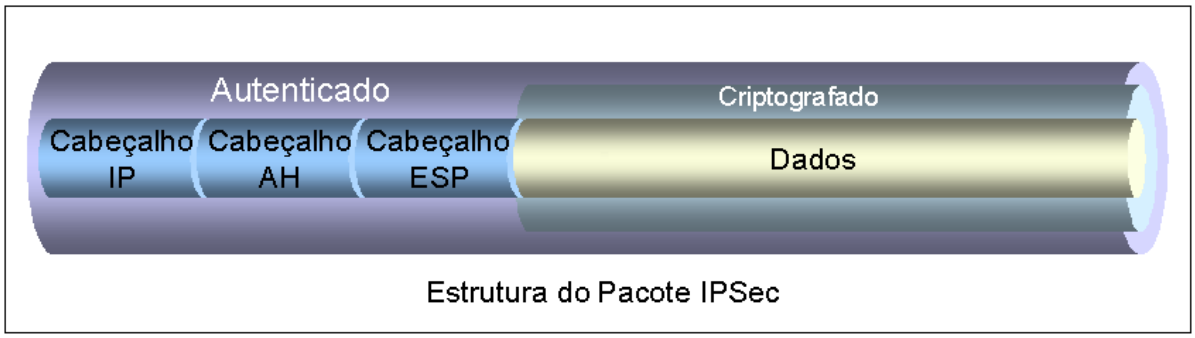
Apesar do potencial da criptografia baseada em identidade, os estudos revisados raramente abordam os impactos práticos da introdução dessa abordagem em infraestruturas heterogêneas. Em particular, a dependência de uma Autoridade de Geração de Chaves (PKG) centralizada levanta preocupações quanto à confiança e resiliência frente a falhas ou comprometimentos. A falta de mecanismos amplamente padronizados para distribuição segura de chaves privadas também dificulta a interoperabilidade com arquiteturas existentes. Além disso, há um vácuo na literatura quanto à aplicação da IBC em cenários de larga escala, como IoT massiva, onde a administração de pseudônimos e a revogação de identidades se tornam particularmente desafiadoras. Assim, embora teoricamente atrativa, a adoção da IBC carece de validações robustas em ambientes reais e ainda enfrenta obstáculos técnicos e regulatórios que precisam ser superados para garantir seu uso confiável em redes 5G.

5.4.1.3 IPsec

O *Internet Protocol Security* (IPsec) fornece autenticação, integridade e confidencialidade em redes 5G com IPv6, sendo nativamente suportado por esse protocolo e amplamente utilizado em comunicações ponta-a-ponta (Dutta; Hammad, 2020; Tang *et al.*, 2022; Suomalainen *et al.*, 2020; Ahmad *et al.*, 2019). Mecanismos como o *Encapsulating Security Payload* (ESP) e o *Authentication Header* (AH) garantem criptografia de pacotes e autenticação de origem, respectivamente (Dutta; Hammad, 2020). O IPsec é empregado na criação de túneis seguros entre segmentos da rede, protegendo planos de controle e de usuário, inclusive em arquiteturas *Dual Stack* (Suomalainen *et al.*, 2020; Ahmad *et al.*, 2019). Apesar de robusto, sua sobrecarga computacional limita sua aplicabilidade em dispositivos IoT com restrições de energia, sendo recomendado o uso complementar de TLS/DTLS nesses cenários (Tang *et al.*, 2022). Ainda assim, o IPsec permanece como solução consolidada para mitigar ataques de interceptação e falsificação em ambientes 5G distribuídos.

A Figura 17 apresenta a estrutura de encapsulamento de um pacote protegido por IPSec. Os cabeçalhos AH e ESP são adicionados ao pacote IP para prover autenticação, integridade e confidencialidade. No contexto do IPv6, o IPSec é incorporado como funcionalidade nativa, sendo amplamente utilizado nos estudos revisados como a principal medida de proteção para dados em trânsito em redes 5G.

Figura 17 – Estrutura do Pacote IPSec.



Fonte: Caldas (2014).

Apesar de sua solidez teórica e adoção consolidada em cenários corporativos, a aplicação prática do IPsec em ambientes 5G com IoT ainda apresenta limitações substanciais. A alta sobrecarga de processamento imposta pelo protocolo o torna inviável para a maioria dos dispositivos de borda com capacidade limitada - justamente onde se concentra o maior

volume de tráfego sensível. Além disso, a gestão de chaves no IPsec, frequentemente realizada manualmente ou via *Internet Key Exchange* (IKE), não escala bem em ambientes dinâmicos e distribuídos, dificultando sua adoção em larga escala em arquiteturas baseadas em *slicing* e mobilidade. Embora a literatura aponte o IPsec como solução primária para proteção de dados em trânsito, poucos estudos discutem alternativas mais leves ou complementares para redes heterogêneas, revelando uma lacuna crítica na pesquisa sobre segurança adaptável em redes de nova geração.

5.4.2 Mecanismos Inteligentes

Com o avanço das redes 5G e a crescente complexidade dos cenários de conectividade - como o uso intensivo de dispositivos da Internet das Coisas (IoT), redes veiculares e aplicações de borda - a detecção e resposta a ameaças de segurança demandam soluções que sejam dinâmicas, escaláveis e adaptativas. Nesse contexto, emergem os chamados mecanismos inteligentes, que utilizam IA, ML e tecnologias descentralizadas para proteger a rede de forma proativa.

Entre os mecanismos mais recorrentes na literatura destacam-se os Sistemas de Detecção de Intrusão com suporte a IA (IDS com IA) e a tecnologia de *Blockchain*. O primeiro visa aprimorar a capacidade de identificar comportamentos anômalos e padrões de ataque que escapam aos mecanismos tradicionais de segurança. Já o segundo oferece uma estrutura distribuída e imutável para validação de eventos e gestão de identidades em ambientes colaborativos e sem confiança mútua.

Esses mecanismos têm sido aplicados a diversos níveis da arquitetura 5G, desde o plano de controle e interfaces de orquestração até aplicações finais de usuários. A adoção dessas técnicas visa não apenas ampliar a detecção e prevenção de ataques, mas também reduzir a dependência de soluções centralizadas e aumentar a resiliência da rede frente a falhas e ataques coordenados.

Nas subseções seguintes, serão apresentados os principais achados da literatura sobre IDS com IA e *Blockchain*, detalhando suas abordagens, aplicações, limitações e perspectivas de adoção em redes 5G/IPv6.

5.4.2.1 IDS com IA

Sistemas de Detecção de Intrusão (IDS) com IA têm ganhado destaque em redes 5G por sua capacidade de identificar ataques *zero-day* e padrões anômalos de tráfego. Utilizando

técnicas como árvores de decisão, *deep learning*, *autoencoders* e florestas aleatórias, esses sistemas operam em tempo real com alta escalabilidade e adaptação a novos vetores de ataque (Hamroun *et al.*, 2025). No entanto, sua eficácia depende fortemente da qualidade dos dados de treinamento e da curadoria de tráfego anômalo representativo. Além disso, a portabilidade entre diferentes ambientes 5G pode exigir ajustes finos e reaprendizado constante. A integração com SDN e MEC permite monitoramento distribuído e resposta local, ampliando a resiliência da rede. Apesar de promissores, os IDS com IA enfrentam desafios quanto ao custo computacional e robustez frente a técnicas de evasão.

Embora os IDS baseados em IA representem um avanço significativo frente aos modelos tradicionais, a análise dos estudos revisados revela um excesso de confiança em abordagens supervisionadas, frequentemente validadas em *datasets* limitados e fora de contexto real. Em muitos casos, a eficácia alegada não considera a complexidade dos ambientes 5G reais, marcados por tráfego criptografado, mobilidade de funções e redes heterogêneas. Além disso, a ausência de padronização para avaliação desses sistemas, bem como a falta de integração prática com mecanismos de resposta automatizada, indica que sua aplicação ainda está distante de ambientes de produção. A literatura raramente discute a viabilidade operacional de treinar e implantar modelos de IA em tempo real nas bordas da rede, o que aponta para uma lacuna crítica entre a pesquisa e a implementação.

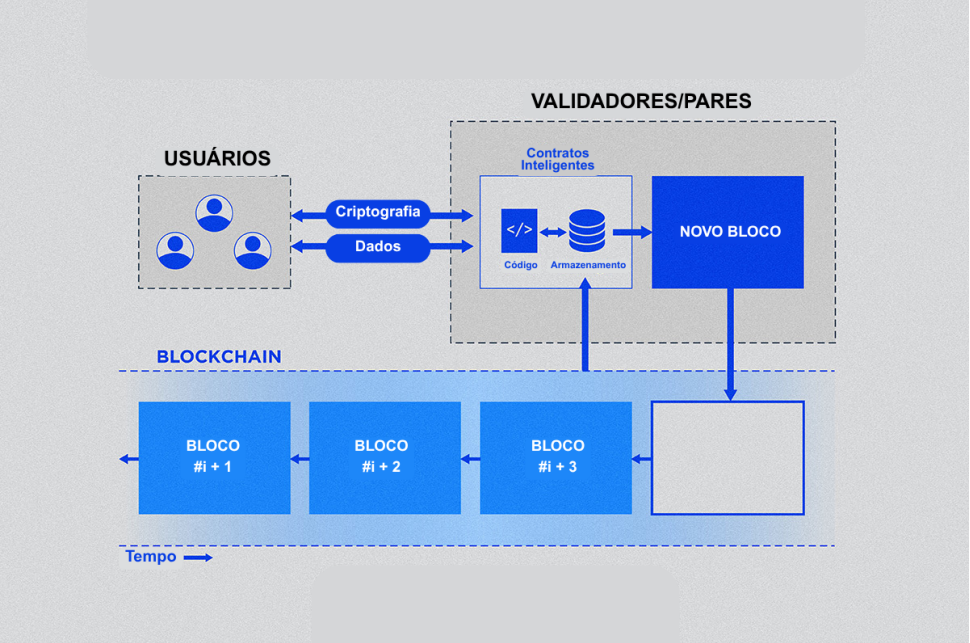
5.4.2.2 Blockchain

A tecnologia *blockchain* tem sido explorada em redes 5G como mecanismo de segurança descentralizado, permitindo registros imutáveis, verificação de integridade e autenticação distribuída, especialmente em cenários com IoT, redes veiculares e computação em borda (Dutta; Hammad, 2020; Tang *et al.*, 2022; Ahmad *et al.*, 2019). Contratos inteligentes (*smart contracts*) possibilitam automação de políticas entre domínios, eliminando pontos únicos de falha e fortalecendo o não-repúdio. A integração com MEC amplia a rastreabilidade e a resiliência contra ataques como *spoofing* e *Man-in-the-Middle*. No entanto, desafios como escalabilidade, latência de consenso e compatibilidade com aplicações de tempo real limitam sua adoção em larga escala. Abordagens com *blockchains permissionadas* e mecanismos de consenso leves são sugeridas como alternativas. Embora complementar, o *blockchain* reforça a segurança por meio de descentralização, integridade e transparência.

A Figura 18 ilustra o funcionamento de contratos inteligentes em uma arquitetura

baseada em *Blockchain*. Os usuários interagem com os contratos via transações contendo dados. O código e o armazenamento do contrato são executados por validadores, que registram um novo bloco na cadeia imutável de blocos (*Blockchain*).

Figura 18 – Contratos Inteligentes em uma Arquitetura Baseada em *Blockchain*.



Fonte: Adaptado de Crypto.com University (2023).

Apesar do entusiasmo da literatura quanto ao uso de *blockchain* como reforço de segurança em redes 5G, há uma lacuna significativa entre o potencial teórico e a adoção prática dessa tecnologia. A maioria dos estudos explora o *blockchain* em contextos restritos - como redes veiculares, ambientes com MEC ou aplicações IoT — onde sua descentralização e transparência agregam valor. No entanto, poucos trabalhos oferecem avaliações empíricas robustas quanto ao desempenho real desses sistemas sob cargas elevadas ou cenários de baixa latência. A latência de consenso, especialmente em *blockchains* públicas ou híbridas, entra em conflito direto com os requisitos de tempo crítico do 5G, particularmente em fatias (*slices*) destinadas à automação industrial ou saúde. Embora soluções como *blockchains* permissionadas com algoritmos de consenso leves mitiguem parte desses problemas, elas frequentemente sacrificam a descentralização plena. Assim, é necessário avançar em diretrizes padronizadas e *benchmarks* que equilibrem segurança, escalabilidade e tempo de resposta, sob diferentes cenários de uso.

5.4.3 Políticas e Orquestração

A crescente complexidade das redes 5G, aliada à diversidade de serviços e dispositivos conectados, exige mecanismos de segurança que sejam ao mesmo tempo coordenados, adaptativos e escaláveis. Nesse cenário, surgem com destaque as abordagens de políticas e orquestração, responsáveis por definir, aplicar e adaptar regras de segurança de forma integrada e automatizada ao longo da rede.

Diferentemente de soluções pontuais como algoritmos criptográficos ou sistemas de detecção, as técnicas de orquestração operam em nível sistêmico, permitindo a implementação de políticas de segurança distribuídas e ajustáveis em tempo real. Esse modelo é essencial para lidar com eventos dinâmicos - como mudanças de contexto, migração de serviços, mobilidade de usuários e ataques distribuídos - sem comprometer o desempenho e a continuidade do serviço.

A literatura aponta três vertentes principais de orquestração em ambientes 5G: a orquestração dinâmica, que permite o replanejamento adaptativo de recursos e políticas; a orquestração baseada em SDN, que aproveita a separação entre plano de controle e plano de dados para flexibilizar a aplicação de regras; e a orquestração baseada em função, com foco em VNFs gerenciadas de forma modular.

Nas subseções seguintes, serão analisadas essas três abordagens, suas aplicações no contexto da segurança em redes 5G/IPv6 e os desafios associados à sua implementação em ambientes reais.

5.4.3.1 Orquestração Dinâmica

A orquestração dinâmica em redes 5G permite o provisionamento e ajuste automático de funções de rede virtualizadas (VNFs) e *slices*, adaptando-se a variações de tráfego, QoS e eventos de segurança. Ao contrário de modelos estáticos, ela opera com decisões baseadas em contexto, muitas vezes suportadas por IA e ML (Batewela *et al.*, 2025a). Em ambientes com SDN e NFV, essa abordagem viabiliza respostas em tempo real a alertas de segurança, como a ativação de IDS ou *firewalls* sob demanda (Bánáti, 2025). No entanto, a automação amplia a superfície de ataque, tornando orquestradores alvos críticos, especialmente quando expostos por interfaces abertas ou sem autenticação robusta (Tang *et al.*, 2022). Além disso, a falta de padrões para integração entre domínios orquestrados pode gerar inconsistências de políticas e comprometer a governança da rede (Batewela *et al.*, 2025b). Assim, a orquestração dinâmica

fortalece a segurança adaptativa, mas requer proteção rigorosa de seus próprios mecanismos.

Embora a orquestração dinâmica represente um avanço essencial para a resiliência e adaptabilidade de redes 5G, sua implementação ainda enfrenta desafios técnicos e operacionais não resolvidos. Os estudos analisados demonstram uma tendência crescente de uso de IA/ML para decisões em tempo real, mas muitas abordagens carecem de validação prática em ambientes complexos e heterogêneos. Além disso, poucos trabalhos abordam como garantir a confiabilidade dos dados de entrada usados por esses orquestradores — fator crítico, dado que decisões erradas podem comprometer a rede como um todo. A dependência de interfaces abertas e APIs expõe pontos únicos de falha, tornando a segurança do próprio orquestrador uma prioridade. Adicionalmente, a ausência de padronização para orquestração interdomínio limita a interoperabilidade e favorece soluções proprietárias com baixo nível de auditabilidade. Portanto, a literatura aponta a orquestração dinâmica como peça-chave na segurança adaptativa, mas sua adoção efetiva depende de avanços em padrões, testes de robustez e mecanismos de defesa proativos integrados ao próprio plano de orquestração.

5.4.3.2 Baseada em SDN

A orquestração baseada em *Software-Defined Networking* (SDN) em redes 5G permite centralizar o controle e automatizar políticas de segurança, favorecendo a adaptação dinâmica em ambientes com *slicing*, *edge computing* e múltiplos domínios (Batewela *et al.*, 2025a). Integrada com NFV, essa abordagem viabiliza orquestração fim-a-fim com isolamento por *Virtual Private Network* (VPNs) *Multiprotocol Label Switching* (MPLS) e monitoramento contínuo. No entanto, o controlador SDN representa um ponto único de falha e alvo crítico para ataques como ARP *spoofing*, injeção de regras e DoS (Dutta; Hammad, 2020). Interfaces abertas *northbound* e *southbound* ampliam o risco de escalonamento de privilégios. A segurança dessa arquitetura exige autenticação forte, verificação de integridade de políticas, sincronização segura entre domínios SDN e técnicas como *hardening* de controladores, criptografia de canais e detecção de anomalias em tempo real (Sullivan *et al.*, 2021).

A centralização do controle promovida pelo SDN oferece ganhos consideráveis em flexibilidade e visibilidade, mas também introduz fragilidades estruturais ainda pouco exploradas na prática. Embora a literatura destaque a eficiência da orquestração baseada em SDN na adaptação dinâmica de políticas de segurança, há escassez de estudos que validem sua resiliência frente a ataques coordenados, especialmente nos planos de dados e controle. O risco inerente

ao ponto único de falha representado pelo controlador é reconhecido, mas raramente tratado com abordagens concretas de tolerância a falhas. Além disso, as interfaces abertas, essenciais para a interoperabilidade e automação, permanecem como vetores críticos de ataque quando mal configuradas ou expostas sem autenticação robusta. A ausência de consenso sobre mecanismos de verificação cruzada entre múltiplos domínios SDN dificulta a adoção de modelos federados de orquestração segura. Portanto, apesar de promissora, a arquitetura baseada em SDN demanda uma camada adicional de segurança endógena ao próprio plano de controle, com foco em redundância, verificação contínua e defesa proativa.

5.4.3.3 Baseada em Função

A Orquestração Baseada em Função (*Function-Based Orchestration* – FBO) permite maior granularidade no controle de serviços 5G ao decompor elementos de rede em funções encadeáveis conforme requisitos de segurança e desempenho. Com suporte de NFV e *Service Function Chaining* (SFC), a FBO viabiliza a inserção dinâmica de funções como *firewalls* e inspeção profunda após a detecção de ameaças, sem interrupção do serviço (Batewela *et al.*, 2025a). Essa flexibilidade é crítica em ambientes de borda com baixa latência. No entanto, desafios incluem sobrecarga de funções de segurança, conflitos entre políticas simultâneas e impacto na QoS (Ahmad *et al.*, 2018). A eficácia da FBO depende de orquestradores inteligentes capazes de avaliar contexto, criticidade e recursos, aplicando políticas adaptativas com base em SLAs e monitoramento contínuo (Khan *et al.*, 2019b). Como solução adaptativa, a FBO reforça a resiliência e personalização de segurança em redes 5G dinâmicas e heterogêneas.

Apesar de sua capacidade de adaptação e resposta contextualizada, a Orquestração Baseada em Função (FBO) ainda carece de validação robusta quanto à sua escalabilidade e interoperabilidade em redes 5G heterogêneas. A literatura frequentemente explora os benefícios da inserção dinâmica de funções de segurança via SFC, mas são escassas as análises sobre a latência introduzida por encadeamentos excessivos ou mal otimizados. Além disso, há pouco consenso sobre a resolução automatizada de conflitos entre múltiplas políticas de segurança, o que pode comprometer a coerência da proteção aplicada em tempo real. A dependência de orquestradores altamente inteligentes levanta preocupações práticas sobre a maturidade dos algoritmos de decisão empregados e sua capacidade de operar sob restrições computacionais típicas de ambientes de borda. Assim, embora a FBO represente um avanço importante rumo à segurança personalizada, sua eficácia plena requer mecanismos complementares de otimização

de cadeia, garantia de qualidade de serviço (*QoS-aware*) e validação contínua do impacto das políticas aplicadas.

5.5 Quadros

Os Quadros 9, 10 e 11 representam a síntese da análise taxonômica aplicada aos 29 artigos selecionados na revisão sistemática conduzida neste trabalho. Cada uma delas reflete a classificação dos estudos conforme os três eixos principais da taxonomia proposta: Tecnologia, Problemas de Segurança e Soluções. Essa estrutura foi concebida para organizar a literatura de forma coerente, permitindo compreender com maior profundidade a abordagem dos autores frente aos desafios e estratégias de segurança em redes 5G integradas ao IPv6.

Cada linha das tabelas corresponde a um artigo analisado, identificado por sua referência numérica, enquanto cada coluna representa uma folha específica da taxonomia. A marcação com o símbolo ✓indica que determinado artigo aborda diretamente o tema correspondente, seja de forma conceitual, prática ou experimental. Essa sistematização visa facilitar a visualização da presença (ou ausência) de cada elemento ao longo do corpus analisado, evidenciando padrões de recorrência e apontando lacunas temáticas relevantes.

No que se refere ao eixo Tecnologia, observou-se uma ampla adoção de conceitos como IPv6, SDN, NFV e MEC, além de diferentes abordagens metodológicas de avaliação, como simulações específicas, testes em ambientes reais e análises descritivas. Esses resultados sugerem um foco significativo da literatura em aspectos estruturais e arquiteturais das redes, em especial no contexto da evolução das infraestruturas 5G.

Já no eixo Problemas de Segurança, a análise revelou maior ênfase em ameaças como *Vazamento de Dados*, *Privacidade*, *Disponibilidade* e ataques *DoS/DDoS*. Tais problemas refletem preocupações centrais na operação de redes heterogêneas e distribuídas, onde a integração de múltiplas tecnologias aumenta a superfície de ataque e a complexidade do gerenciamento seguro.

Por fim, o eixo Soluções apresenta a variedade de estratégias propostas para mitigar as vulnerabilidades identificadas. Dentre elas, destacam-se o uso de mecanismos criptográficos como *RSA* e *IPsec*, abordagens baseadas em *Blockchain*, aplicação de técnicas de *Inteligência Artificial* em sistemas de detecção de intrusão (IDS com IA), além da adoção de orquestrações dinâmicas e funções baseadas em SDN e NFV. Essa diversidade de soluções indica uma tendência da literatura em adotar abordagens combinadas e adaptativas, alinhadas à natureza dinâmica das

redes 5G.

Além de permitir a visualização organizada dos temas, essas tabelas funcionam como base empírica para os gráficos apresentados na próxima seção, os quais evidenciam as distribuições quantitativas da taxonomia. A partir dessa estrutura, torna-se possível observar tendências emergentes, identificar áreas pouco exploradas e fundamentar discussões sobre oportunidades de pesquisa futura no campo da segurança em redes 5G com IPv6.

O Quadro 8 apresenta a correspondência entre as citações utilizados ao longo do texto e os identificadores numéricos atribuídos a cada artigo nas tabelas de classificação (Ref. [1] a Ref. [29]). Essa padronização foi adotada para facilitar a leitura das tabelas taxonômicas, permitindo a rápida identificação dos artigos sem a necessidade de repetição dos dados completos de autoria.

Quadro 8 – Correspondência entre as citações no texto e suas respectivas referências numeradas.

Citação no texto	**Referência numerada**
Dutta e Hammad (2020)	Ref. [1]
Hu *et al.* (2022)	Ref. [2]
Bjerre *et al.* (2022)	Ref. [3]
Olimid e Nencioni (2020)	Ref. [4]
Sullivan *et al.* (2021)	Ref. [5]
Khan *et al.* (2019b)	Ref. [6]
Filsfils e Camarillo (2020)	Ref. [7]
Arfaoui *et al.* (2018)	Ref. [8]
Alwis *et al.* (2024)	Ref. [9]
Tang *et al.* (2022)	Ref. [10]
Batewela *et al.* (2025b)	Ref. [11]
Saleem *et al.* (2020)	Ref. [12]
Bánáti (2025)	Ref. [13]
Mohammed *et al.* (2023)	Ref. [14]
Hamroun *et al.* (2025)	Ref. [15]
Degefa *et al.* (2022)	Ref. [16]
Al-Shareeda e Manickam (2022)	Ref. [17]
Suomalainen *et al.* (2020)	Ref. [18]
Ahmad *et al.* (2018)	Ref. [19]
Gao *et al.* (2024)	Ref. [20]
Gupta *et al.* (2018)	Ref. [21]
Ahmad *et al.* (2019)	Ref. [22]
Salahdine *et al.* (2023)	Ref. [23]
Sethi *et al.* (2022)	Ref. [24]
Batewela *et al.* (2025a)	Ref. [25]
Oruma e Petrovic (2023)	Ref. [26]
Jover e Marojevic (2019)	Ref. [27]
Singh *et al.* (2024)	Ref. [28]
Ahmed *et al.* (2024)	Ref. [29]

Fonte: Elaborado pelo autor.

O Quadro 9 apresenta a classificação dos artigos em relação ao eixo "Tecnologia", conforme definido na taxonomia construída neste capítulo. As colunas da tabela representam os principais recursos, arquiteturas e abordagens tecnológicas discutidas nos estudos analisados, incluindo as variantes do 5G (*Standalone e Non-Standalone*), o uso do protocolo IPv6, integração com Internet das Coisas (IoT), computação de borda (MEC), técnicas como SDN e NFV, utilização do modelo *Dual Stack*, aplicação de *Network Slicing*, além dos tipos de avaliação empregados (simulações, experimentos em ambientes reais e análises teóricas ou descritivas).

Cada linha corresponde a um artigo identificado por sua referência numérica, e a presença do símbolo ✓indica que aquele trabalho aborda de maneira explícita o tema da coluna correspondente, seja de forma prática, conceitual ou experimental. Essa representação permite identificar padrões de adoção tecnológica na literatura, evidenciar quais soluções têm sido mais exploradas e apontar áreas com potencial para investigações futuras.

Quadro 9 – Eixo Tecnologia.

Referência	5G SA	5G NSA	IPv6	MEC	IoT Integrado	Network Slicing	SDN	NFV	Dual Stack	Simulador Específico	Ambiente Real	Teórica/ Descritiva
Ref. [1]	✓		✓	✓	✓		✓	✓			✓	
Ref. [2]	✓	✓	✓	✓	✓	✓	✓	✓			✓	
Ref. [3]	✓			✓	✓	✓	✓	✓				✓
Ref. [4]	✓		✓	✓	✓	✓				✓		
Ref. [5]	✓	✓	✓	✓	✓	✓	✓	✓				✓
Ref. [6]	✓		✓	✓								✓
Ref. [7]	✓		✓	✓		✓	✓	✓		✓	✓	
Ref. [8]	✓		✓	✓	✓					✓		
Ref. [9]	✓		✓		✓					✓		
Ref. [10]	✓		✓	✓	✓		✓	✓			✓	
Ref. [11]	✓		✓	✓		✓						
Ref. [12]	✓		✓	✓	✓		✓	✓				✓
Ref. [13]	✓		✓	✓	✓		✓	✓				✓
Ref. [14]	✓		✓	✓	✓							✓
Ref. [15]	✓		✓		✓							
Ref. [16]	✓		✓	✓	✓	✓	✓	✓		✓	✓	
Ref. [17]	✓		✓		✓		✓	✓		✓		
Ref. [18]	✓		✓		✓					✓		
Ref. [19]	✓		✓	✓	✓							✓
Ref. [20]	✓		✓			✓					✓	✓
Ref. [21]	✓		✓		✓		✓	✓	✓			✓
Ref. [22]	✓		✓	✓	✓	✓						✓
Ref. [23]	✓		✓	✓	✓		✓	✓			✓	
Ref. [24]	✓		✓	✓	✓	✓	✓	✓			✓	
Ref. [25]	✓		✓	✓	✓	✓	✓	✓			✓	
Ref. [26]	✓		✓		✓							✓
Ref. [27]	✓		✓									✓
Ref. [28]	✓		✓		✓	✓						✓
Ref. [29]	✓		✓	✓	✓	✓						✓

Fonte: Elaborado pelo autor.

O Quadro 10 classifica os artigos segundo os principais problemas de segurança em redes 5G com suporte ao protocolo IPv6. Este eixo da taxonomia reúne vulnerabilidades que afetam a confiabilidade, privacidade e integridade das comunicações.

As colunas representam categorias recorrentes de ameaças, como ataques DoS/DDoS, escuta não autorizada, falsificação de identidade, autenticação fraca, vazamento de dados, fragmentação na orquestração de serviços, entre outras.

Cada linha corresponde a um artigo da revisão, identificado pela referência. A marcação com ✓indica que o estudo aborda explicitamente o problema em questão.

Essa organização facilita a identificação das ameaças mais exploradas pela literatura e evidencia lacunas para pesquisas futuras.

Quadro 10 – Eixo Problemas de Segurança.

Referência	DoS/ DDoS	Eaves-dropping	Spoofing/ Hijacking	Autenticação Insegura	Vaz. de Dados	Orquest. Fragmentada	Priva-cidade	Disponi-bilidade	Integri-dade
Ref. [1]	✓	✓	✓			✓	✓	✓	
Ref. [2]	✓				✓	✓	✓	✓	
Ref. [3]	✓	✓				✓	✓	✓	
Ref. [4]	✓	✓		✓		✓	✓		
Ref. [5]	✓	✓	✓		✓	✓	✓	✓	
Ref. [6]			✓			✓		✓	
Ref. [7]	✓	✓	✓		✓	✓	✓	✓	
Ref. [8]	✓	✓	✓		✓	✓	✓		
Ref. [9]	✓		✓			✓		✓	
Ref. [10]	✓	✓	✓		✓	✓	✓		
Ref. [11]	✓	✓	✓			✓	✓	✓	✓
Ref. [12]	✓					✓		✓	
Ref. [13]	✓		✓		✓	✓	✓	✓	✓
Ref. [14]	✓					✓		✓	
Ref. [15]	✓	✓	✓			✓	✓	✓	
Ref. [16]	✓	✓	✓		✓	✓	✓		
Ref. [17]	✓					✓	✓		
Ref. [18]	✓		✓			✓			
Ref. [19]	✓				✓	✓	✓	✓	
Ref. [20]	✓	✓	✓	✓		✓	✓	✓	
Ref. [21]				✓		✓		✓	
Ref. [22]		✓			✓	✓	✓	✓	
Ref. [23]		✓				✓	✓	✓	
Ref. [24]						✓	✓	✓	
Ref. [25]				✓		✓	✓	✓	✓
Ref. [26]					✓	✓			
Ref. [27]				✓	✓	✓		✓	
Ref. [28]					✓	✓	✓	✓	
Ref. [29]					✓	✓	✓	✓	

Fonte: Elaborado pelo autor.

O Quadro 11 reúne as principais soluções propostas nos artigos para mitigar vulnerabilidades em redes 5G com suporte ao protocolo IPv6. As colunas representam diferentes

estratégias identificadas, como criptografia RSA, criptografia baseada em identidade, uso de IPsec, IDS com inteligência artificial, *blockchain*, orquestração dinâmica, soluções baseadas em SDN e mecanismos por função.

O símbolo ✓indica a presença da respectiva abordagem no artigo analisado, permitindo identificar as soluções mais adotadas na literatura revisada.

Quadro 11 – Eixo Solução.

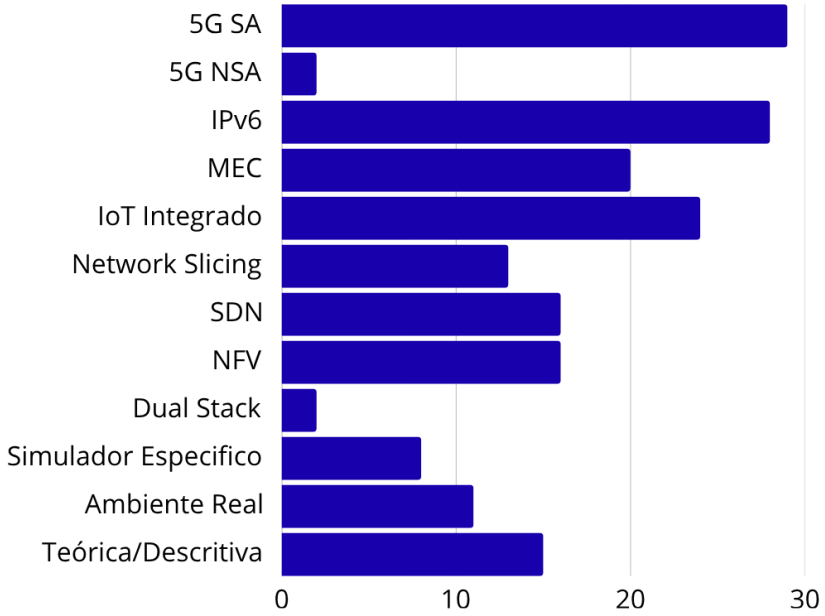
Referência	RSA	Baseada em Identidade	IPsec	IDS com IA	Blockchain	Orquestração Dinâmica	Baseado em SDN	Baseada em Função
Ref. [1]	✓			✓	✓		✓	
Ref. [2]	✓		✓	✓	✓		✓	
Ref. [3]	✓		✓	✓	✓	✓	✓	✓
Ref. [4]	✓		✓	✓				
Ref. [5]	✓			✓	✓		✓	
Ref. [6]		✓		✓	✓			
Ref. [7]				✓			✓	
Ref. [8]			✓	✓				
Ref. [9]				✓	✓			
Ref. [10]			✓	✓	✓		✓	
Ref. [11]				✓		✓	✓	✓
Ref. [12]				✓	✓		✓	
Ref. [13]				✓		✓	✓	
Ref. [14]		✓						
Ref. [15]	✓		✓	✓	✓	✓	✓	✓
Ref. [16]	✓		✓	✓	✓	✓	✓	
Ref. [17]								
Ref. [18]								
Ref. [19]								
Ref. [20]			✓				✓	
Ref. [21]								
Ref. [22]					✓	✓	✓	
Ref. [23]							✓	
Ref. [24]					✓		✓	
Ref. [25]					✓	✓	✓	✓
Ref. [26]								
Ref. [27]								
Ref. [28]								
Ref. [29]								

Fonte: Elaborado pelo autor.

5.6 Análise Visual da Taxonomia

A seguir, são apresentados gráficos que ilustram a distribuição e frequência das abordagens analisadas nos artigos revisados. Esses elementos visuais reforçam a compreensão da estrutura taxonômica e destacam as tendências mais recorrentes na literatura.

Figura 19 – Frequência de Ocorrência por Folha do Eixo "Tecnologia".

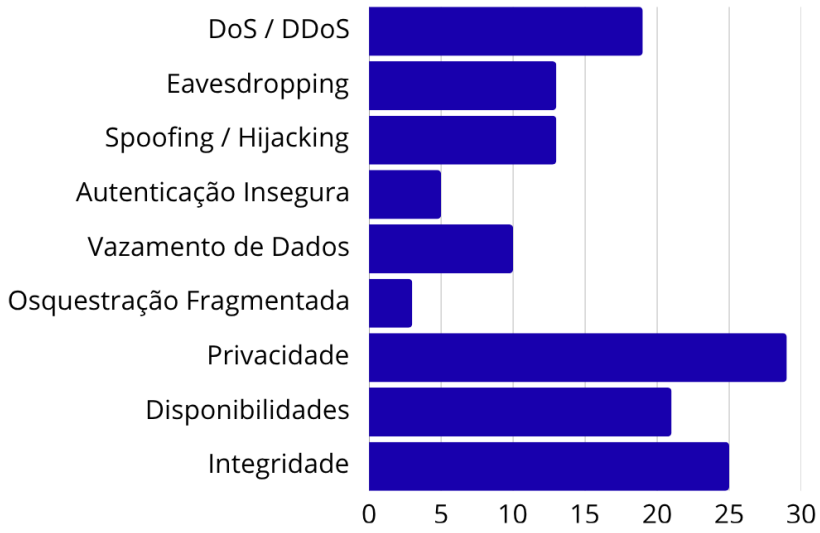


Fonte: Elaborada pelo autor.

A Figura 19 apresenta a distribuição de ocorrências por folha do eixo Tecnologia. Nota-se forte concentração em tecnologias amplamente exploradas como IPv6, 5G SA, IoT Integrado, SDN e NFV, refletindo o foco da literatura em arquitetura de redes modernas e virtualização. A presença da folha Teórica/Descritiva com destaque mostra a predominância de estudos conceituais. Já folhas como Ambiente Real e Simulador Específico aparecem com menor frequência, evidenciando a escassez de experimentações empíricas no domínio.

A Figura 20 mostra os dados referentes ao eixo Problemas de Segurança. Os principais destaques são Privacidade, Integridade, Disponibilidade e ataques como *DoS/DDoS* e *Spoofing*. Isso revela que os estudos se concentram nas ameaças clássicas da segurança da informação (CID), com menor atenção a vulnerabilidades mais específicas como Autenticação Insegura ou Orquestração Fragmentada, que ainda são pouco abordadas.

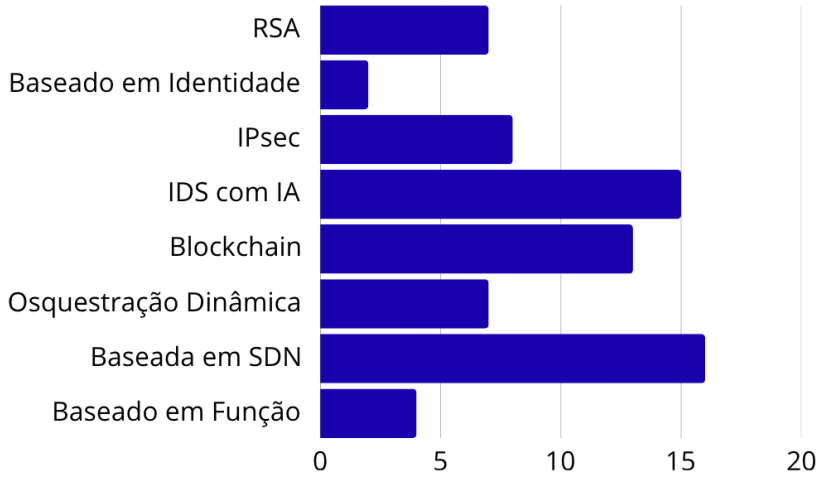
Figura 20 – Frequência de Ocorrência por Folha do Eixo "Problemas de Segurança".



Fonte: Elaborada pelo autor.

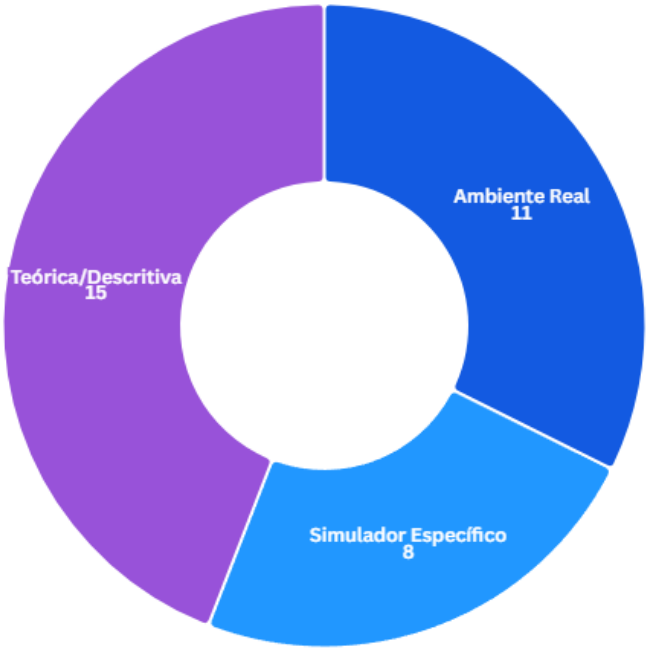
A Figura 21 representa o eixo Soluções, revelando maior presença de estratégias como IDS com IA, Baseado em SDN, *Blockchain* e Orquestração Dinâmica. Essas abordagens refletem a busca por soluções modernas e adaptativas frente às novas ameaças em ambientes distribuídos. Em contrapartida, há lacunas notáveis em soluções como Baseada em Identidade e Baseada em Função, além do uso ainda tímido de mecanismos como IPSec, o que aponta para oportunidades de pesquisas futuras nessas direções.

Figura 21 – Frequência de Ocorrência por Folha do Eixo "Soluções".



Fonte: Elaborada pelo autor.

Figura 22 – Classificação dos Métodos de Avaliação Utilizados nos Estudos.



Fonte: Elaborada pelo autor.

A Figura 22 ilustra a classificação metodológica dos artigos analisados, agrupando-os segundo o tipo de avaliação adotada: teórica ou descritiva, simulada e experimental. Essa análise permite compreender o nível de maturidade técnica e aplicabilidade das soluções propostas na literatura.

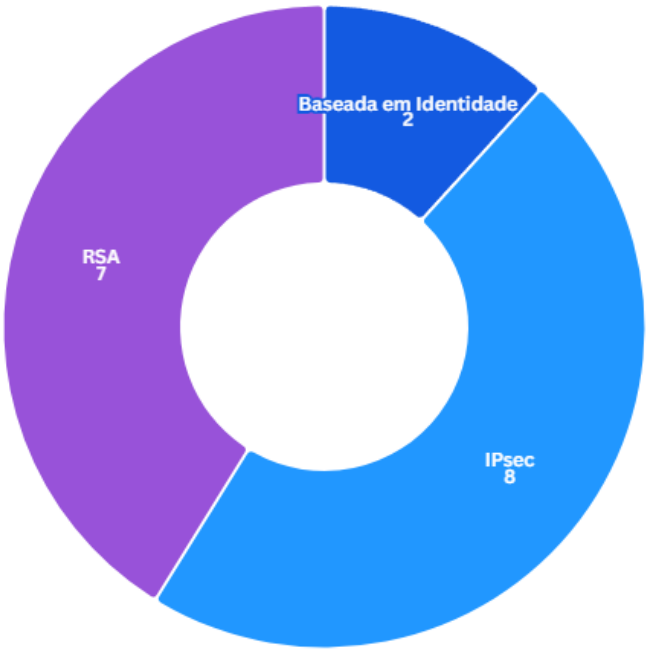
Verifica-se que a maioria dos trabalhos adota abordagens teóricas ou descritivas, totalizando 15 publicações que discutem problemas, propostas e estruturas conceituais sem a execução de experimentos ou simulações computacionais. Embora esse tipo de abordagem seja fundamental para a formação de fundamentos e taxonomias, ele também revela uma limitação quanto à validação prática das soluções.

Em seguida, destacam-se os estudos que realizaram testes em ambiente real (11 ocorrências), os quais apresentaram análises baseadas em dados reais, redes montadas em laboratório ou dispositivos físicos. Essa proporção é relevante, pois demonstra um esforço crescente em validar as propostas em condições mais próximas da realidade operacional.

Por fim, 8 artigos utilizaram simuladores específicos, como NS-3, OMNet++ ou ferramentas proprietárias, para reproduzir cenários de rede e testar o desempenho de mecanismos de segurança ou protocolos sob condições controladas. Esse tipo de avaliação representa um equilíbrio entre análise teórica e validação prática, permitindo testes em larga escala com menor custo.

A distribuição geral evidencia que, embora existam iniciativas de experimentação prática, a maior parte dos estudos ainda se concentra em análises descritivas, o que reforça a necessidade de mais pesquisas voltadas à implementação e à medição empírica em contextos reais.

Figura 23 – Distribuição das Estratégias Criptográficas Utilizadas.



Fonte: Elaborada pelo autor.

A Figura 23 apresenta a distribuição das estratégias criptográficas utilizadas nos artigos analisados. Este gráfico permite observar quais mecanismos de proteção de dados foram mais abordados na literatura voltada à segurança em redes 5G e IPv6.

A técnica mais presente foi o IPsec, com 8 ocorrências. Seu destaque está relacionado à compatibilidade com IPv6 e ao fato de ser um protocolo amplamente consolidado para autenticação e criptografia em nível de rede. A utilização do IPsec em contextos que envolvem mobilidade, segmentação e controle de tráfego demonstra sua relevância prática mesmo diante do surgimento de novas soluções.

A criptografia RSA aparece em seguida, com 7 ocorrências. Apesar de ser um algoritmo clássico, ainda é frequentemente empregado em propostas que envolvem autenticação de entidades, troca de chaves e proteção de sessões em ambientes distribuídos. Sua popularidade decorre da simplicidade de implementação e do suporte em diferentes camadas da pilha de protocolos.

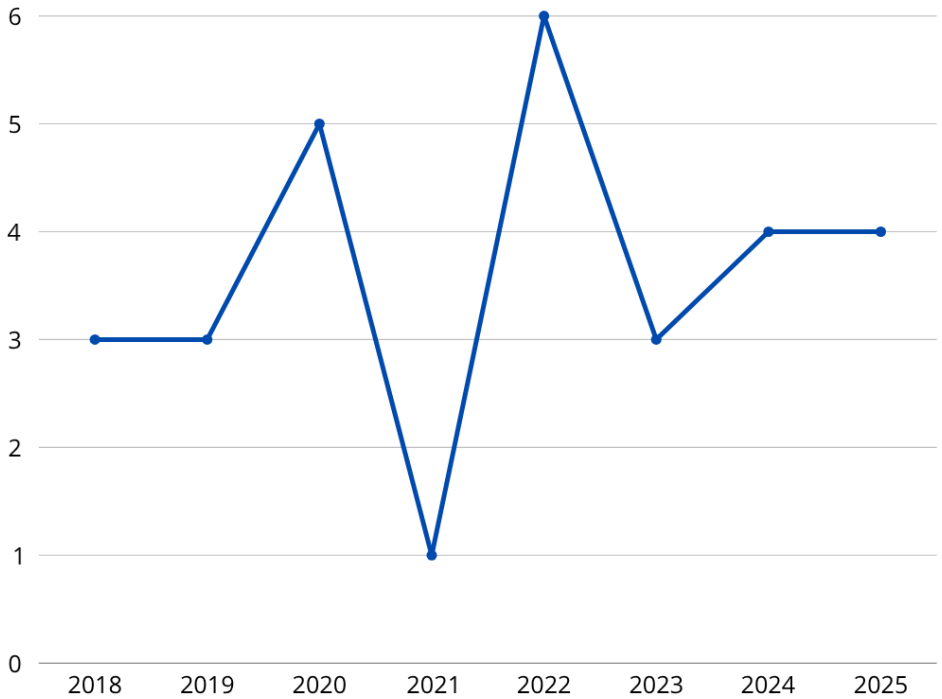
Por outro lado, a criptografia baseada em identidade foi mencionada apenas em 2 artigos, o que indica um nível de adoção ainda restrito. Esse tipo de abordagem apresenta vantagens em ambientes altamente dinâmicos, como redes veiculares ou IoT, por dispensar infraestrutura de chave pública convencional. No entanto, sua baixa representatividade na amostra analisada sugere que ainda há barreiras para sua aplicação prática em cenários 5G amplamente distribuídos.

De maneira geral, o gráfico evidencia uma predominância de soluções tradicionais e compatíveis com a arquitetura IP, ao passo que técnicas mais recentes, como aquelas baseadas em identidade, ainda não são amplamente exploradas no contexto de segurança para 5G e IPv6.

A Figura 24 apresenta a quantidade de artigos selecionados em cada ano do recorte temporal adotado (2018 a 2025). Este gráfico de linha reforça a análise cronológica da produção científica e permite identificar tendências de interesse da comunidade acadêmica sobre o tema segurança em redes 5G com IPv6.

Observa-se um crescimento considerável no ano de 2022, com um pico de seis artigos, o que pode estar relacionado ao amadurecimento das tecnologias 5G e ao aumento da adoção do IPv6 em ambientes produtivos. Após esse pico, a produção mantém-se relativamente estável, com leve oscilação, sugerindo que o tema permanece relevante e com interesse contínuo por parte da comunidade científica.

Figura 24 – Quantidade de Artigos Selecionados por Ano de Publicação.



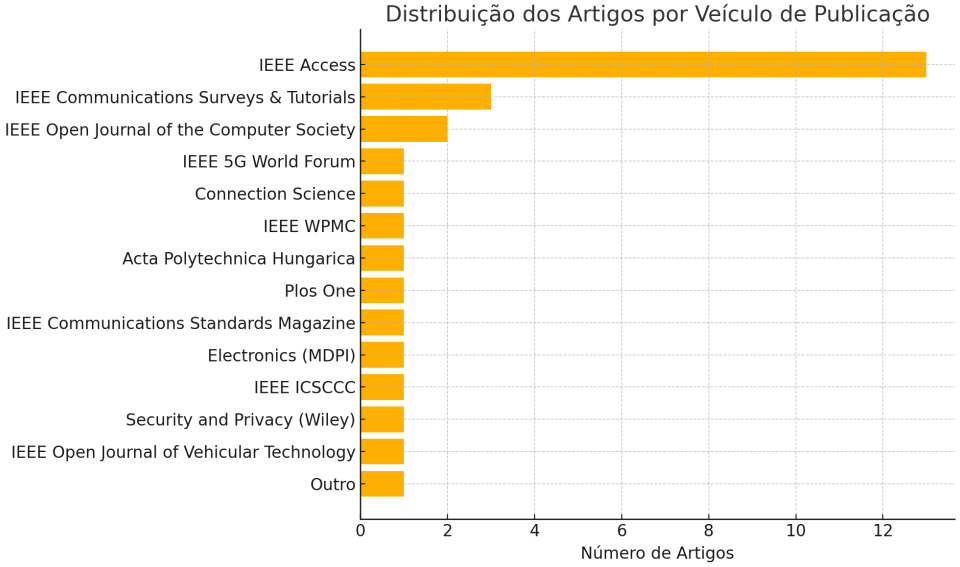
Fonte: Elaborada pelo autor.

A Figura 25 apresenta a distribuição dos 29 artigos selecionados nesta revisão segundo os veículos em que foram publicados. Observa-se uma predominância significativa da base *IEEE Access*, com 13 publicações, seguida por periódicos de alto fator de impacto como *IEEE Communications Surveys & Tutorials* (3 artigos) e periódicos de acesso aberto como *Electronics* (MDPI) e *Plos One*.

Conferências também tiveram participação relevante, como a *IEEE 5G World Forum*, o *IEEE WPMC* e o *ICSCCC*, que refletem a natureza emergente e dinâmica dos temas analisados, especialmente nos tópicos de segurança e arquitetura de redes móveis. Além disso, revistas multidisciplinares como a *Security and Privacy* (*Wiley*) e periódicos institucionais como o *IEEE Open Journal of the Computer Society* também marcaram presença.

Essa diversidade mostra que a discussão sobre segurança em redes 5G com IPv6 está sendo tratada tanto em espaços consolidados da engenharia elétrica quanto em fóruns emergentes e especializados em cibersegurança, redes veiculares e IoT. A predominância de veículos da IEEE também demonstra a centralidade da instituição nas publicações científicas sobre o tema.

Figura 25 – Distribuição dos Artigos Por Veículo de Publicação.



Fonte: Elaborada pelo autor.

5.7 Taxonomia Analítica

A constância de publicações nos anos de 2024 e 2025 indica que, mesmo após os primeiros anos de implantação do 5G, ainda há lacunas e desafios de segurança que motivam novas pesquisas. Isso confirma que a integração entre 5G e IPv6 continua sendo um campo fértil para investigações, especialmente diante da crescente demanda por conectividade segura em ambientes IoT e industriais.

Além disso, o gráfico evidencia que o período selecionado (2018-2025) abrange efetivamente o estágio de consolidação do 5G e a transição prática para o IPv6, justificando o recorte adotado na revisão sistemática.

A fim de aprofundar a análise dos artigos revisados, foi desenvolvida uma taxonomia analítica que busca identificar correlações entre os três eixos temáticos principais: tecnologias empregadas, ameaças de segurança abordadas e soluções propostas. Esta abordagem complementar à taxonomia funcional visa evidenciar não apenas a classificação, mas as relações de dependência e cobertura entre os elementos.

5.7.1 Tecnologias versus Ameaças

O Quadro 12 apresenta a associação entre as tecnologias analisadas e as ameaças de segurança abordadas nos artigos. Essa matriz permite observar quais tecnologias estão mais expostas a determinados vetores de ataque, contribuindo para o mapeamento de áreas críticas.

Quadro 12 – Relação entre Tecnologias e Ameaças.

Tecnologia	**DoS/DDoS**	**Eavesdropping**	**Spoofing**	**Hijacking**	**Autent. Insegura**
5G SA	✓	✓	✓	✓	✓
5G NSA	✓		✓		✓
IPv6	✓	✓	✓		✓
IoT Integrado	✓	✓		✓	✓
Network Slicing	✓			✓	✓
SDN	✓	✓	✓		
NFV	✓				
Dual Stack					✓
MEC	✓	✓			

Fonte: Elaborado pelo autor.

5.7.2 Soluções versus Ameaças Mitigadas

O Quadro 13 sintetiza as soluções propostas nos artigos e as respectivas ameaças que cada uma busca mitigar. A análise permite observar a abrangência e a eficácia de cada abordagem, além de evidenciar lacunas de cobertura.

Quadro 13 – Relação entre Soluções e Ameaças Mitigadas.

Solução	**DoS/DDoS**	**Eavesdropping**	**Spoofing**	**Hijacking**	**Autent. Insegura**
IDS com IA	✓			✓	
Blockchain	✓	✓			✓
RSA		✓	✓		✓
Baseada em Identidade			✓		✓
IPsec		✓	✓	✓	
Orquestração Dinâmica				✓	
Baseada em SDN	✓				
Baseada em Função				✓	

Fonte: Elaborado pelo autor.

5.8 Discussão

A presente seção discute criticamente os principais achados da taxonomia desenvolvida, buscando identificar tendências recorrentes, lacunas metodológicas e oportunidades futuras de pesquisa. A análise está dividida em três subseções: (i) análise da taxonomia funcional, (ii) análise da taxonomia analítica e (iii) discussão das ausências e implicações.

5.8.1 Análise da Taxonomia Descritiva

A taxonomia descritiva desenvolvida neste capítulo teve como objetivo estruturar e classificar, de forma sistemática, os principais aspectos técnicos, desafios de segurança e soluções identificadas na literatura recente sobre redes 5G e IPv6. A partir da análise dos artigos selecionados, foi possível observar tendências relevantes, lacunas conceituais e padrões metodológicos que contribuem para o entendimento do estado da arte na área.

A cobertura dos temas classificados demonstrou um predomínio do eixo Tecnologia. Folhas como IPv6, SDN, NFV, IDS com IA e Privacidade apresentaram os maiores volumes de marcações, indicando que os estudos revisados mantêm foco significativo nas camadas arquiteturais e em soluções automatizadas de detecção de anomalias. Essa concentração sugere uma maturidade crescente no tratamento técnico da segurança em redes emergentes, sobretudo

em ambientes com alto grau de heterogeneidade, como 5G, IoT e comunicações veiculares.

O eixo Problemas de Segurança também apresentou presença expressiva, com destaque para os requisitos de privacidade, integridade e disponibilidade. Esses dados reforçam que, apesar da ênfase técnica, há uma consciência clara na literatura sobre os impactos diretos que falhas de segurança podem causar em ambientes críticos e sensíveis a latência. Ainda assim, certos tipos de ameaça, como *spoofing/hijacking* e orquestração fragmentada, foram menos abordados, revelando espaços potenciais para pesquisas futuras.

No eixo Soluções, identificou-se a prevalência de mecanismos baseados em IA e abordagens distribuídas como *Blockchain*. Em contrapartida, soluções criptográficas tradicionais, como IPsec e algoritmos baseados em identidade, apresentaram baixa frequência, o que pode refletir tanto uma limitação de aplicabilidade quanto uma tendência a priorizar métodos mais flexíveis e adaptativos frente à dinâmica das redes modernas.

Do ponto de vista metodológico, observou-se que grande parte dos estudos adota avaliações teóricas ou simuladas, com menor incidência de validação em ambiente real. Essa característica sugere que a área ainda carece de experimentações empíricas mais robustas, capazes de comprovar a eficácia das propostas em cenários próximos da operação prática. A escassez de trabalhos com validação real também se reflete nas folhas menos recorrentes da taxonomia, como ambiente real, orquestração baseada em função e autenticação insegura.

Por fim, a estrutura da taxonomia permitiu não apenas classificar os temas centrais encontrados nos artigos, mas também evidenciar a interdependência entre os eixos. A literatura mais recente tende a tratar tecnologia, riscos e contramedidas de forma integrada, o que valida a proposta de organização taxonômica adotada neste trabalho. A partir dessa visão panorâmica, a discussão dos resultados contribui para a identificação de áreas já consolidadas e de pontos ainda pouco explorados, o que poderá orientar investigações futuras mais direcionadas.

O Quadro 14 apresenta uma síntese das tecnologias analisadas ao longo da taxonomia, relacionando-as com os principais problemas de segurança identificados e as soluções propostas nos estudos revisados. Esta consolidação permite visualizar de forma integrada os pontos de convergência entre os eixos discutidos.

A análise apresentada no Quadro 14 evidencia a forte correlação entre tecnologias emergentes, suas fragilidades inerentes e as soluções que vêm sendo propostas para mitigar riscos em redes 5G. Observa-se que mecanismos como SDN, NFV, MEC e *Network Slicing*, embora fundamentais para a escalabilidade e flexibilidade da infraestrutura, introduzem novas superfícies

de ataque, frequentemente associadas a vulnerabilidades em controle centralizado, orquestração insegura e isolamento deficiente entre funções. Em resposta, as abordagens mais recorrentes nos estudos analisados envolvem orquestração inteligente com suporte a ML, segmentação de rede baseada em políticas e mecanismos reforçados de autenticação e inspeção. Essa síntese confirma a interdependência crítica entre as dimensões tecnológicas, os desafios de segurança e as estratégias de defesa, reforçando a necessidade de soluções integradas e adaptativas desde as camadas de arquitetura até o gerenciamento dinâmico dos serviços.

Quadro 14 – Síntese de Tecnologias, Problemas Associados e Soluções Encontradas.

Tecnologia	**Problemas Relacionados**	**Soluções Encontradas**
5G SA	Vulnerabilidades em GTP e *slicing*	IPsec, segmentação por função
5G NSA	Hereditariedade de falhas do 4G	*Firewalls* virtuais
IPv6	*Spoofing*, *hijacking*, DoS no NDP	IPsec, inspeção ARP e DAI
MEC	Limitação de recursos, ataques na borda	IDS distribuído, orquestração adaptativa
SDN	Controle centralizado vulnerável, DoS	Monitoramento com IA, fortalecimento do controlador
NFV	Exposição de VNFs, orquestração insegura	Gerência de VNFs com IA, isolamento lógico
IoT	Baixa autenticação, vazamento de dados	Autenticação baseada em identidade, IBC
Network Slicing	Ataques *inter-slice*, falta de isolamento	Políticas de isolamento, *slicing* dinâmico seguro

Fonte: Elaborado pelo autor.

5.8.2 Análise da Taxonomia Analítica

A análise cruzada evidencia alguns padrões relevantes. Tecnologias como 5G SA, IPv6 e IoT Integrado aparecem frequentemente associadas a múltiplas ameaças, o que reflete sua adoção ampla e complexidade estrutural. Em contrapartida, tecnologias como NFV e *Dual Stack* aparecem pouco associadas a ameaças específicas, sugerindo uma lacuna na investigação sobre seus riscos.

No eixo das soluções, destaca-se a frequência de sistemas de detecção baseados em inteligência artificial (IDS com IA) e o uso de *blockchain*, refletindo uma tendência da literatura em empregar abordagens inteligentes e descentralizadas. No entanto, nota-se uma baixa recorrência de soluções baseadas em criptografia por identidade, apesar de seu potencial em cenários distribuídos. Essa ausência pode ser atribuída à complexidade de implementação ou ao pouco domínio da técnica na comunidade científica da área.

Outro ponto crítico identificado é a escassez de validação prática. Poucos artigos utilizaram testes em ambientes reais, limitando-se a simulações teóricas ou modelos conceituais. Isso reduz a confiabilidade das soluções frente a situações do mundo real, como mobilidade intensa, interferência de sinal e falhas de sincronização.

Dessa forma, os dados sugerem que, embora haja um esforço notável em investigar as vulnerabilidades e soluções na integração entre 5G e IPv6, ainda existem lacunas importantes a serem exploradas, tanto no aprofundamento de certas tecnologias quanto na experimentação empírica. Como pesquisador, entende-se que o avanço da área dependerá cada vez mais da combinação entre inovação conceitual e validação prática, em cenários heterogêneos e de alta demanda como os previstos para redes 5G e além.

5.8.3 Lacunas, Frequências e Implicações

A análise taxonômica dos 29 artigos revisados revela não apenas as áreas mais exploradas na literatura sobre segurança em redes 5G e IPv6, mas também lacunas significativas que merecem atenção. Algumas folhas da taxonomia apresentaram baixa frequência ou mesmo ausência, o que levanta questionamentos relevantes sobre as escolhas metodológicas e os focos predominantes da comunidade científica.

Um dos pontos mais notáveis foi a baixa presença de estudos sobre criptografia baseada em identidade (IBC - *Identity-Based Cryptography*). Apesar de essa abordagem ser considerada promissora por simplificar o gerenciamento de chaves públicas em ambientes altamente distribuídos como IoT e redes 5G, poucos artigos a abordaram de forma central. Esta ausência pode ser explicada por alguns fatores: a complexidade da implementação prática da IBC, sua menor compatibilidade com padrões amplamente consolidados como PKI, e a escassez de *frameworks* maduros que facilitem sua integração em redes comerciais. Além disso, muitos autores parecem privilegiar soluções mais generalistas, como RSA e IPsec, ainda que estas nem sempre sejam ideais para cenários móveis ou de borda.

Outro aspecto crítico diz respeito à escassez de validações em ambientes reais. A maioria das propostas analisadas foi testada em simuladores personalizados ou discutida de forma teórica/descritiva. A presença limitada da folha “Ambiente Real” evidencia um distanciamento entre a pesquisa acadêmica e os cenários operacionais concretos. Isso pode decorrer de limitações de acesso a infraestruturas 5G reais, alto custo de experimentação e dificuldades de replicabilidade em ambientes produtivos. No entanto, essa lacuna compromete a generalização dos resultados e

destaca a necessidade de mais iniciativas colaborativas entre universidades, operadoras e centros de testes.

Além disso, folhas como “Orquestração Fragmentada”, “Baseada em Função” e “Autenticação Insegura” também apresentaram baixas marcações. Tais temas dizem respeito a falhas emergentes da arquitetura modular e à fragilidade dos mecanismos de coordenação entre funções virtuais e físicas. A pouca atenção dada a esses aspectos pode refletir tanto a dificuldade de mensuração empírica dessas vulnerabilidades quanto uma tendência da literatura a priorizar soluções propositivas em detrimento da exploração de falhas existentes. Do ponto de vista do pesquisador, é preocupante que aspectos como orquestração e autenticação - pilares da segurança em redes segmentadas e dinâmicas - ainda careçam de estudos aprofundados.

Por fim, a concentração elevada em folhas como SDN, NFV, IDS com IA e Privacidade demonstra uma convergência dos esforços científicos em torno de soluções automatizadas, inteligentes e centradas na infraestrutura. Embora essa ênfase seja justificável dada a criticidade dessas tecnologias no contexto 5G, o desequilíbrio observado entre os temas indica que ainda há um campo fértil de investigação pouco explorado, sobretudo no que tange à resiliência operacional, interoperabilidade prática e mensuração empírica de eficácia em contextos reais.

A reflexão crítica sobre essas ausências e concentrações reforça a importância de abordagens mais amplas e experimentais, bem como da diversificação temática nas futuras pesquisas. Cabe à comunidade científica buscar esse equilíbrio, promovendo avanços não apenas teóricos, mas também práticos e validados.

5.8.4 Discussões Técnicas Específicas

Além da análise geral dos eixos da taxonomia, algumas fragilidades técnicas observadas na literatura merecem destaque, tanto por sua recorrência quanto por seus impactos práticos.

5.8.4.1 Orquestração Fragmentada Como Risco Real

A orquestração fragmentada ocorre quando não há um mecanismo centralizado, coerente e seguro de gerenciamento dos recursos virtuais e serviços distribuídos - especialmente em ambientes com *Network Slicing*, NFV e MEC. Essa fragmentação pode levar à exposição de interfaces não monitoradas, inconsistência na aplicação de políticas de segurança e falhas na segmentação de tráfego entre domínios. Como apontado por diversos autores, esse tipo de

desorganização na infraestrutura de orquestração favorece ataques laterais, vazamentos de dados e dificuldade de resposta a incidentes.

5.8.4.2 Limitações do IPsec em Ambientes Complexos

Embora o IPsec seja uma das soluções criptográficas mais consolidadas para prover confidencialidade e integridade no tráfego de rede, ele não é capaz de mitigar por si só ataques baseados em autenticação fraca ou comprometida. Isso porque o *handshake* inicial e a distribuição de chaves ainda dependem de mecanismos auxiliares, que muitas vezes são vulneráveis, especialmente em dispositivos com pouca capacidade de processamento, como sensores IoT. Além disso, o IPsec não previne vazamentos de dados originados em camadas superiores, como aplicações ou sistemas operacionais mal configurados.

5.8.4.3 Fortalecimento do Controlador SDN Contra DoS e Injeção de Regras

O controlador SDN, por concentrar a lógica de decisão da rede, é alvo crítico para ataques como DoS ou injeção de regras maliciosas. A literatura aponta várias estratégias de mitigação, entre elas:

- Monitoramento contínuo com apoio de IA, permitindo a detecção de fluxos anômalos em tempo real;
- Mecanismos de autenticação mútua entre controlador e *switches*, impedindo o envenenamento da tabela de regras;
- Limitação da taxa de mensagens *Packet_In* por origem, reduzindo a superfície de ataque por sobrecarga;
- Segmentação do plano de controle com replicação redundante do controlador.

Esses mecanismos reforçam a resiliência da infraestrutura SDN e têm sido recomendados como boas práticas nos estudos mais recentes, especialmente em ambientes críticos como redes 5G autônomas.

5.9 Respostas às Perguntas de Pesquisa

Nesta seção, apresentam-se as respostas às Perguntas de Pesquisa (PPx), conforme definidas no protocolo da revisão sistemática construído na ferramenta *Parsifal*. Cada resposta foi elaborada com base nas análises realizadas ao longo do capítulo anterior, que incluem

tanto a taxonomia funcional quanto a taxonomia analítica, além das discussões qualitativas correspondentes. O objetivo é fornecer uma síntese estruturada e fundamentada que atenda aos objetivos propostos por meio das perguntas norteadoras da investigação.

5.9.1 PP1: Quais são as principais vulnerabilidades de segurança associadas à integração entre 5G e IPv6?

A análise dos artigos revelou que as principais vulnerabilidades decorrem da combinação entre as especificidades do protocolo IPv6 e a complexidade arquitetural das redes 5G. Entre os problemas mais recorrentes estão:

- **Ataques ao protocolo IPv6**, como *spoofing*, *hijacking* e DoS via NDP;
- **Falhas de autenticação**, incluindo a ausência de mecanismos robustos em dispositivos IoT e no acesso à rede;
- **Orquestração fragmentada**, que compromete o isolamento entre funções e fatias de rede (*slices*);
- **Vazamento de dados** e violação de privacidade, especialmente em ambientes com mobilidade e heterogeneidade elevada;
- **Ausência de isolamento em *slices***, tornando o *network slicing* suscetível a ataques *inter-slice*.

Essas vulnerabilidades foram mapeadas na taxonomia descritiva (Seção 5.1) e sintetizadas no Quadro 14, evidenciando padrões recorrentes na literatura.

5.9.2 PP2: Quais são as soluções mais eficazes propostas na literatura para mitigar as vulnerabilidades de segurança em redes que integram 5G e IPv6?

As soluções mais frequentemente propostas envolvem mecanismos inteligentes e técnicas de segmentação adaptativa. Dentre elas, destacam-se:

- **IDS com IA**, utilizados tanto no núcleo quanto nas bordas da rede;
- ***Blockchain***, aplicado em contextos de autenticação e rastreabilidade;
- **Criptografia IPsec**, ainda que com uso limitado e pouca presença em estudos mais recentes;
- **Orquestração baseada em SDN ou em função**, para isolar funções críticas e mitigar vulnerabilidades estruturais;
- **Políticas de *slicing* dinâmico**, para garantir maior controle e resiliência no provisiona-

mento de serviços.

O Quadro 14 relaciona essas soluções às respectivas tecnologias e problemas que elas visam mitigar, enquanto a discussão crítica (Seção 5.8) analisa suas limitações e aplicabilidades práticas.

5.9.3 PP3: Quais lacunas de pesquisa e problemas em aberto ainda persistem na segurança de redes que integram 5G e IPv6?

A revisão sistemática permitiu identificar diversas lacunas relevantes na literatura:

- **Baixa presença de testes em ambientes reais**, o que compromete a validação prática das soluções propostas;
- **Pouca exploração de criptografia baseada em identidade (IBC)**, apesar de seu potencial para cenários distribuídos e IoT;
- **Escassez de estudos aplicados à orquestração segura**, especialmente no contexto de NFV e *slicing*;
- **Carência de abordagens integradas que tratem tecnologia, ameaça e mitigação de forma conjunta**;
- **Limitações no uso de métricas padronizadas de avaliação**, dificultando a comparação entre soluções.

Essas lacunas são discutidas em detalhes na Subseção 5.8.3, que analisa tanto as ausências nas folhas da taxonomia quanto as tendências metodológicas observadas nos artigos.

6 DESAFIOS E DIREÇÕES FUTURAS

O levantamento realizado neste trabalho evidenciou que, embora as soluções de segurança para redes 5G/IPv6 apresentem avanços significativos, ainda persistem desafios críticos relacionados à arquitetura, validação prática e integração de tecnologias emergentes.

6.1 Segurança no Plano de Controle das Redes 5G

Um dos desafios recorrentes está na proteção do plano de controle das redes 5G, especialmente frente ao uso extensivo de SDN e NFV. A centralização do controle, embora ofereça vantagens de gerenciamento, também representa um ponto único de falha. Esse problema é destacado em diversos estudos revisados, que apontam a vulnerabilidade das arquiteturas centradas em controladores únicos (Dutta; Hammad, 2020; Tang *et al.*, 2022). Estudos futuros devem explorar formas de descentralizar o controle sem comprometer a eficiência e a orquestração das redes.

6.2 Limitações na Integração de Tecnologias Emergentes

Embora tecnologias como *Blockchain* e IA já tenham sido aplicadas em alguns trabalhos, sua integração com as camadas de comunicação e segurança ainda é incipiente. Os artigos analisados demonstram que essas abordagens, quando presentes, aparecem de forma isolada ou em estágios conceituais (Khan *et al.*, 2019b; Ahmad *et al.*, 2018). Há carência de modelos unificados que combinem essas tecnologias de forma coesa, interoperável e escalável em ambientes heterogêneos como redes móveis, IoT e sistemas veiculares.

6.3 Validação em Ambientes Reais e Reprodutibilidade

A predominância de abordagens teóricas e simulações foi evidenciada nas tabelas e gráficos apresentados. Poucos artigos realizam experimentos em ambiente real, o que limita a comprovação da eficácia prática das soluções propostas (Bjerre *et al.*, 2022; Gupta *et al.*, 2018). Além disso, a literatura analisada raramente oferece conjuntos de dados, configurações de rede ou ferramentas reprodutíveis, dificultando a verificação de resultados por outros pesquisadores. Essa limitação compromete a transparência científica e a replicabilidade das propostas.

6.4 Ausência de Padrões para Orquestração Segura

A literatura mostra múltiplas abordagens para orquestração de políticas de segurança, mas ainda sem consenso sobre modelos padronizados. Trabalhos distintos propõem mecanismos de orquestração baseados em SDN, segmentação ou controle por domínio, mas carecem de integração e compatibilidade (Batewela *et al.*, 2025b; Batewela *et al.*, 2025a). A fragmentação de decisões e a coexistência de múltiplas camadas de controle geram vulnerabilidades e inconsistências entre domínios. Investigações futuras podem se concentrar na construção de estruturas normativas e interoperáveis para ambientes fatiados e *multitenant*.

6.5 Fragmentação das Estratégias Criptográficas

As soluções criptográficas abordadas nos trabalhos revisados ainda são restritas em diversidade e profundidade. Técnicas tradicionais, como RSA e IPsec, são exploradas com maior frequência (Saleem *et al.*, 2020; Degefa *et al.*, 2022), enquanto abordagens mais recentes, como criptografia baseada em identidade, *Blockchain* e criptografia leve, aparecem de forma pontual e, em sua maioria, sem integração com os mecanismos de controle e orquestração da rede.

6.6 Perspectivas para Futuras Pesquisas

Considerando os desafios analisados, são recomendadas as seguintes direções para pesquisas futuras:

- Desenvolvimento de *frameworks* modulares de segurança aplicáveis a ambientes 5G/IPv6 integrados com IoT;
- Avaliação comparativa de protocolos de orquestração sob cenários adversos;
- Aplicação de aprendizado de máquina para orquestração autônoma e reconfiguração dinâmica;
- Criação de ambientes de teste controlados e reprodutíveis para validação de soluções de segurança;
- Integração de métricas de desempenho e confiabilidade nos processos de tomada de decisão em segurança.

Diante dos desafios apresentados, é possível concluir que o campo da segurança em redes 5G e IPv6 permanece em consolidação, especialmente no que se refere à integração entre tecnologias emergentes, padronização de soluções e validação prática das propostas. A

análise dos artigos selecionados evidenciou que, embora exista uma produção científica crescente e diversificada, ainda são necessários esforços adicionais para transpor as soluções do nível conceitual para aplicações robustas em cenários reais (Khan *et al.*, 2019b; Tang *et al.*, 2022; Batewela *et al.*, 2025a).

Ao mapear essas lacunas, esta pesquisa oferece subsídios relevantes para futuros trabalhos que busquem aprofundar aspectos críticos como orquestração segura, reprodutibilidade de experimentos e adaptação dinâmica de estratégias de proteção. A superação dos obstáculos identificados será fundamental para garantir a segurança, a confiabilidade e a escalabilidade das redes de próxima geração, especialmente diante do aumento da complexidade e heterogeneidade dos ambientes conectados.

7 CONCLUSÃO

Este trabalho teve como objetivo investigar os desafios de segurança decorrentes da integração entre redes móveis de quinta geração (5G) e o protocolo IPv6, por meio de uma revisão sistemática da literatura. A motivação central reside no fato de que a convergência entre essas duas tecnologias, embora necessária para atender à crescente demanda por conectividade, amplia significativamente a superfície de ataque das redes futuras.

Com base em critérios rigorosos de inclusão e exclusão, foram selecionados 29 artigos científicos que abordam, de forma direta ou indireta, aspectos de segurança nessa integração. Esses artigos foram analisados com apoio de uma taxonomia descritiva estruturada em três eixos: Tecnologias, Problemas de Segurança e Soluções Propostas. Essa estrutura possibilitou a categorização precisa dos temas abordados e a identificação de tendências, lacunas e padrões recorrentes na literatura.

A seguir, foi elaborada uma segunda taxonomia, de natureza analítica, com o intuito de estabelecer correlações entre tecnologias, ameaças e contramedidas. Essa abordagem relacional permitiu uma compreensão mais aprofundada das interdependências entre os elementos, oferecendo uma visão integrada dos desafios enfrentados pela comunidade científica.

Os principais achados indicam que tecnologias como SDN, NFV, IoT Integrado e *Network Slicing* são recorrentes nos estudos analisados, tanto como facilitadoras da arquitetura 5G quanto como fontes de novas vulnerabilidades. Soluções como IDS com Inteligência Artificial e *Blockchain* foram frequentemente propostas como estratégias de mitigação. No entanto, observou-se a baixa presença de estudos que explorem criptografia baseada em identidade, bem como a escassez de validações em ambientes reais.

Além da construção das taxonomias, o trabalho também respondeu de forma direta às perguntas de pesquisa previamente definidas no protocolo, utilizando os achados das análises e a discussão crítica para fundamentar as respostas. Foram ainda discutidas as lacunas temáticas mais relevantes, como orquestração fragmentada, falhas de autenticação e insuficiência de mecanismos de isolamento de funções.

A principal contribuição deste trabalho consiste na sistematização do conhecimento atual sobre segurança na convergência entre 5G e IPv6, por meio de uma taxonomia dupla (descritiva e analítica) e de uma discussão técnica aprofundada sobre tendências, fragilidades e oportunidades de pesquisa. Metodologicamente, a utilização da ferramenta *Parsifal* garantiu transparência, rastreabilidade e reprodutibilidade ao processo de revisão.

Espera-se que esta pesquisa possa subsidiar pesquisadores, profissionais e formuladores de políticas no desenvolvimento de soluções mais eficazes, integradas e empiricamente validadas para redes seguras de próxima geração.

REFERÊNCIAS

AHMAD, I.; KUMAR, T.; LIYANAGE, M.; OKWUIBE, J.; YLIANTTILA, M.; GURTOV, A. Overview of 5g security challenges and solutions. **IEEE Communications Standards Magazine**, v. 2, n. 1, p. 36–43, 2018.

AHMAD, I.; SHAHABUDDIN, S.; KUMAR, T.; OKWUIBE, J.; GURTOV, A.; YLIANTTILA, M. Security for 5g and beyond. **IEEE Communications Surveys Tutorials**, v. 21, n. 4, p. 3682–3722, 2019.

AHMED, S. F.; ALAM, M. S. B.; AFRIN, S.; RAFA, S. J.; TAHER, S. B.; KABIR, M.; MUYEEN, S. M.; GANDOMI, A. H. Toward a secure 5g-enabled internet of things: A survey on requirements, privacy, security, challenges, and opportunities. **IEEE Access**, v. 12, p. 13125–13145, 2024.

AL-SHAREEDA, M. A.; MANICKAM, S. Msr-dos: Modular square root-based scheme to resist denial of service (dos) attacks in 5g-enabled vehicular networks. **IEEE Access**, v. 10, p. 120606–120615, 2022.

ALWIS, C. D.; PORAMBAGE, P.; DEV, K.; GADEKALLU, T. R.; LIYANAGE, M. A survey on network slicing security: Attacks, challenges, solutions and research directions. **IEEE Communications Surveys Tutorials**, v. 26, n. 1, p. 534–570, 2024.

ARFAOUI, G.; BISSON, P.; BLOM, R.; BORGAONKAR, R.; ENGLUND, H.; FéLIX, E.; KLAEDTKE, F.; NAKARMI, P. K.; NäSLUND, M.; O'HANLON, P.; PAPAY, J.; SUOMALAINEN, J.; SURRIDGE, M.; WARY, J.-P.; ZAHARIEV, A. A security architecture for 5g networks. **IEEE Access**, v. 6, p. 22466–22479, 2018.

ARKKO, J.; NIKANDER, P. Limitations of ipsec policy mechanisms. In: SPRINGER. **International Workshop on Security Protocols**. [*S. l.*], 2003. p. 241–251.

BÁNÁTI, A. Developing security information and events management use cases for 5g specific vulnerabilities and attacks. **Acta Polytechnica Hungarica**, v. 22, n. 2, 2025.

BATEWELA, S.; LIYANAGE, M.; ZEYDAN, E.; YLIANTTILA, M.; RANAWEERA, P. Security orchestration in 5g and beyond smart network technologies. **IEEE Open Journal of the Computer Society**, v. 6, p. 554–573, 2025.

BATEWELA, S.; RANAWEERA, P.; LIYANAGE, M.; ZEYDAN, E.; YLIANTTILA, M. Addressing security orchestration challenges in next-generation networks: A comprehensive overview. **IEEE Open Journal of the Computer Society**, p. 1–20, 2025.

BJERRE, S. A.; BLOMSTERBERG, M. W. K.; ANDERSEN, B. 5g attacks and countermeasures. In: IEEE. **2022 25th International Symposium on Wireless Personal Multimedia Communications (WPMC)**. [*S. l.*], 2022. p. 285–290.

BRITO, S. H. B. **Autoconfiguração de Endereços IPv6 (SLAAC)**. 2013. Disponível em: http://labcisco.blogspot.com.br/2013/05/autoconfiguracao-de-enderecosipv6-slaac.html. Acesso em: 29 ajan. 2025.

CALDAS, B. **IPSec - Introdução**. 2014. Disponível em: https://abcsec.wordpress.com/2014/03/30/ipsec-introducao/. Acesso em: 29 abr. 2025.

CAO, J.; MA, M.; LI, H.; MA, R.; SUN, Y.; YU, P.; XIONG, L. A survey on security aspects for 3gpp 5g networks. **IEEE communications surveys & tutorials**, IEEE, v. 22, n. 1, p. 170–195, 2019.

COMER, D. E. **Redes de computadores e internet-6**. [*S. l.*]: Bookman Editora, 2016.

Crypto.com University. **O que são contratos inteligentes e como funcionam?** 2023. Disponível em: https://crypto.com/pt/university/smart-contracts. Acesso em: 22 jun. 2025.

DEERING, D. S. E.; HINDEN, B. **Internet Protocol, Version 6 (IPv6) Specification**. RFC Editor, 2017. RFC 8200. (Request for Comments, 8200). Disponível em: https://www.rfc-editor.org/info/rfc8200. Acesso em: 20 abr. 2025.

DEGEFA, F.; RYU, J.; KIM, H.; WON, D. Mes-fpmipv6: Mih-enabled and enhanced secure fast proxy mobile ipv6 handover protocol for 5g networks. **Plos one**, Public Library of Science San Francisco, CA USA, v. 17, n. 5, p. e0262696, 2022.

DUTTA, A.; HAMMAD, E. 5g security challenges and opportunities: A system approach. In: IEEE. **2020 IEEE 3rd 5G world forum (5GWF)**. [*S. l.*], 2020. p. 109–114.

FILSFILS, C.; CAMARILLO, P. **ASIC-FRIENDLY SRV6-BASED SD-WAN SERVICE THEFT PREVENTION MECHANISM**. 2020. Technical Disclosure Commons. Disponível em: https://www.tdcommons.org/dpubs_series/2934. Acesso em: 6 fev. 2025.

GAO, S.; LIN, R.; FU, Y.; LI, H.; CAO, J. Security threats, requirements and recommendations on creating 5g network slicing system: A survey. **Electronics**, MDPI, v. 13, n. 10, p. 1860, 2024.

GUPTA, S.; PARNE, B. L.; CHAUDHARI, N. S. Security vulnerabilities in handover authentication mechanism of 5g network. In: **2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)**. [*S. l.*: *s. n.*], 2018. p. 369–374.

HAMROUN, C.; FLADENMULLER, A.; PARIENTE, M.; PUJOLLE, G. Intrusion detection in 5g and wi-fi networks: A survey of current methods, challenges, and perspectives. **IEEE Access**, v. 13, p. 40950–40976, 2025.

HU, J.; LIANG, W.; HOSAM, O.; HSIEH, M.-Y.; SU, X. 5gss: A framework for 5g-secure-smart healthcare monitoring. **Connection Science**, Taylor & Francis, v. 34, n. 1, p. 139–161, 2022.

HUMAYUN, M.; HAMID, B.; JHANJHI, N.; SUSEENDRAN, G.; TALIB, M. 5g network security issues, challenges, opportunities and future directions: A survey. In: IOP PUBLISHING. **Journal of Physics: Conference Series**. [*S. l.*], 2021. v. 1979, n. 1, p. 012037.

IPV6.BR. **IPv6**: cabeçalho. NIC.br (Núcleo de Informação e Coordenação do Ponto BR), 2012. Disponível em: http://ipv6.br/post/cabecalho/. Acesso em: 30 jan. 2025.

IPV6.BR. **IPv6**: endereçamento. NIC.br (Núcleo de Informação e Coordenação do Ponto BR), 2012. Disponível em: http://ipv6.br/post/enderecamento/. Acesso em: 29 jan. 2025.

JANKIEWICZ, E.; NARTEN, D. T.; LOUGHNEY, J. A. **IPv6 Node Requirements**. RFC Editor, 2011. RFC 6434. (Request for Comments, 6434). Disponível em: https://www.rfc-editor.org/info/rfc6434. Acesso em: 14 mai. 2025.

JOVER, R. P.; MAROJEVIC, V. Security and protocol exploit analysis of the 5g specifications. **IEEE Access**, v. 7, p. 24956–24963, 2019.

JÚNIOR, L. G.; SOUZA, J.; NUNES, R. M.; BOGO, M. Análise da segurança em redes puramente ipv6. **VII ENCONTRO DE ESTUDANTES DE INFORMÁTICA DO ESTADO DO TOCANTINS**, 2005.

KHAN, R.; KUMAR, P.; JAYAKODY, D. N. K.; LIYANAGE, M. A survey on security and privacy of 5g technologies. **IEEE Communications Surveys & Tutorials**, IEEE, v. 22, n. 1, p. 196–248, 2019.

KHAN, R.; KUMAR, P.; JAYAKODY, D. N. K.; LIYANAGE, M. A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions. **IEEE Communications Surveys & Tutorials**, IEEE, v. 22, n. 1, p. 196–248, 2019.

KIM, D.; ZARRI, M. Road to 5g: Introduction and migration. **White Paper**, 2018.

KITCHENHAM, B. Procedures for performing systematic reviews. **Keele, UK, Keele University**, Citeseer, v. 33, n. 2004, p. 1–26, 2004.

KITCHENHAM, B.; BRERETON, O. P.; BUDGEN, D.; TURNER, M.; BAILEY, J.; LINKMAN, S. Systematic literature reviews in software engineering–a systematic literature review. **Information and software technology**, Elsevier, v. 51, n. 1, p. 7–15, 2009.

LIMA, M. A. C. d. **Garantia de qualidade de serviço com 5G priorizando aplicações de missão crítica**. Trabalho de Conclusão de Curso (Graduação), IF Goiano, Instituto Federal Goiano, 2022. Bacharelado em Sistemas de Informação. Disponível em: https://repositorio.ifgoiano.edu.br/handle/prefix/2317. Acesso em: 6 ago. 2025.

LIU, N.; XIA, J.; CAI, Z.; YANG, T.; HOU, B.; WANG, Z. A survey on ipv6 security threats and defense mechanisms. In: SUN, X.; ZHANG, X.; XIA, Z.; BERTINO, E. (Ed.). **Artificial Intelligence and Security**. Cham: Springer International Publishing, 2022. p. 583–598. ISBN 978-3-031-06794-5.

MENDES, H. F. d. S. Trabalho de Conclusão de Curso (Bacharelado em Engenharia de Telecomunicações), **Abordagem teórica da aplicação de virtualização de funções de rede na tecnologia de comunicação 5G**. Niterói, RJ: [*S. n.*], 2019. 64f.

MOHAMMED, B. A.; AL-SHAREEDA, M. A.; MANICKAM, S.; AL-MEKHLAFI, Z. G.; ALRESHIDI, A.; ALAZMI, M.; ALSHUDUKHI, J. S.; ALSAFFAR, M. Fc-pa: Fog computing-based pseudonym authentication scheme in 5g-enabled vehicular networks. **IEEE Access**, v. 11, p. 18571–18581, 2023.

MOREIRA, M. M. 5g–evolução, mimo massivo, beamforming e formas de onda. **Repositório Institucional da Universidade Federal Fluminense**, v. 1, p. 01–72, 2018.

OLIMID, R. F.; NENCIONI, G. 5g network slicing: A security overview. **IEEE Access**, v. 8, p. 99999–100009, 2020.

OLIVEIRA, L. A.; ALENCAR, M. S.; LOPES, W. T. A. Evolução da arquitetura de redes móveis rumo ao 5g. **Revista de Tecnologia da Informação e Comunicação**, v. 8, n. 2, p. 43–50, 2018.

ORUMA, S. O.; PETROVIC, S. Security threats to 5g networks for social robots in public spaces: A survey. **IEEE Access**, v. 11, p. 63205–63237, 2023.

PARK, J. H.; RATHORE, S.; SINGH, S. K.; SALIM, M. M.; AZZAOUI, A.; KIM, T. W.; PAN, Y.; PARK, J. H. A comprehensive survey on core technologies and services for 5g security: Taxonomies, issues, and solutions. **Hum.-Centric Comput. Inf. Sci**, v. 11, n. 3, 2021.

SALAHDINE, F.; HAN, T.; ZHANG, N. Security in 5g and beyond recent advances and future challenges. **Security and Privacy**, Wiley Online Library, v. 6, n. 1, p. e271, 2023.

SALEEM, K.; ALABDULJABBAR, G. M.; ALROWAIS, N.; AL-MUHTADI, J.; IMRAN, M.; RODRIGUES, J. J. P. C. Bio-inspired network security for 5g-enabled iot applications. **IEEE Access**, v. 8, p. 229152–229160, 2020.

SERIES, M. Imt vision–framework and overall objectives of the future development of imt for 2020 and beyond. **Recommendation ITU**, Electronic Publication Geneva, Switzerland, v. 2083, n. 0, p. 1–21, 2015.

SERMPEZIS, P.; KOTRONIS, V.; ARAKADAKIS, K.; VAKALI, A. Estimating the impact of bgp prefix hijacking. In: **2021 IFIP Networking Conference (IFIP Networking)**. [*S. l.*: *s. n.*], 2021. p. 1–10.

SETHI, R.; KADAM, A.; PRABHU, K.; KOTA, N. Security considerations to enable time-sensitive networking over 5g. **IEEE Open Journal of Vehicular Technology**, v. 3, p. 399–407, 2022.

SHIRANZAEI, A.; KHAN, R. Z. Ipv6 security issues—a systematic review. **Next-Generation Networks: Proceedings of CSI-2015**, Springer, p. 41–49, 2018.

SINGH, V. P.; SINGH, M. P.; HEGDE, S.; GUPTA, M. Security in 5g network slices: Concerns and opportunities. **IEEE Access**, v. 12, p. 52727–52743, 2024.

SOUSA, A. M. d. **Implementação da técnica de pilha dupla para transição de redes IPv4 para redes IPv6**. Trabalho de Conclusão de Curso (Graduação), Florianópolis, SC, 2018. Curso Superior de Tecnologia em Gestão da Tecnologia da Informação. Disponível em: https://repositorio.ifsc.edu.br/bitstream/handle/123456789/398/AdeyvisonMotaSousaTCC-Final%20-AJUSTADO.pdf?sequence=1. Acesso em: 6 ago. 2025.

SPADINGER, R. Implementação da tecnologia 5g no contexto da transformação digital e da indústria 4.0. Instituto de Pesquisa Econômica Aplicada (Ipea), 2024.

SULLIVAN, S.; BRIGHENTE, A.; KUMAR, S. A. P.; CONTI, M. 5g security challenges and solutions: A review by osi layers. **IEEE Access**, v. 9, p. 116294–116314, 2021.

SUOMALAINEN, J.; JUHOLA, A.; SHAHABUDDIN, S.; MäMMELä, A.; AHMAD, I. Machine learning threatens 5g security. **IEEE Access**, v. 8, p. 190822–190842, 2020.

TANENBAUM, A. S.; WETHERALL, D. J. **Redes de Computadores**. 5. ed. [*S. l.*]: Pearson Universidades, 2011. ISBN 9788576059240.

TANG, Q.; ERMIS, O.; NGUYEN, C. D.; OLIVEIRA, A. D.; HIRTZIG, A. A systematic analysis of 5g networks with a focus on 5g core security. **IEEE Access**, v. 10, p. 18298–18319, 2022.

TELECO. **Arquitetura do 5G – Parte 2**. 2024. Disponível em: https://www.teleco.com.br/tutoriais/tutorial5gnr2/pagina_3.asp. Acesso em: 04 ago. 2025.