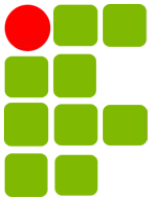


Instituto Federal de Educação, Ciência e Tecnologia da Paraíba
Campus Campina Grande
Coordenação do Curso Superior de Tecnologia em Telemática

NFV e SDN: Vantagens e Desvantagens Comparada a Redes Tradicionais

Wagner Gabriel Oliveira da Silva

Orientador: Dr. Éwerton Rômulo Silva Castro

Campina Grande, Junho de 2026

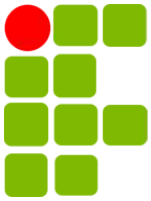
Catalogação na fonte:
Ficha catalográfica elaborada por Gustavo César Nogueira da Costa – CRB 15/479

S586n Silva, Wagner Gabriel Oliveira da.
NFV e SDN: vantagens e desvantagens comparada a redes tradicionais / Wagner Gabriel Oliveira da Silva. - Campina Grande, 2026.
39 f.: il.

Trabalho de Conclusão de Curso (Graduação em Tecnologia em Telemática) - Instituto Federal da Paraíba, 2026.
Orientador: Prof.Dr. Éwerton Rômulo Silva Castro

1. Telemática. 2. Redes definidas por software - (SDN. 3. Virtualização de funções de rede (NFV). 4. Arquitetura de redes - Infraestrutura. I. Castro, Éwerton Rômulo Silva. II Título.

CDU 004.7



Instituto Federal de Educação, Ciência e Tecnologia da Paraíba
Campus Campina Grande
Coordenação do Cursos Superior de Tecnologia em Telemática

NFV e SDN: Vantagens e Desvantagens Comparada a Redes Tradicionais

Wagner Gabriel Oliveira da Silva

Monografia apresentada à Coordenação do Curso de Telemática do IFPB - Campus Campina Grande, como requisito parcial para conclusão do curso de Tecnologia em Telemática.

Orientador: Dr. Éwerton Rômulo Silva Castro

Campina Grande, Junho de 2026

NFV e SDN: Vantagens e Desvantagens Comparada a Redes Tradicionais (Hardware Específico)

Wagner Gabriel Oliveira da Silva

Dr. Éwerton Rômulo Silva Castro
Orientador

Dr. Elmano Ramalho Cavalcanti
Membro da Banca

Dr. Petrônio Carlos Bezerra
Membro da Banca

Campina Grande, Paraíba, Brasil
Junho/2026

Dedico este trabalho à minha família, especialmente meus avós e meu tio, que me deram todo apoio e suporte necessário para que hoje possa concluir meu curso.

Todo mundo é um gênio. Mas, se você julgar um peixe por sua capacidade de subir em uma árvore, ela vai passar toda a sua vida acreditando que ele é estúpido.

Albert Einstein

Agradecimentos

Em primeiro lugar, agradeço a Deus, que guiou meus passos e permitiu que meus objetivos fossem alcançados ao longo de todos os anos de estudo. Sou imensamente grato à minha família, especialmente aos meus avós, Elias Pereira e Severina Oliveira e também meu tio, Waldenis Oliveira por todo o apoio e suporte oferecidos durante essa longa jornada. Agradeço imensamente ao Professor Dr. Éwerton Rômulo Silva Castro. Sua participação na minha trajetória acadêmica fez toda a diferença. Por fim, agradeço a todos os professores do Instituto Federal da Paraíba, Campus Campina Grande, pelo compromisso, dedicação e pelos ensinamentos transmitidos ao longo da minha formação, fundamentais para o meu crescimento acadêmico e profissional.

Resumo

O presente estudo, realizado por meio de uma RSL tem por objetivo analisar e comparar as vantagens e desvantagens dos paradigmas SDN e NFV em relação à arquitetura de redes tradicionais. A pesquisa adotou como metodologia as diretrizes do protocolo PRISMA, utilizando bases de dados acadêmicas de alto impacto. A estratégia de busca focou em estudos que abordavam SDN, NFV, redes tradicionais e os eixos de comparação (custo, desempenho, agilidade e segurança). No total, 13 artigos foram selecionados e analisados em profundidade para extração de dados, abrangendo o estado da arte entre 2012 e 2025. A RSL confirmou que a principal vantagem da "softwarização" reside na significativa redução de CAPEX e na melhoria da agilidade operacional e do TTM, impulsionada pelo uso de COTS. O SDN contribui com a programabilidade e o controle centralizado, aumentando a eficiência energética. Contudo, a análise também identificou desafios cruciais, como a dificuldade em garantir o mesmo nível de desempenho e baixa latência das funções virtuais em comparação a equipamentos ASICs, a complexidade do *framework* MANO e as novas superfícies de ataque.

Palavras-chave: Redes Definida por *Software*, Virtualização de Funçôes de Rede, Redes Tradicionais/Legadas, Comparação/Vantagens/Desvantagens.

Abstract

The present study aims to analyze and compare the advantages and disadvantages of SDN and NFV paradigms in relation to traditional network architectures. The research adopted a systematic literature review methodology following the PRISMA guidelines, utilizing high-impact academic databases. The search strategy focused on studies addressing SDN, NFV, traditional networks, and the comparison axes (cost, performance, agility, and security). In total, 13 articles were selected and analyzed in depth for data extraction, covering the state of the art between 2012 and 2025. The review confirmed that the primary advantage of network "softwarization"lies in the significant reduction of CAPEX and the improvement of operational agility and time-to-market, driven by the use of commercial off-the-shelf hardware. SDN contributes with programmability and centralized control, increasing energy efficiency. However, the analysis also identified crucial challenges, such as the difficulty in guaranteeing the same level of performance and low latency of virtual functions compared to ASIC equipment, the complexity of the management and orchestration framework, and new attack surfaces.

Keywords: Software-Defined Networking, Network Functions Virtualization, Traditional Networks/Legacy Networks, Comparison/Advantages/Disadvantages.

Sumário

Lista de Abreviaturas

APIs	*Application Programming Interface* (Interface de Programação de Aplicações)
ASICs	*Application-Specific Integrated Circuits* (Circuitos Integrados de Aplicação Específica)
CAPEX	*Capital Expenditure* (Custo de Capital)
COTS	*Commercial Off-the-Shelf* (Hardware de Prateleira)
DoS	*Denial of Service* (Negação de Serviço)
ETSI	*European Telecommunications Standards Institute* (Instituto Europeu de Normas de Telecomunicações)
ICN	*Information-centric networking* (Redes Centradas na Informação)
IoT	*Internet of Things* (Internet das Coisas)
MANO	*Management and Orchestration* (Gerenciamento e Orquestração)
NBI	*Northbound APIs* (Interfaces de Programação de Aplicações de "Norte")
NFV	*Network Functions Virtualization* (Virtualização de Funções de Rede)
NFVI	*Network Functions Virtualization Infrastructure* (Infraestrutura de Virtualização de Funções de Rede)
OPEX	*Operational Expenditure* (Custos Operacionais)
PRISMA	*Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (Principais Itens para Relatar Revisões Sistemáticas e Meta-análises)
QoS	*Quality of Service* (Qualidade de Serviço)
RSL	Revisão Sistemática da Literatura

SBI	*Southbound APIs* (Interfaces de Programação de Aplicações de "Sul")
SDN	*Software-Defined Networking* (Redes Definidas por Software)
SFCs	*Service Function Chains* (Cadeias de Funções de Serviço)
TTM	*Time-to-Market* (Tempo de Lançamento no Mercado)
VNFs	*Virtualized Network Functions* (Funções de Rede Virtualizadas)

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

A base da sociedade moderna tem sido a infraestrutura das redes de comunicação; no entanto, o modelo tradicional, consolidado ao longo de várias décadas, chegou a um ponto de transformação. Historicamente, as redes eram montadas com base em aparelhos de *hardware* (parte física e tangível de computadores, celulares e dispositivos eletrônicos) proprietário e especializado, nos quais as funções de controle, dados e gerenciamento estavam intimamente integradas. Como resultado desta integração vertical, surgiram sistemas robustos, mas internamente inflexíveis, caros e lentos para se ajustar às novas exigências do mercado [Yang *et al.* 2020; Zhang *et al.* 2018]. A introdução de novos serviços ou mesmo a ampliação da capacidade demandava a compra e implementação de novos equipamentos dedicados, resultando em elevados CAPEX (*Capital Expenditure* Custo de Capital) e um longo ciclo de inovação. O cenário atual, impulsionado pela IoT (*Internet of Things* Internet das Coisas), pela computação em nuvem e pela necessidade de serviços sob demanda, exige uma infraestrutura de rede que seja ágil, programável e capaz de escalar rapidamente. A propagação de bilhões de dispositivos e a chegada das redes 5G trazem uma complexidade e um volume de tráfego que as redes convencionais têm dificuldade em administrar de maneira eficiente [Alam *et al.* 2020; Akyildiz, Lin e Wang 2015].

Como resposta, surgiram dois paradigmas inovadores: o SDN (*Software-Defined Networking* Redes Definidas por Software) e o NFV (*Network Functions Virtualization* Virtualização de Funções de Rede). Embora possuam focos distintos — o SDN na centralização do controle e o NFV na virtualização de funções em *hardware* COTS (*Commercial Off-the-Shelf hardware* de Prateleira) — ambos visam desvincular as funções de rede do *hardware* subjacente [Duan, Ansari e Toy 2016]. Esta RSL (Revisão Sistemática da Literatura) analisa 13 estudos selecionados que demonstram como essa "softwarização" transforma redes estáticas em plataformas dinâmicas [Bonfim, Dias e Fernandes 2018]. Além de grandes *Data Centers* (Centro de Dados), este estudo investiga os impactos dessas tecnologias em pequenas redes e em arquiteturas emergentes, como as redes centradas em informação, onde a virtualização de nós busca superar a estagnação do modelo TCP/IP tradicional [Castillo 2024]. Portanto, busca-se analisar as vantagens e desvantagens desses conceitos, fornecendo uma base sólida

sobre a transição para uma infraestrutura de rede definida por *software*.

1.1 Justificativa e Relevância do Trabalho

A escolha deste tema deve-se à necessidade de superar as limitações do modelo de redes tradicional, que se tornou um gargalo para a inovação. A dependência de *hardware* proprietário resultou em infraestruturas rígidas e de difícil escalabilidade, incapazes de lidar com o volume massivo de tráfego da era do 5G e da *edge computing* (computação de borda) tecnologia que aproxima o processamento e o armazenamento de dados dos dispositivos finais para reduzir a latência. Investigar a transição para modelos como o SDN e o NFV é essencial para compreender a evolução da rede para uma plataforma programável. Este estudo é de suma importância para a área de Telemática, pois a "softwarização" representa uma mudança de paradigma na entrega de serviços. A pesquisa destaca a drástica redução do CAPEX e do OPEX (*Operational Expenditure* Custos Operacionais) ao substituir equipamentos dedicados por *software* (conjunto de instruções, dados ou programas lógicos usados para operar computadores e dispositivos eletrônicos, executando tarefas específica) executado em instâncias virtuais [Mijumbi *et al.* 2015]. A adoção dessas tecnologias reduz significativamente o TTM (*Time-to-Market* Tempo de Lançamento no Mercado), permitindo o lançamento de serviços em horas [Han *et al.* 2013]. Além disso, o controle centralizado permite uma otimização holística e energética dos recursos [Hameed *et al.* 2025]. A relevância deste trabalho amplia-se ao abordar temas críticos e atuais, como a segurança em ambientes *multi-tenant* (multi-inquilino) e o papel dos *hypervisores* no isolamento de recursos físicos [Blenk *et al.* 2016; Natarajan e Wolf 2012]. Ao consolidar evidências de 13 artigos selecionados via protocolo PRISMA, esta monografia oferece uma visão atualizada (2012-2025) sobre como o SDN e o NFV fornecem a agilidade necessária para gerenciar a heterogeneidade de dispositivos em redes modernas, garantindo a sustentabilidade técnica e econômica das futuras infraestruturas de comunicação.

1.2 Objetivos

Esta seção apresenta o objetivo geral que norteia esta pesquisa, bem como os objetivos específicos estabelecidos para delimitar as etapas necessárias para a sua execução e análise.

1.2.1 Objetivo Geral

Reunir e analisar, de maneira sistemática, os principais estudos sobre a implementação e integração de SDN e NFV, visando identificar os benefícios operacionais, os desafios de isolamento de recursos e os impactos que essa transição representa frente às arquiteturas de redes tradicionais.

1.2.2 Objetivos Específicos

- Avaliar os impactos da "softwarização" de rede nos eixos de custo, desempenho e agilidade operacional;
- Identificar as vulnerabilidades de segurança e os desafios de desempenho (sobrecarga de virtualização) introduzidos pelas novas arquiteturas.

1.3 Organização do Trabalho

Para facilitar a compreensão da temática e dos procedimentos adotados, este trabalho está estruturado em cinco capítulos, organizados da seguinte forma:

- Capítulo 1 – Introdução: Apresenta o contexto do estudo, a justificativa para a análise da "softwarização" de redes, além de delimitar o objetivo geral e os objetivos específicos desta pesquisa;
- Capítulo 2 – Fundamentação Teórica: Reúne os conceitos essenciais sobre redes tradicionais, SDN, NFV e IoT;
- Capítulo 3 – Metodologia: Este capítulo detalha a metodologia da RSL, definindo as questões de pesquisa, termos de busca e os critérios de inclusão e exclusão de artigos;
- Capítulo 4 – Resultados: Neste capítulo, realiza-se o resumo individual de cada um dos 13 artigos selecionados, detalhando suas principais contribuições para o estado da arte. O conteúdo é organizado em agrupamentos temáticos, comparando os estudos sob as óticas de arquitetura, desempenho/eficiência e segurança cibernética;
- Capítulo 5 – Considerações Finais: Sintetiza as conclusões obtidas, verificando o cumprimento dos objetivos propostos e indicando sugestões para trabalhos futuros com base nas lacunas identificadas.

Capítulo 2

Fundamentação Teórica

2.1 Redes Tradicionais

As redes tradicionais, que dominaram o cenário de comunicação por décadas, são definidas por uma arquitetura de integração vertical [Mijumbi *et al.* 2015]. Nessa estrutura, cada dispositivo de rede como roteadores, *switches* de camada 3, *firewalls* e balanceadores de carga é uma unidade autônoma onde os planos de dados, controle e gerenciamento estão rigidamente interligados. O plano de dados é responsável pelo encaminhamento físico dos pacotes, o plano de controle executa os protocolos de roteamento OSPF (*Open Shortest Path First* Abra o Caminho Mais Curto Primeiro) ou BGP (*Border Gateway Protocol* Protocolo de *Gateway* de Fronteira) para tomar decisões de caminho, e o plano de gerenciamento permite a configuração do dispositivo.

A principal característica dessas redes é o uso de *hardware* proprietário e especializado, frequentemente otimizado com ASICs *(Application-Specific Integrated Circuits* Circuitos Integrados de Aplicação Específica) para desempenho máximo [Yang *et al.* 2020]. Embora isso garanta alta performance e confiabilidade, impõe severas limitações. A dependência de fornecedores específicos e o alto custo de aquisição e manutenção desses equipamentos resultam em um elevado CAPEX. Além disso, a lógica de controle distribuída e a necessidade de configurar individualmente cada dispositivo tornam o gerenciamento complexo e propenso a erros. A aplicação de uma política de segurança ou a otimização de um caminho de tráfego em toda a rede exige intervenções manuais demoradas e complexas, resultando em baixa agilidade e um longo TTM para novos serviços.

A rigidez e a dificuldade de inovação inerentes a essa arquitetura foram os incentivadores para o surgimento dos conceitos de aplicação. A Figura 2.1 ilustra os componentes que constituem a infraestrutura de redes tradicionais, caracterizada por uma arquitetura rígida e dependente de *proprietary hardware* (*hardware* dedicado). Nota-se a presença de dispositivos com funções específicas e isoladas, como roteadores, *switches*, *firewalls* e pontos de acesso, cada qual operando com seu próprio plano de controle e gerenciamento. Esta configuração, embora fundamental para a evolução das telecomunicações, apresenta desafios significativos

de escalabilidade e flexibilidade, uma vez que a implementação de novas políticas de rede ou a alteração na topologia exige intervenções físicas ou configurações manuais individualizadas em cada equipamento, o que contrasta com a agilidade proposta pelos novos paradigmas de redes "softwarizadas" [Bonfim, Dias e Fernandes 2018].

Figura 2.1: *Dispositivos de Redes Tradicionais.*
Fonte: Autor, com auxílio de Inteligência Artificial (2026).

2.2 SDN

O SDN (*Software-Defined Networking* Redes Definidas por *Software*) emergiu como uma resposta direta às limitações de rigidez e complexidade das redes tradicionais, propondo uma separação fundamental entre o plano de controle e o plano de dados [Zhang *et al.* 2018]. A essência do SDN reside na centralização do plano de controle em uma entidade lógica única, o Controlador SDN. Este controlador mantém uma visão global e unificada de toda a topologia da rede, atuando como o "cérebro" da infraestrutura. Essa visão centralizada permite que os administradores de rede implementem políticas de forma consistente e otimizem o tráfego de maneira holística, algo impossível em redes distribuídas. A arquitetura SDN é composta por três planos:

- Plano de Aplicação (*Application Plane*): Contém as aplicações de rede (balanceadores de carga, sistemas de segurança, gerenciamento de tráfego) que definem o comportamento da rede. Elas se comunicam com o controlador através das NBI (*Northbound APIs* Interfaces de Programação de Aplicações de "Norte");
- Plano de Controle (*Control Plane*): O Controlador SDN, que traduz as políticas de alto nível das aplicações em regras de fluxo específicas;

- Plano de Dados (*Data Plane*): Composto por dispositivos de encaminhamento simples (muitas vezes *switches* COTS) que apenas executam as regras de fluxo. A comunicação entre o controlador e o plano de dados é feita através das SBI (*Southbound APIs* Interfaces de Programação de Aplicações de "Sul"), sendo o protocolo *OpenFlow* o padrão mais proeminente [Hussain *et al.* 2022].

A principal vantagem do SDN é a programabilidade. Ao expor a lógica de controle através de APIs (*Application Programming Interface* Interface de Programação de Aplicações), o SDN permite que desenvolvedores criem aplicações que interagem diretamente com a rede, automatizando tarefas e introduzindo novos serviços rapidamente. Isso resulta em maior agilidade, flexibilidade e a capacidade de inovar sem depender de ciclos de desenvolvimento de *hardware* proprietário. A arquitetura do SDN, representada na Figura 2.2, propõe a desagregação entre o plano de controle e o plano de dados. Diferente da rede tradicional, a inteligência é centralizada em um controlador lógico, que traduz políticas de alto nível em regras de fluxo, comunicando-se com os dispositivos de encaminhamento através de protocolos padrão, como o *OpenFlow* [Hussain *et al.* 2022]. Essa abstração permite um gerenciamento dinâmico e programável de toda a infraestrutura, facilitando a automação da rede [Zhang *et al.* 2018].

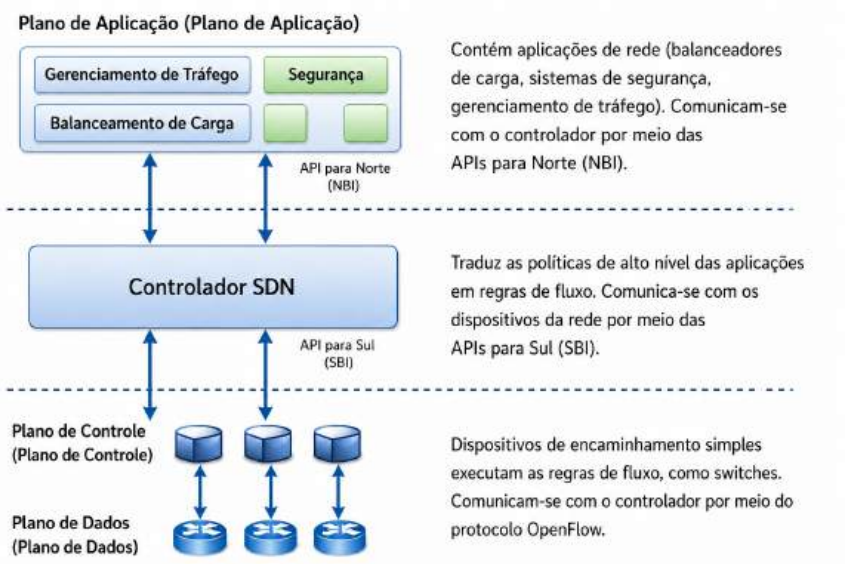


Figura 2.2: *Arquitetura de Planos SDN.*
Fonte: Autor, com auxílio de Inteligência Artificial (2026).

2.3 NFV

O NFV (*Network Functions Virtualization* Virtualização de Funções de Rede) é um conceito complementar ao SDN, focado na virtualização das funções de rede que tradicionalmente exigiam *hardware* dedicado e especializado, as chamadas *middleboxes* (Caixas Intermediárias) [Yang *et al.* 2020]. O NFV foi inicialmente proposto pelo ETSI (*European Telecommunications Standards Institute* Instituto Europeu de Normas de Telecomunicações) e tem como objetivo principal a redução de custos e o aumento da flexibilidade operacional. Ao substituir equipamentos proprietários caros por *software* rodando em infraestrutura COTS, as operadoras e empresas podem reduzir drasticamente o CAPEX. Além disso, a virtualização permite que as funções de rede sejam implantadas, escaladas e movidas dinamicamente, de acordo com a demanda, o que otimiza o uso de recursos e reduz o OPEX.

A arquitetura NFV é tipicamente dividida em três domínios principais:

- VNFs (*Virtualized Network Functions* Funções de Rede Virtualizadas): O *software* que implementa a função de rede (firewall virtual, NAT virtual, VPN virtual);
- NFVI (*Network Functions Virtualization Infrastructure* Infraestrutura de Virtualização de Funções de Rede): O ambiente de *hardware* e *software* (servidores COTS, *hypervisores*) onde as VNFs são executadas;
- MANO (*Management and Orchestration* Gerenciamento e Orquestração): O framework responsável pelo gerenciamento do ciclo de vida das VNFs (instanciação, escalonamento, término) e pela orquestração dos recursos da NFVI;

A capacidade de implantar e encadear rapidamente VNFs para criar SFCs (*Service Function Chains* Cadeias de Funções de Serviço) é um dos maiores benefícios do NFV. Isso permite que novos serviços sejam lançados em questão de horas ou dias, em contraste com os meses necessários no modelo tradicional. O NFV, portanto, foca na eficiência da infraestrutura, enquanto o SDN foca na programabilidade da rede. A arquitetura NFV, ilustrada na Figura 2.3, visa dissociar as funções de rede (como Firewalls, VPNs e NAT) do *hardware* proprietário, permitindo que estas sejam executadas como instâncias de *software* sobre *Hardware* COTS. Nesse ecossistema, os *hypervisores* de rede desempenham um papel crucial na abstração dos recursos físicos para as instâncias virtuais [Blenk *et al.* 2016]. Esse gerenciamento é realizado pelo *framework* MANO, responsável por automatizar o ciclo de vida e a alocação de recursos das funções virtualizadas, sendo esta a base arquitetural detalhada por [Mijumbi *et al.* 2015]."

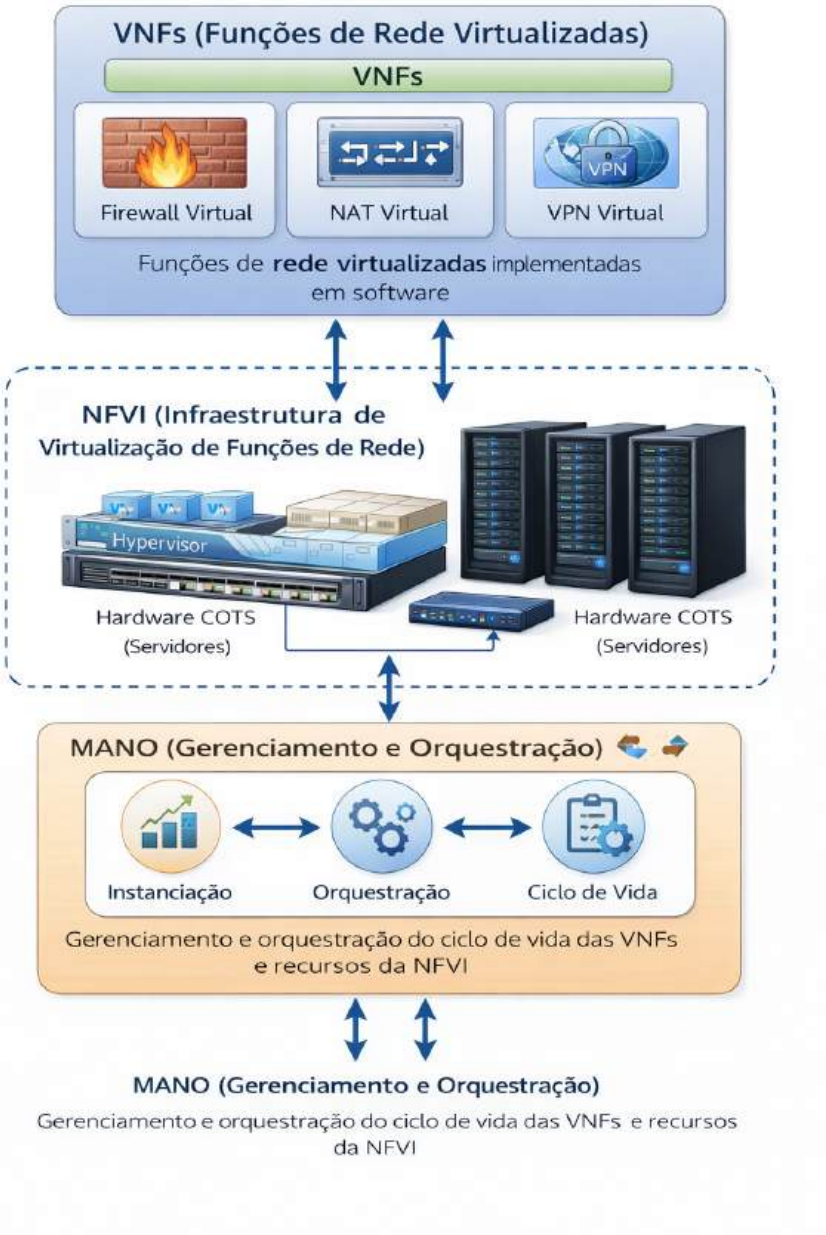


Figura 2.3: *Domínios da Arquitetura NFV.*
Fonte: Autor, com auxílio de Inteligência Artificial (2026).

2.4 IoT

A IoT (*Internet of Things* Internet das Coisas) representa a evolução da conectividade, onde bilhões de dispositivos heterogêneos — desde sensores de baixo consumo a veículos autônomos — estão ligados à rede para trocar dados e automatizar processos. Esta escala massiva impõe desafios sem precedentes às arquiteturas de rede tradicionais devido à necessidade de baixa latência, gestão de densidade e suporte a diferentes protocolos de comunicação [Alam *et al.* 2020].

A importância da IoT para este estudo reside na sua sinergia com o SDN e o NFV:

- Gestão de Tráfego e QoS (*Quality of Service* Qualidade de Serviço): A natureza dinâmica da IoT exige que a rede se adapte rapidamente a picos de tráfego. O SDN oferece o controle centralizado necessário para aplicar políticas de QoS de forma abrangente, garantindo que aplicações críticas (como saúde ou segurança) tenham prioridade sobre tráfego menos sensível [Bonfim, Dias e Fernandes 2018];
- *Edge Computing* (Computação de Borda) e NFV: Para evitar o congestionamento do núcleo da rede e reduzir a latência, muitas funções de processamento da IoT são movidas para a borda da rede (Edge). O NFV permite que funções como *gateways* de segurança, *firewalls* e processadores de dados sejam implantados como VNFs em dispositivos de borda, eliminando a necessidade de *hardware* especializado em cada local remoto [Alam *et al.* 2020];
- Segurança e Escalabilidade: A IoT expande a superfície de ataque de forma exponencial. A integração SDN/NFV permite uma resposta rápida a incidentes de segurança através do isolamento de fluxos de tráfego comprometidos e da rápida atualização de funções de segurança virtualizadas [Hussain *et al.* 2022].

Desta forma, a IoT deixa de ser apenas uma rede de dispositivos para se tornar uma rede inteligente e programável, onde o SDN gere a conectividade flexível e o NFV garante que as SFC necessárias estejam disponíveis onde e quando o dispositivo IoT precisar [Duan, Ansari e Toy 2016] [Hameed *et al.* 2025]. A Figura 2.4 ilustra a convergência tecnológica entre SDN, NFV e a IoT. A integração demonstra como a virtualização permite que funções de segurança e processamento *Edge Computing* sejam movidas para a borda da rede, reduzindo a latência e garantindo a escalabilidade necessária para o grande volume de dispositivos IoT. Simultaneamente, o controlador SDN assegura a qualidade de serviço QoS e a proteção proativa, mitigando ataques em redes complexas [Alam *et al.* 2020] [Yang *et al.* 2020].

Figura 2.4: *Sinergia Entre IoT e SDN/NFV.*
Fonte: Autor, com auxílio de Inteligência Artificial (2026).

Capítulo 3

Metodologia

3.1 Metodologia

A metodologia empregada para desenvolvimento do trabalho foi a RSL (Revisão Sistemática da Literatura), um método que visa sintetizar um amplo conjunto de informações existentes sobre um fenômeno específico. Dessa forma, a RSL realizada buscou analisar e comparar as vantagens e desvantagens do SDN e do NFV em relação às redes tradicionais baseadas em *hardware* específico, consolidando informações relevantes a partir de estudos previamente publicados. Para garantir a clareza, análise e síntese dos estudos, foram seguidas as diretrizes do método PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses* Principais Itens para Relatar Revisões Sistemáticas e Meta-análises) [Page *et al.* 2021]. Este protocolo orientou as etapas de identificação, triagem, elegibilidade e inclusão dos artigos científicos que compõem o corpo de análise desta revisão.

3.1.1 Questões de Pesquisa

As questões a seguir foram elaboradas para direcionar a análise comparativa entre as novas arquiteturas de rede e o modelo legado, abordando os eixos de custo, desempenho e segurança:

a) Quais são os principais benefícios econômicos e operacionais da adoção de SDN e NFV em comparação ao *hardware* específico das redes tradicionais?

b) Quais são os desafios técnicos e de desempenho mais significativos na implementação de Funções de rede virtualizadas VNFs?

c) Quais são os novos riscos e vulnerabilidades de segurança introduzidos pela centralização do controle e pela virtualização?

d) Qual é o impacto da programabilidade do SDN na eficiência energética e na gestão de tráfego de redes densas, como em cenários de IoT?

e) Quais são as tendências futuras para a integração SDN/NFV na orquestração de redes de próxima geração?

3.2 Palavras-Chave

A etapa de busca por literatura relevante na revisão sistemática é aprimorada pela definição cuidadosa de palavras-chave, que formam a base para as *strings* (Palavras) de busca nas bases de dados científicas selecionadas. As palavras-chave foram selecionadas para cobrir os pilares fundamentais da pesquisa: a arquitetura legada, os novos paradigmas de "softwarização" [Mijumbi *et al.* 2015] e os eixos comparativos de impacto econômico e operacional. Assim, a Tabela 3.1 mapeia esses conceitos nos idiomas nativo e inglês, atuando como um guia metodológico para a construção da estratégia de busca e identificação sistemática dos estudos mais relevantes.

Tabela 3.1: *Palavras-Chave Utilizadas na Pesquisa*

Termos em Português	**Termos Equivalentes em Inglês**
Rede Definida por Software	Software-Defined Networking (SDN)
Virtualização de Funções de Rede	Network Functions Virtualization (NFV)
Redes Tradicionais / Legadas	Traditional Networks / Legacy Networks
Comparação / Vantagens / Desvantagens	Comparison / Advantages / Disadvantages

3.2.1 Termos de Busca

Para compreender a fundo a comparação entre o modelo de redes tradicionais e as arquiteturas SDN e NFV, foi realizada uma pesquisa sistemática na base de dados acadêmica Capes. As *strings* de busca foram formuladas com base em palavras-chave relevantes que cobrissem os três principais componentes da questão de pesquisa: as tecnologias de "softwarização", a referência ao modelo legado e os eixos de comparação (vantagens/desvantagens). As lógicas impostas, como o operador "OR" para sinônimos e "AND" para a intersecção de conceitos, visam maximizar a abrangência da busca, ao mesmo tempo em que preservam a relevância dos resultados. Abaixo tem as *strings* utilizadas nas bases de dados. Esses dados são essenciais para entender a amplitude da pesquisa existente sobre os paradigmas de SDN e NFV.

("SDN" OR "Software-Defined Networking") AND ("NFV" OR "Network Function Virtualization") AND ("Traditional Networks" OR "Legacy Networks") AND ("Comparison" OR "Advantages" OR "Disadvantages")

3.2.2 Critérios de Inclusão

Os critérios de inclusão são fundamentais para a seleção dos artigos para esta RSL, conforme orientado pelo protocolo PRISMA. Este processo garante que a base de evidências seja composta por informações altamente relevantes e dotadas de autoridade científica, permitindo uma comparação justa entre as arquiteturas SDN/NFV e as redes tradicionais [Page *et al.* 2021]. A definição desses critérios visa mitigar vieses de seleção e focar em estudos que apresentem dados técnicos sólidos sobre os eixos de custo, desempenho e agilidade. O recorte temporal iniciado em 2012 justifica-se por ser este o ano do marco inicial da NFV, com a publicação do primeiro *whitepaper* (Documento Técnico) pelo ETSI, desencadeando uma variedade de publicações sobre a "softwarização" de redes [Mijumbi *et al.* 2015]. Além disso, a exigência de revisão por pares assegura que as conclusões sobre vantagens e desvantagens tenham sido validadas pela comunidade científica [Bonfim, Dias e Fernandes 2018]. Mais abaixo temos uma visão clara e objetiva dos critérios de inclusão e adotados, facilitando a reprodutibilidade do estudo e a compreensão dos requisitos específicos que os artigos escolhidos devem cumprir.

Critérios de Inclusão (CI):

- CI1: Artigos publicados entre 2012 e 2025;
- CI2: Artigos revisados por pares;
- CI3: Artigos que estejam na língua inglesa;
- CI4: Artigos indexados nas bases de dados IEEE Xplore, ScienceDirect, Scopus e Google Acadêmico;
- CI5: Artigos que realizam comparativos diretos ou análises de desempenho entre SDN/NFV e infraestruturas legadas;
- CI6: Trabalhos do tipo *Survey*, *Literature Review* ou estudos experimentais com foco em arquitetura de rede.

3.3 Dados Coletados

A busca inicial realizada nas três bases de dados selecionadas resultou em um montante bruto de 828 publicações. A distribuição desses resultados revela um cenário heterogêneo quanto ao volume de registros indexados em cada plataforma, evidenciando o alcance de busca para o ecossistema de redes programáveis. O Google Acadêmico apresentou o maior volume de publicações identificado, totalizando 529 artigos, o que corresponde a 63,89% do escopo bruto da pesquisa. Esse domínio numérico resulta diretamente da qualidade da plataforma em realizar buscas amplas em arquivos institucionais, teses, trabalhos e registros

de eventos, capturando uma teia densa de discussões que abrange desde revisões gerais até estudos de caso práticos e avaliações de desempenho.

Em seguida, o Portal de Periódicos CAPES consolidou-se como a segunda maior fonte de dados da revisão, retornando 271 registros, o que representa 32,73% do total acumulado. Por se tratar de uma associação nacional que inclui importantes bases internacionais e periódicos revisados por especialistas, portanto, o grande volume nesta base garante que discussões consolidadas sobre a transição arquitetural e o embate direto entre a programabilidade em software e a rigidez do hardware dedicado.

Por fim, a base Scopus apresentou a menor incidência quantitativa em termos brutos, com 28 publicações identificadas, equivalendo a 3,38% da amostragem inicial. Apesar do menor volume relativo, a inclusão desses registros é altamente estratégica, visto o rigor de indexação da Scopus, que concentra pesquisas de alto impacto voltadas à infraestrutura, eficácia e métricas analíticas de desempenho de novas arquiteturas em substituição às redes legadas.

A Figura 3.1 ilustra a distribuição percentual consolidada desses resultados, permitindo visualizar graficamente o peso de cada base de dados antes da etapa de filtragem e eliminação de duplicatas pelo método PRISMA.

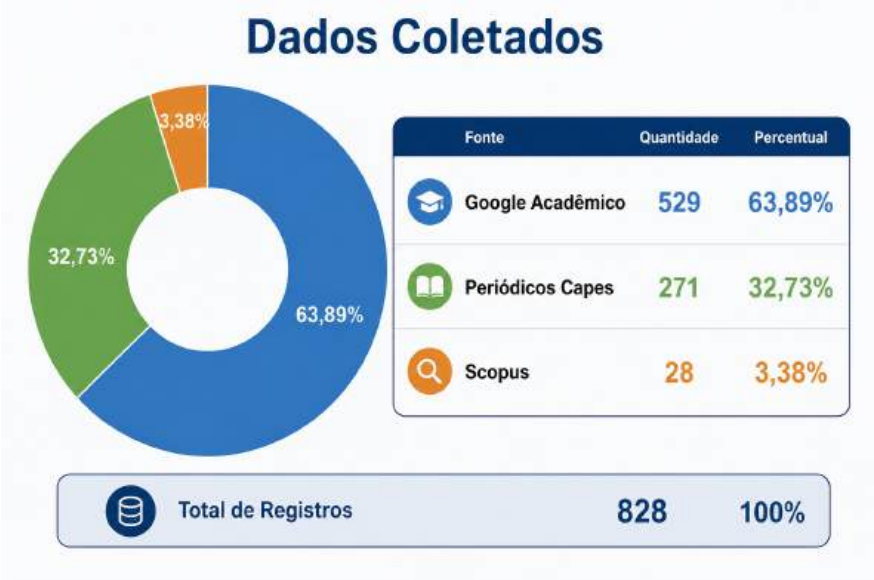


Figura 3.1: *Distribuição dos resultados do termo nas bases de dados.*
Fonte: Autor, com auxílio de Inteligência Artificial (2026).

3.4 Artigos Escolhidos

A escolha dos artigos que compõem esta revisão foi fundamentada em critérios de relevância temática, visando responder à questão central sobre as vantagens e desvantagens de SDN e NFV frente às redes tradicionais. O processo de afunilamento seguiu estritamente o protocolo PRISMA, sendo dividido em quatro fases principais: Identificação, Triagem, Elegibilidade e Inclusão. Na fase de Identificação, a busca inicial nas bases consultadas (Google Acadêmico, Portal de Periódicos CAPES e Scopus) retornou um montante bruto de 828 registros. Após

o processo de remoção de duplicatas e limpeza de metadados realizado com o auxílio das ferramentas *Mendeley e Zotero Connector*, foram eliminados 482 artigos repetidos, resultando em um total de 346 registros únicos para análise.

A fase de Triagem foi composta pela filtragem técnica baseada na leitura criteriosa de títulos e resumos:

- Nesta etapa, foram aplicados filtros de aderência temática (foco no embate entre SDN/NFV e hardware específico) e recortes de elegibilidade. Esse processo resultou na exclusão de 318 registros que não atendiam ao escopo técnico desta pesquisa ou consistiam em materiais não revisados por pares (como resumos simples de eventos, tutoriais ou apresentações), restando 28 artigos selecionados para o passo seguinte.

Na fase de Elegibilidade, os 28 artigos remanescentes foram submetidos a uma análise detalhada por meio de leitura integral. O objetivo foi verificar a presença de evidências comparativas diretas, metodologias claras e resultados verificáveis. Esta análise fina resultou na exclusão de 15 registros que, embora relevantes no resumo, não aprofundavam a discussão técnica necessária sobre a infraestrutura de hardware ou não apresentavam métricas comparáveis.

Por fim, na fase de Inclusão, restaram os 13 estudos escolhidos para a síntese qualitativa e quantitativa final. Estes artigos representam as evidências mais robustas sobre a "softwarização" de redes no cenário científico, abrangendo desde análises de latência, eficiência energética e *throughput* (Taxa de Transferência) até impactos em OPEX e CAPEX. Todo este fluxo está detalhado no fluxograma da Figura 3.2.

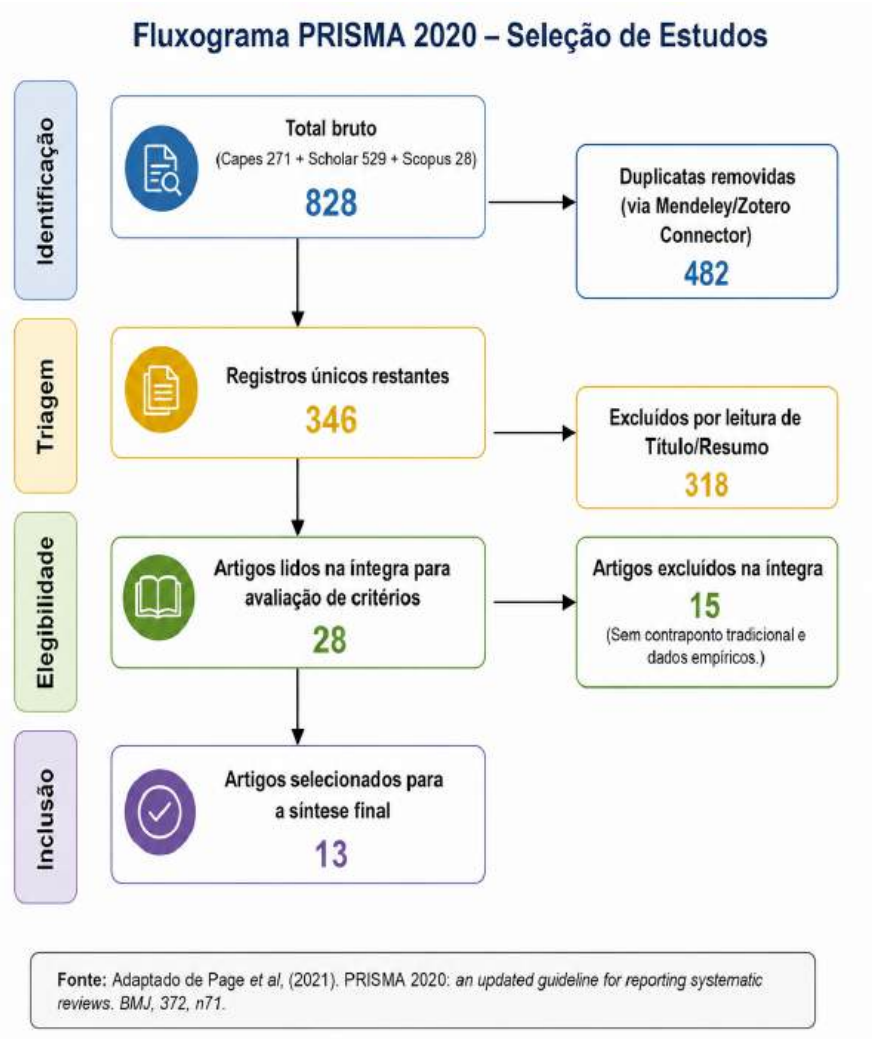


Figura 3.2: *Fluxograma de seleção dos Artigos.*

Capítulo 4

Resultados

4.1 Resultados da RSL

Os resultados obtidos, sintetizados nas Tabelas 4.1 e 4.2, respondem diretamente à questão central desta pesquisa ao categorizar as evidências por suas contribuições teóricas, práticas e comparativas. A análise dos 13 artigos selecionados confirmou a relevância e a complementaridade dos paradigmas SDN e NFV, demonstrando que a migração para a "softwarização" transforma redes estáticas em plataformas dinâmicas essenciais para viabilizar infraestruturas modernas, como as redes 5G [Akyildiz, Lin e Wang 2015].

A consolidação dessas evidências permitiu observar uma evolução cronológica e temática na literatura: enquanto o foco inicial residia na redução de custos (CAPEX/OPEX) e na automação via *framework* MANO [Mijumbi *et al.* 2015], as discussões mais recentes avançaram para camadas de abstração complexas. Esse novo panorama técnico destaca o papel dos *hypervisores* de rede no isolamento de recursos [Blenk *et al.* 2016] e a integração de funções virtualizadas em redes centradas em conteúdo, visando superar as limitações de roteamento das topologias legadas [Castillo 2024]. Assim, os resultados aqui expostos oferecem uma visão holística sobre o equilíbrio entre custo, desempenho, escalabilidade e segurança nos novos modelos de rede.

Tabela 4.1: *Coleta de dados: Resumo das aplicações e potenciais impactos encontrados nos artigos analisados.*

Artigo	**Autor(es)/Ano**	**Periódico**	**Aplicação Sugerida**	**Impactos Potenciais**
Network Function Virtualization: State-of-the-art and Research Challenges	[Mijumbi *et al.* 2015]	IEEE Communications Surveys & Tutorials	Aplicável como base teórica para contextualizar NFV	Identifica lacunas: adaptação, migração, inalterabilidade.
Network function virtualization: Challenges and opportunities for innovations	[Han *et al.* 2013]	IEEE Network Magazine	Discussão prática sobre limitações e desafios reais	Destaca que NFV não substitui *hardware* imediatamente, podendo introduzir despesa geral, ajudando a delimitar cenários de aplicação.
Software Defined Networking (SDN) Research Review	[Zhang *et al.* 2018]	IEEE Communications Surveys & Tutorials	Revisão de SDN para comparações SDN vs. NFV	Apresenta avanços e limitações do controle programável, ajudando a identificar pontos de integração SDN–NFV.
A Survey of Network Virtualization Techniques for Internet of Things Using SDN and NFV	[Alam *et al.* 2020]	International Journal of Computer Networks and Communications Security	Aplicações SDN/NFV em IoT	Mostra como NFV+SDN podem melhorar escalabilidade, segurança e otimização de recursos em IoT.
Recent Advances of Resource Allocation in Network Function Virtualization	[Yang *et al.* 2020]	IEEE Transactions on Parallel and Distributed Systems	Focado em alocação de recursos, encadeamento de função de serviço, qualidade de serviço	Redução de CAPEX/OPEX, desafios de roteamento e QoS.
Software-Defined Networking: Categories, Analysis, and Future Directions	[Hussain *et al.* 2022]	Sensors	Revisão e análise de categorias de SDN, incluindo testes de rede e verificação e segurança	Simplificação do gerenciamento e programação da rede. Ajuda para academia e indústria implementarem e testarem aplicações.
Security issues in network virtualization for the future Internet	[Natarajan e Wolf 2012]	International Conference on Computing, Networking and Communications (ICNC)	Endereçamento e discussão de questões de segurança em virtualização de rede (NV) para o futuro da Internet	Reforça a confiança e responsabilização e o monitoramento de Redes Virtuais (VN).
Integrated NFV/SDN Architectures: A Systematic Literature Review	[Bonfim, Dias e Fernandes 2018]	ACM Computing Surveys (Revisão Sistemática da Literatura)	Revisão Sistemática da Literatura (RSL) focada em arquiteturas NFV/SDN integradas	As tecnologias NFV e SDN são complementares e capazes de fornecer uma solução de rede consolidada. SDN facilita a conectividade flexível e automatizada entre VNFs (Funções de Rede Virtual).

Tabela 4.2: *Coleta de dados: Resumo das aplicações e potenciais impactos encontrados nos artigos analisados.*

Artigo	**Autor(es)/Ano**	**Periódico**	**Aplicação Sugerida**	**Impactos Potenciais**
A Comparative Study of the Energy Efficiency of Traditional Network Topology and Software-Defined Networking (SDN) Topology	[Hameed *et al.* 2025]	International Journal of Innovations in Science & Technology (IJIST)	Estudo comparativo da eficiência energética entre topologias de rede tradicionais e topologias SDN	O SDN centraliza o controle da rede, facilitando a alocação e otimização de recursos com eficiência energética. Demonstra como o SDN pode oferecer benefícios ao meio ambiente e à economia ao reduzir o uso de recursos e custos operacionais.
Software-defined network virtualization: an architectural framework for integrating SDN and NFV for service provisioning in future networks	[Duan, Ansari e Toy 2016]	IEEE Network	Apresentação de uma estrutura arquitetural chamada SDNV para integrar SDN e NFV, fornecendo uma visão coletiva para a provisão de serviços em redes futuras	Permite a exploração total das vantagens de SDN e NFV. Aborda a provisão de serviços ponta a ponta em infraestruturas compostas. Potencial para redução do consumo de energia ao construir uma infraestrutura de rede mais ecológica.
Survey on Network Virtualization Hypervisors for Software Defined Networking	[Blenk *et al.* 2016]	IEEE Communications Surveys & Tutorials	Análise de camadas de abstração e isolamento em redes virtualizadas.	Demonstra como o uso de *hypervisores* permite o compartilhamento de infraestrutura física por múltiplos locatários com segurança e isolamento de recursos.
Wireless Software-Defined Networks (W-SDNs) and Network Function Virtualization (NFV) for 5G Cellular Systems	[Akyildiz, Lin e Wang 2015]	Computer Networks (Elsevier)	Integração de SDN e NFV em infraestruturas de redes móveis 5G.	Evidencia a viabilidade da "cloudificação" da rede de acesso, proporcionando elasticidade, baixa latência e redução de custos em larga escala.
An Overview of Integration of the Virtualization of Network Functions in the Context of Information Centric Networks	[Castillo 2024]	IEEE Cloud Summit	Implementação de NFV em arquiteturas de redes centradas em conteúdo.	Propõe a substituição de modelos baseados em *host* por modelos focados em dados, otimizando o roteamento e equilibrando custos entre provedores e usuários.

4.1.1 Panorama Geral das Publicações Selecionadas

O portfólio final desta revisão consolidou-se em 13 artigos representativos do estado da arte na transição das redes tradicionais para os paradigmas de "softwarização". A distribuição cronológica e metodológica da amostra evidencia a evolução e a maturidade do tema, englobando desde revisões de escopo amplo até avaliações experimentais de desempenho, o que assegura uma base de dados abrangente para responder aos objetivos desta pesquisa [Mijumbi *et al.* 2015].

A análise preliminar da literatura selecionada revela uma divisão clara de abordagens. De um lado, um grupo expressivo de estudos concentra-se nas fundações arquiteturais e nas vantagens econômicas e operacionais da convergência SDN/NFV, com ênfase na otimização de CAPEX/OPEX, ganho de agilidade e viabilização de ecossistemas modernos como o 5G [Bonfim, Dias e Fernandes 2018; Duan, Ansari e Toy 2016; Hameed *et al.* 2025; Akyildiz, Lin e Wang 2015].

De outro, emergem investigações focadas nos desafios técnicos da implementação prática, englobando a sobrecarga (*overhead*) das funções virtuais frente aos *hardwares* ASICs [Han *et al.* 2013; Alam *et al.* 2020], a complexidade dos *frameworks* de orquestração [Yang *et al.* 2020], os novos riscos de segurança em ambientes multi-inquilino ou IoT [Zhang *et al.* 2018; Hussain *et al.* 2022], e o uso de *hypervisores* e novas topologias para superar as limitações do modelo legado [Blenk *et al.* 2016; Castillo 2024].

Para sistematizar e aprofundar essa análise comparativa, os 13 estudos foram mapeados e organizados de acordo com suas principais contribuições. A seção a seguir detalha esse agrupamento temático e estabelece os eixos de discussão que fundamentam as conclusões deste trabalho.

4.2 Agrupamento Temático e Comparação

Para viabilizar a análise comparativa, os 13 artigos selecionados foram categorizados em três eixos temáticos principais baseados em suas contribuições dominantes: Arquitetura e Integração, Desempenho e Eficiência, e Segurança.

4.2.1 Arquitetura e Integração de Redes "Softwarizadas"

Os estudos concentrados neste eixo estabelecem que a transição para a "softwarização" supera uma simples substituição de componentes físicos, consistindo em uma reestruturação lógica e conceitual da infraestrutura corporativa podem ser observados no Quadro 4.3.

Tabela 4.3: *Comparativo entre artigos sobre Arquitetura e Integração*

Autor (Ano)	**Foco Principal**	**Contribuição Central**
[Mijumbi *et al.* 2015]	Arquitetura NFV	Detalhamento do *framework* ETSI e MANO.
[Duan, Ansari e Toy 2016]	Integração SDN/NFV	Conectividade dinâmica para cadeias de serviços.
[Bonfim, Dias e Fernandes 2018]	Softwarização	Desagregação de *hardware* e *software*.
[Natarajan e Wolf 2012]	Virtualização	Isolamento de redes virtuais (Multi-tenancy).
[Blenk *et al.* 2016]	Hipervisor SDN	Abstração e isolamento em redes fatiadas.
[Castillo 2024]	Integração ICN/NFV	Virtualização de nós em redes centradas em conteúdo.

A convergência entre as propostas de [Mijumbi *et al.* 2015] e [Duan, Ansari e Toy 2016] evidencia que o acoplamento do controle centralizado à virtualização de funções é o pré-requisito para a automação de topologias complexas. Essa perspectiva de abstração é refinada por [Blenk *et al.* 2016] ao demonstrar a viabilidade técnica do isolamento lógico em cenários multi-inquilino, cujos pilares de segurança e coexistência inicial remetem aos requisitos fundamentais propostos por [Natarajan e Wolf 2012]. Expandindo o escopo das aplicações, [Castillo 2024] transpõe essa flexibilidade estrutural para redes centradas em dados, superando a rigidez do modelo de roteamento *host-to-host* tradicional.

4.2.2 Desempenho e Eficiência Operacional

Este grupo reúne as investigações voltadas aos impactos práticos causados pela introdução das camadas de virtualização na linha de frente do processamento de pacotes, bem como estratégias de sustentabilidade podem ser observados no Quadro 4.4.

Tabela 4.4: *Comparativo entre artigos sobre Desempenho e Eficiência Operacional*

Autor (Ano)	**Foco Principal**	**Contribuição Central**
[Han *et al.* 2013]	Desempenho NFV	Identificação de gargalos em VNFs vs. *hardware* dedicado.
[Alam *et al.* 2020]	IoT e Edge	Avaliação de latência em funções virtualizadas na borda.
[Hameed *et al.* 2025]	Eficiência Energética	Estratégias de redes verdes através de controle centralizado.
[Akyildiz, Lin e Wang 2015]	Sistemas 5G	Avaliação qualitativa de SDN/NFV em redes móveis.

A literatura desse eixo revela uma divisão inseparável ao paradigma. Enquanto [Hameed *et al.* 2025] quantifica reduções expressivas no consumo energético decorrentes da consolidação de recursos, [Han *et al.* 2013] e [Alam *et al.* 2020] alertam para os impactos severos na latência nominal e na formação de gargalos em funções virtualizadas quando comparadas à velocidade de comutação dos circuitos ASICs. Todavia, a análise de [Akyildiz, Lin e Wang

2015] refle que, no ecossistema 5G, a "cloudificação" das funções é obrigatória para garantir a elasticidade da rede. Assim, conclui-se que o ganho em agilidade operacional e escalabilidade justifica a tolerância a perdas marginais de desempenho bruto.

4.2.3 Segurança e Resiliência em Redes Definidas por Software

O terceiro eixo agrupa o mapeamento de vulnerabilidades nas interfaces de comunicação e a proposição de mecanismos de defesa baseados na visibilidade total do fluxo de tráfego podem ser observados no Quadro 4.5.

Tabela 4.5: *Comparativo entre artigos sobre Segurança e Resiliência em SDN*

Autor (Ano)	**Foco Principal**	**Contribuição Central**
[Zhang *et al.* 2018]	Vulnerabilidades SDN	Mapeamento de ataques ao controlador e interfaces.
[Yang *et al.* 2020]	Segurança em IoT	Uso de SDN para mitigação dinâmica de ataques DDoS.
[Hussain *et al.* 2022]	Visibilidade de Rede	Benefícios do controle centralizado para auditoria de segurança.

Os resultados demonstram que a centralização do plano de controle atua simultaneamente como um facilitador e um vetor de risco arquitetural. Sob a ótica defensiva, [Hussain *et al.* 2022] e [Yang *et al.* 2020] provam que a concentração da inteligência simplifica a auditoria global do tráfego e acelera a mitigação de ataques distributivos em ambientes de alta densidade como a IoT. Em contrapartida, [Zhang *et al.* 2018] ressalta que essa mesma centralização institui um ponto único de falha crítico: caso o controlador seja saturado ou comprometido, a integridade operacional de toda a infraestrutura subjacente é interrompida. Esse cenário reitera a necessidade de tratar a segurança de forma nativa e distribuída nas arquiteturas de próxima geração.

Capítulo 5

Considerações Finais e Sugestões para Trabalhos Futuros

Este capítulo apresenta, primeiramente, as considerações finais obtidas a partir da revisão sistemática realizada, destacando as principais conclusões sobre a viabilidade e os impactos da transição das redes tradicionais para os paradigmas SDN e NFV.

5.1 Considerações Finais

Este trabalho analisou, por meio de uma revisão sistemática da literatura, as vantagens e desvantagens dos paradigmas SDN e NFV em comparação com a arquitetura de redes baseada em hardware específico. A pesquisa confirmou que as inovações introduzidas pela "softwarização" da infraestrutura não representam apenas uma evolução incremental, mas uma resposta arquitetural imperativa para atender às demandas de escalabilidade e dinamismo impostas pela computação em nuvem, IoT e pelas redes 5G.

Os resultados consolidados apontam que a principal vantagem da convergência entre SDN e NFV reside na otimização econômica e na agilidade operacional. A desagregação entre hardware e software viabilizada pelo NFV promove uma redução drástica de CAPEX e OPEX ao migrar funções de rede para *hardware* padronizado de prateleira [Mijumbi *et al.* 2015; Hameed *et al.* 2025]. Paralelamente, a programabilidade e a centralização do plano de controle introduzidas pelo SDN asseguram uma gestão de tráfego dinâmica e uma eficiência energética superior [Zhang *et al.* 2018; Hussain *et al.* 2022]. Essa sinergia reduz significativamente o tempo de lançamento de novos serviços no mercado, provendo a elasticidade necessária para suportar o tráfego massivo contemporâneo por meio da "cloudificação" da rede de acesso [Akyildiz, Lin e Wang 2015].

Por outro lado, a transição para esses paradigmas impõe desafios críticos de engenharia. Os dados revisados reiteram que o desempenho bruto e a latência das funções virtuais ainda

encontram barreiras quando comparados à velocidade de comutação dos circuitos integrados específicos das redes tradicionais [Han *et al.* 2013]. Sob a ótica da resiliência, a centralização do controlador SDN introduz um ponto único de falha potencial e novas superfícies de ataque. Além disso, o suporte a ambientes multi-inquilino exige o uso rigoroso de *hypervisores* de rede para garantir o isolamento efetivo de recursos entre fatias virtuais distintas [Blenk *et al.* 2016].

A complexidade operacional dos *frameworks* de orquestração [Yang *et al.* 2020] e a necessidade de evolução para redes centradas em conteúdo [Castillo 2024] representam as fronteiras atuais da área para superar o engessamento do modelo TCP/IP tradicional. Conclui-se, portanto, que a integração consolidada do SDN e NFV [Bonfim, Dias e Fernandes 2018; Duan, Ansari e Toy 2016] oferece a plataforma flexível e escalável necessária para as próximas décadas. Embora os gargalos técnicos exijam mitigação contínua, os ganhos em flexibilidade estrutural e programabilidade superam as limitações da rigidez legada, definindo o futuro definitivo da infraestrutura de redes.

5.1.1 Sugestões para Trabalhos Futuros

Visando transpor as evidências documentais para cenários práticos de validação, sugerem-se os seguintes trabalhos futuros:

- **Implementação e Simulação em Ambiente de Laboratório:** Desenvolver cenários de testes controlados utilizando emuladores e simuladores de rede de código aberto (como *Mininet* ou *Kathará*). O objetivo é avaliar experimentalmente as métricas de desempenho bruto, como latência no plano de controle, vazão da taxa de transferência e a eficácia do isolamento de recursos em *hypervisores* sob condições de estresse de tráfego;

- **Estudo de Caso em Pequenas Infraestruturas:** Avaliar a viabilidade técnica e econômica da aplicação prática de controladores SDN e funções virtualizadas em ambientes de menor escala (como redes locais de pequenas empresas ou comércios). Essa etapa buscará mensurar o impacto real na simplificação do gerenciamento cotidiano e validar se a redução de investimentos (CAPEX/OPEX) prevista na literatura de larga escala se replica de forma proporcional nesses cenários;

- **Auditoria de Segurança Prática:** Realizar testes de vulnerabilidade e simulações de ataques de negação de serviço voltados ao plano de controle centralizado nos cenários simulados, testando a resiliência das camadas de abstração e medindo o tempo de convergência e mitigação da rede de forma automatizada.

Referências Bibliográficas

[Akyildiz, Lin e Wang 2015] AKYILDIZ, I. F.; LIN, S.-C.; WANG, P. Wireless software-defined networks (w-sdns) and network function virtualization (nfv) for 5g cellular systems: An overview and qualitative evaluation. *Computer Networks*, Elsevier, v. 93, p. 345–358, 2015. 1, 17, 19, 20, 21, 23

[Alam *et al.* 2020] ALAM, I. *et al.* A survey of network virtualization techniques for internet of things using sdn and nfv. *ACM Computing Surveys*, v. 53, n. 2, p. 35, 2020. 1, 9, 18, 20, 21

[Blenk *et al.* 2016] BLENK, A. *et al.* Survey on network virtualization hypervisors for software defined networking. *IEEE Communications Surveys & Tutorials*, v. 18, n. 1, p. 655–685, 2016. 2, 7, 17, 19, 20, 21, 24

[Bonfim, Dias e Fernandes 2018] BONFIM, M. S.; DIAS, K. L.; FERNANDES, S. F. L. Integrated nfv/sdn architectures: A systematic literature review. *ACM Computing Surveys*, v. 51, n. 4, p. 74, 2018. 1, 5, 9, 13, 18, 20, 21, 24

[Castillo 2024] CASTILLO, A. C. An overview of integration of the virtualization of network functions in the context of information centric networks. *arXiv preprint arXiv:2408.01910*, 2024. Disponível em: <https://arxiv.org/abs/2408.01910>. 1, 17, 19, 20, 21, 24

[Duan, Ansari e Toy 2016] DUAN, Q.; ANSARI, N.; TOY, M. Software-defined network virtualization: An architectural framework for integrating sdn and nfv for service provisioning in future networks. *IEEE Network*, v. 30, n. 5, p. 8–16, 2016. 1, 9, 19, 20, 21, 24

[Hameed *et al.* 2025] HAMEED, S. *et al.* A comparative study of the energy efficiency of traditional network topology and software-defined networking (sdn) topology. *International Journal of Innovations in Science & Technology*, v. 7, n. 3, p. 1341–1352, 2025. 2, 9, 19, 20, 21, 23

[Han *et al.* 2013] HAN, B. *et al.* Network functions virtualization: Challenges and opportunities for innovations. *IEEE Communications Magazine*, v. 51, n. 12, p. 1–9, 2013. 2, 18, 20, 21, 24

[Hussain *et al.* 2022] HUSSAIN, M. *et al.* Software-defined networking: Categories, analysis, and future directions. *Sensors*, v. 22, n. 15, p. 5551, 2022. 6, 9, 18, 20, 22, 23

[Mijumbi *et al.* 2015] MIJUMBI, R. *et al.* Network function virtualization: State-of-the-art and research challenges. *IEEE Communications Surveys & Tutorials*, v. 17, n. 3, p. 1515–1544, 2015. 2, 4, 7, 12, 13, 17, 18, 20, 21, 23

[Natarajan e Wolf 2012] NATARAJAN, S.; WOLF, T. Security issues in network virtualization for the future internet. In: *International Conference on Computing, Networking and Communications (ICNC)*. Maui, HI, USA: IEEE, 2012. p. 1–18. 2, 18, 21

[Page *et al.* 2021] PAGE, M. J. *et al.* The prisma 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, v. 372, p. n71, 2021. 11, 13

[Yang *et al.* 2020] YANG, S. *et al.* Recent advances of resource allocation in network function virtualization. *IEEE Transactions on Parallel and Distributed Systems*, v. 31, n. 8, p. 1761–1775, 2020. 1, 4, 7, 9, 18, 20, 22, 24

[Zhang *et al.* 2018] ZHANG, Z. *et al.* Software defined networking (sdn) research review. In: *International Conference on Mechanical, Electronic, Control and Automation Engineering (MECAE)*. Beijing, China: Atlantis Press, 2018. p. 1–19. 1, 5, 6, 18, 20, 22, 23

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

Documento Digitalizado Restrito

TCC - Wagner Gabriel Oliveira da Silva

Assunto:	TCC - Wagner Gabriel Oliveira da Silva
Assinado por:	Wagner Gabriel
Tipo do Documento:	Anexo
Situação:	Finalizado
Nível de Acesso:	Restrito
Hipótese Legal:	Informação Pessoal (Art. 31 da Lei no 12.527/2011)
Tipo do Conferência:	Cópia Simples

Documento assinado eletronicamente por:

- **Wagner Gabriel Oliveira da Silva**, **DISCENTE (202521210028) DE TECNOLOGIA EM TELEMÁTICA - CAMPINA GRANDE**, em 28/06/2026 11:41:01.

Este documento foi armazenado no SUAP em 28/06/2026. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifpb.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1898310
Código de Autenticação: ff64b7ccf5