ReGeo ISSN: 2177-3246

ARQUITETURA ZERO TRUST EM INFRAESTRUTURAS DE REDES: UMA REVISÃO DE ESCOPO SOBRE MECANISMOS, EVIDÊNCIAS E DESAFIOS DE IMPLEMENTAÇÃO

ZERO TRUST ARCHITECTURE IN NETWORK INFRASTRUCTURES: A SCOPING REVIEW ON MECHANISMS, EVIDENCE, AND IMPLEMENTATION CHALLENGES

ARQUITECTURA ZERO TRUST EN INFRAESTRUCTURAS DE RED: UNA REVISIÓN DE ALCANCE SOBRE MECANISMOS, EVIDENCIAS Y DESAFÍOS DE IMPLEMENTACIÓN

https://doi.org/10.56238/revgeov17n7-173

Data de submissão: 23/06/2026 **Data de publicação:** 23/07/2026

Yago Rodrigues Cabral
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: yagorodriguescabral@gmail.com

Wilker José Caminha dos Santos
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: wilkercaminha@uepa.br
Orcid: https://orcid.org/0000-0002-5265-583X

Rosemary Maria Pimentel Coutinho
Instituição: Instituto Federal do Pará (IFPA)
E-mail: rosemary.coutinho@ifpa.edu.br
Orcid: https://orcid.org/0000-0002-3444-1248

Vitória Nazaré Costa Seixas
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: vitoria.seixas@uepa.br
Orcid: https://orcid.org/0000-0003-0716-3876

Elzelis Muller da Silva
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: elzelis@uepa.br
Orcid: https://orcid.org/0000-0001-6778-520X

Patrícia Danielle Lima de Lima
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: patricia.lima@uepa.br
Orcid: https://orcid.org/0000-0002-1068-2813

Thiago Nicolau Magalhães de Souza Conte
Instituição: Universidade do Estado do Pará (UEPA)
E-mail: thiagonconte@uepa.br
Orcid: https://orcid.org/0000-0002-1288-366X

RESUMO
A Arquitetura Zero Trust (ZTA) propõe a substituição da confiança implícita por verificação contínua, visando mitigar ameaças em ambientes descentralizados. Esta revisão de escopo analisou 15 estudos

(2022-2026) para mapear mecanismos, evidências e desafios de implementação da ZTA. Os resultados indicam que a ZTA não é uma solução única, mas uma abordagem adaptável que utiliza tecnologias como SDN, blockchain e aprendizado de máquina conforme o contexto (IoT, nuvem ou redes corporativas). A microsegmentação e o controle de acesso baseado em identidade mostraram alta eficácia na redução da superfície de ataque e na contenção de movimentos laterais. Entretanto, a implementação enfrenta desafios técnicos, incluindo latência, impactos no desempenho e complexidade de integração com sistemas legados. A principal lacuna identificada é a falta de padronização nas métricas de avaliação, o que limita a comparabilidade entre estudos. Conclui-se que a adoção da ZTA exige planejamento contextual, sendo necessário avançar em métricas padronizadas e estudos em larga escala.

Palavras-chave: Arquitetura Zero Trust. Segurança de Redes. Microsegmentação. Revisão de Escopo. Verificação Contínua.

ABSTRACT

Zero Trust Architecture (ZTA) proposes replacing implicit trust with continuous verification to mitigate threats in decentralized environments. This scoping review analyzed 15 studies (2022-2026) to map ZTA mechanisms, evidence, and implementation challenges. The results indicate that ZTA is not a single solution, but an adaptable approach that utilizes technologies such as SDN, blockchain, and machine learning according to the context (IoT, cloud, or corporate networks). Microsegmentation and identity-based access control showed high effectiveness in reducing the attack surface and containing lateral movement. However, implementation faces technical challenges, including latency, performance impacts, and the complexity of integrating with legacy systems. The main gap identified is the lack of standardization in evaluation metrics, which limits comparability between studies. It is concluded that the adoption of ZTA requires contextual planning, necessitating progress in standardized metrics and large-scale studies.

Keywords: Zero Trust Architecture. Network Security. Micro-segmentation. Scoping Review. Continuous Verification.

RESUMEN

La Arquitectura Zero Trust (ZTA) propone la sustitución de la confianza implícita por la verificación continua, con el objetivo de mitigar amenazas en entornos descentralizados. Esta revisión de alcance analizó 15 estudios (2022-2026) para mapear mecanismos, evidencias y desafíos de implementación de la ZTA. Los resultados indican que la ZTA no es una solución única, sino un enfoque adaptable que utiliza tecnologías como SDN, blockchain y aprendizaje automático según el contexto (IoT, nube o redes corporativas). La microsegmentación y el control de acceso basado en identidad mostraron una alta eficacia en la reducción de la superficie de ataque y en la contención de movimientos laterales. Sin embargo, la implementación enfrenta desafíos técnicos, incluyendo latencia, impactos en el rendimiento y la complejidad de integración con sistemas heredados. La principal brecha identificada es la falta de estandarización en las métricas de evaluación, lo que limita la comparabilidad entre estudios. Se concluye que la adopción de la ZTA requiere una planificación contextual, siendo necesario avanzar en métricas estandarizadas y estudios a gran escala.

Palabras clave: Arquitectura Zero Trust. Seguridad de Redes. Microsegmentación. Revisión de Alcance. Verificación Continua.

1 INTRODUÇÃO

As arquiteturas de segurança de redes corporativas enfrentam transformações profundas devido à complexidade dos ambientes contemporâneos. Os modelos tradicionais, baseados em perímetros rígidos e na confiança implícita de recursos internos, mostram-se progressivamente insuficientes frente à sofisticação das ameaças e à descentralização dos ativos organizacionais (DIAZ RIVERA et al., 2023; HARI N.N. et al., 2026). A expansão da computação em nuvem (IaaS e SaaS), somada à computação de borda e ao crescimento exponencial de dispositivos IoT, consolidou infraestruturas distribuídas e heterogêneas (AMEER et al., 2024).

Nesse cenário, o perímetro de segurança, tipicamente associado ao modelo *castle-and-moat*, torna-se pouco definido. A confiança baseada exclusivamente na localização lógica ou física de usuários e dispositivos impõe riscos críticos: o comprometimento de um único *endpoint* pode facilitar movimentos laterais e o acesso a ativos sensíveis na ausência de mecanismos de verificação contínua, autorização e segmentação rigorosa.

Como resposta, a Arquitetura Zero Trust (ZTA) propõe a substituição da confiança implícita por um modelo de verificação explícita e contínua. O princípio de que nenhum recurso deve ser considerado confiável por padrão, independentemente de sua localização, está consolidado em diretrizes como o NIST SP 800-207 (NIST, 2020). Mecanismos como microsegmentação, autenticação baseada em identidade e aplicação dinâmica de políticas são, portanto, fundamentais para reduzir a superfície de ataque.

Entretanto, a implementação da ZTA introduz desafios significativos. Estudos recentes (MA et al., 2025; ABDELHADY et al., 2026) apontam impactos na latência de autenticação e autorização, especialmente em dispositivos de recursos limitados, além de complexidades operacionais na gestão de controles e na usabilidade. Torna-se necessário, portanto, examinar as evidências empíricas sobre a eficácia desses mecanismos em cenários reais.

Embora a literatura aborde propostas de ZTA, há uma lacuna no mapeamento sistematizado dos mecanismos investigados, das evidências empíricas de desempenho e dos obstáculos recorrentes de implementação. A dispersão dessas informações justifica a realização de uma revisão de escopo, capaz de caracterizar a extensão, a natureza e as principais vertentes da produção científica atual sobre o tema.

Diante desse contexto, o presente estudo objetiva mapear e analisar a literatura publicada entre 2022 e 2026, articulando-a com diretrizes normativas para compreender a aplicação da ZTA em infraestruturas de rede. Busca-se identificar os principais mecanismos empregados, com ênfase em microsegmentação, controle de acesso baseado em identidade e componentes de decisão (PDP) e

execução (PEP), bem como caracterizar as evidências relacionadas à mitigação de ameaças, métricas de desempenho e desafios práticos, sistematizando o estado da arte e identificando lacunas para pesquisas futuras.

2 REFERENCIAL TEÓRICO

2.1 FUNDAMENTOS E PRINCÍPIOS DA ARQUITETURA ZERO TRUST

Os modelos tradicionais de segurança baseados no perímetro (*castle-and-moat*) tornaram-se insuficientes com a expansão da nuvem, mobilidade e dispositivos IoT. A confiança implícita no ambiente interno é uma fragilidade crítica, pois facilita a movimentação lateral e amplia o alcance de incidentes após o comprometimento de credenciais ou endpoints. Em resposta, a Arquitetura Zero Trust (ZTA) substitui esse modelo pela verificação explícita e contínua, fundamentada no princípio "*never trust, always verify*".

Nesse paradigma, a concessão de acesso não depende da localização física ou lógica, mas de decisões dinâmicas orientadas por identidade, contexto, estado do ativo e comportamento observado. Ao tratar autenticação e autorização como processos constantes e granulares, a ZTA busca limitar a exposição de recursos e reduzir drasticamente os riscos de utilização indevida de ativos ou identidades comprometidas na infraestrutura.

2.2 MODELO ARQUITETURAL E COMPONENTES DA ZTA SEGUNDO O NIST SP 800-207

O NIST SP 800-207 define a ZTA através da separação entre o plano de controle (decisões) e o plano de dados (comunicação). O Ponto de Decisão de Política (PDP) centraliza a inteligência: o Mecanismo de Política (PE) decide sobre o acesso com base em contexto, enquanto o Administrador de Política (PA) estabelece ou encerra os caminhos de comunicação. A aplicação real cabe ao Ponto de Execução de Política (PEP), que media o acesso entre sujeito e recurso conforme as ordens do plano de controle.

Tecnologicamente, as Redes Definidas por Software (SDN) são ideais para suportar essa arquitetura, pois sua separação entre controle e encaminhamento facilita a atualização dinâmica de regras. Contudo, em ambientes IoT, a heterogeneidade e as restrições de processamento, memória e energia limitam o uso de mecanismos pesados de autenticação, exigindo adaptações arquiteturais que respeitem a capacidade limitada desses dispositivos.

2.3 MECANISMOS DE CONTROLE E APLICAÇÃO DE POLÍTICAS

A operacionalização dos princípios da ZTA envolve mecanismos destinados a restringir a exposição de recursos, controlar privilégios e avaliar continuamente as solicitações de acesso, destacando-se a microsegmentação, o menor privilégio e o controle de acesso orientado por identidade e contexto. A microsegmentação consiste na divisão lógica da infraestrutura em segmentos de menor granularidade, permitindo aplicar políticas específicas a cargas de trabalho e fluxos de comunicação. Diferentemente de abordagens baseadas na localização de rede, ela incorpora atributos de identidade e contexto para limitar a movimentação lateral e reduzir o alcance potencial de incidentes.

O Princípio do Menor Privilégio (PoLP) estabelece que usuários e serviços recebam apenas as permissões necessárias à execução de suas funções. Na ZTA, este princípio associa-se a mecanismos de concessão temporária, como o acesso Just-in-Time (JIT), no qual privilégios são disponibilizados em períodos delimitados. Embora a identidade amplie a relevância da autenticação, a decisão dinâmica deve considerar também o estado do dispositivo, a sensibilidade do recurso e o comportamento observado.

A verificação contínua constitui o elemento transversal aos mecanismos da ZTA. Em vez de considerar a autenticação inicial como garantia permanente de confiança, o modelo admite a reavaliação constante das condições de acesso durante a sessão. Essa característica permite ajustar políticas e restringir acessos conforme mudanças nas condições de segurança ou identificação de anomalias. Tais fundamentos baseiam a análise de tecnologias como Redes Definidas por Software, inteligência artificial e identidades descentralizadas. Contudo, a extensão de seu uso e os desafios de adoção são aspectos centrais examinados nesta revisão de escopo.

3 METODOLOGIA

3.1 DELINEAMENTO DA PESQUISA

O estudo caracteriza-se como uma revisão de escopo, desenvolvida com o objetivo de mapear os mecanismos, as evidências empíricas e os desafios relacionados à implementação da Arquitetura Zero Trust (*Zero Trust Architecture* – ZTA) em infraestruturas de redes. A escolha desse delineamento decorreu da heterogeneidade dos contextos tecnológicos, das abordagens arquiteturais e das métricas de avaliação identificadas na literatura, abrangendo ambientes de nuvem, Internet das Coisas (IoT), redes móveis e infraestruturas corporativas distribuídas.

A condução metodológica da revisão foi orientada pelas recomendações aplicáveis às revisões de escopo. O relato das etapas de identificação, seleção e inclusão dos estudos observou as diretrizes do *Preferred Reporting Items for Systematic Reviews and Meta-Analyses extension for Scoping*

Reviews (PRISMA-ScR), enquanto a descrição da estratégia de busca considerou as recomendações do PRISMA-S.

A revisão buscou caracterizar a extensão e a natureza das evidências disponíveis, sem realizar uma avaliação comparativa formal da eficácia das intervenções ou uma síntese quantitativa dos efeitos. Foram mapeados os mecanismos técnicos investigados, os contextos de implementação, as métricas empregadas e os principais resultados e desafios relatados pelos estudos primários. O documento normativo NIST SP 800-207 foi utilizado como referência conceitual para a interpretação dos componentes e princípios da ZTA, não integrando o corpus de estudos empíricos selecionados.

3.2 QUESTÕES DE PESQUISA

A revisão foi orientada pela seguinte questão principal:

QP – Quais mecanismos, evidências empíricas e desafios de implementação da Arquitetura Zero Trust em infraestruturas de redes são relatados na literatura científica recente?

A partir da questão principal, foram definidas quatro questões secundárias:

QS1 – Quais mecanismos, princípios e componentes da ZTA têm sido implementados ou avaliados em infraestruturas de redes?

QS2 – Em quais contextos tecnológicos e ambientes de infraestrutura as implementações de ZTA são investigadas?

QS3 – Quais métricas e evidências empíricas são utilizadas para avaliar aspectos de segurança e desempenho das implementações?

QS4 – Quais desafios, limitações e lacunas relacionados à implementação da ZTA são relatados nos estudos?

As questões foram utilizadas para orientar a estratégia de busca, os critérios de elegibilidade, a extração dos dados e a organização temática dos resultados.

3.3 ESTRATÉGIA DE BUSCA E FONTES DE INFORMAÇÃO

A busca bibliográfica foi realizada na base IEEE Xplore, selecionada em razão de sua cobertura de publicações técnicas nas áreas de engenharia, redes de computadores e segurança da informação. O recorte temporal compreendeu estudos publicados entre 2022 e 2026, considerando a produção científica recente relacionada à implementação da ZTA.

A estratégia de busca combinou termos relacionados à Arquitetura Zero Trust, aos contextos de infraestrutura, aos mecanismos de controle e às abordagens de avaliação. A expressão de busca foi estruturada com operadores booleanos, conforme apresentado na Tabela 1.

Tabela 1. Parâmetros de Busca e Estratégia de Coleta

Base de Dados	String de Busca Final	Filtros Aplicados	Total de Resultados Brutos
IEEE Xplore	("zero trust" OR "zero trust architecture" OR ZTA OR ZTNA) AND (network* OR infrastructure OR cloud OR enterprise OR hybrid) AND (microsegment* OR "lateral movement" OR "policy decision point" OR "policy enforcement point" OR authentication OR "least privilege") AND (evaluation OR experiment OR implementation OR security OR performance)	Tipo: Artigos Revisados por Pares	89

Fonte: Elaborado pelos autores (2026)

A busca foi executada em 12 de Julho de 2026, nos campos Title, Abstract, Keywords, com aplicação dos filtros referentes ao período de publicação e ao tipo de documento. A estratégia inicial identificou 89 registros.

A utilização exclusiva da IEEE Xplore delimitou o mapeamento às evidências indexadas nessa fonte. Essa decisão metodológica foi considerada na interpretação dos resultados e nas limitações da revisão.

3.4 CRITÉRIOS DE ELEGIBILIDADE

Os critérios de elegibilidade foram definidos de acordo com o objetivo e as questões de pesquisa da revisão.

Foram incluídos estudos: (a) publicados em periódicos ou anais de conferências revisados por pares; (b) publicados entre 2022 e 2026; (c) relacionados diretamente à implementação ou avaliação da Arquitetura Zero Trust em infraestruturas de redes; (d) que investigassem mecanismos, componentes ou princípios associados à ZTA, como microsegmentação, controle de acesso orientado por identidade, menor privilégio, verificação contínua ou componentes de decisão e aplicação de políticas; e (e) que apresentassem protótipos, simulações, ambientes experimentais, *testbeds* ou estudos de caso com descrição dos mecanismos e dos resultados avaliados.

Foram excluídos: (a) estudos secundários, incluindo revisões de literatura; (b) documentos de natureza exclusivamente comercial e *white papers* de fornecedores sem processo de revisão por pares; (c) trabalhos relacionados à segurança de redes que não apresentassem associação explícita com princípios ou mecanismos da ZTA; e (d) estudos exclusivamente conceituais que não descrevessem ambiente de implementação, mecanismo investigado ou resultados de avaliação.

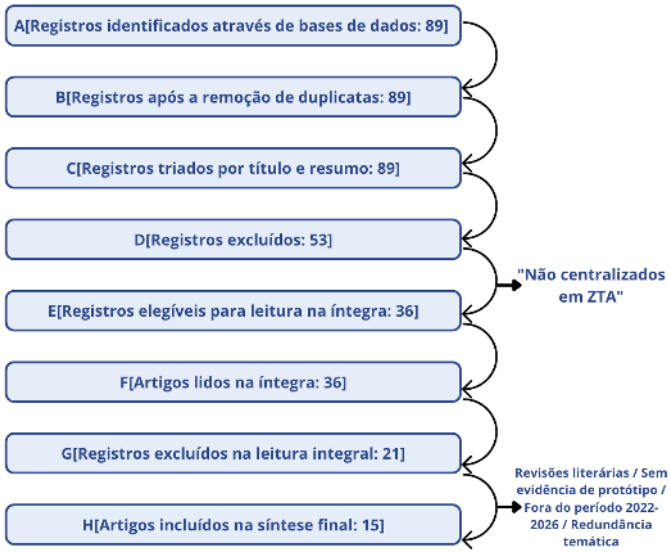
3.5 SELEÇÃO DOS ESTUDOS

O processo de seleção foi realizado em duas etapas. Inicialmente, os títulos e resumos dos 89 registros identificados foram examinados à luz dos critérios de elegibilidade. Nessa etapa, 53 registros foram excluídos, resultando em 36 estudos encaminhados para leitura integral.

Na segunda etapa, os 36 textos foram avaliados integralmente. Foram excluídos os estudos que, após a leitura completa, não apresentaram aderência ao objetivo da revisão ou não descreveram suficientemente o ambiente de implementação ou avaliação, o mecanismo Zero Trust investigado e os resultados utilizados na análise. Ao final do processo, 15 estudos compuseram o corpus da revisão.

As etapas de identificação, triagem e inclusão dos estudos foram organizadas em um diagrama de fluxo baseado no PRISMA-ScR (Ver Figura 1)

Figura 1. Fluxograma PRISMA-ScR do processo de seleção dos estudos.



Fonte: Elaborado pelos autores (2026) com base em Santos *et al.* (2026)

3.6 EXTRAÇÃO E SÍNTESE DOS DADOS

A extração dos dados foi realizada por meio de um formulário padronizado elaborado para esta revisão. Para cada estudo incluído, foram registrados: identificação bibliográfica; ano de publicação; contexto de infraestrutura; ambiente de implementação ou avaliação; mecanismo ou componente Zero Trust investigado; tecnologia de suporte utilizada; ameaça ou problema de segurança abordado; métricas de segurança; métricas de desempenho; principais resultados empíricos; desafios de implementação; limitações relatadas pelos autores; e lacunas de pesquisa identificadas.

Os dados extraídos foram organizados em uma matriz de análise e submetidos à síntese descritiva e categorização temática. Os mecanismos identificados foram agrupados de acordo com sua função predominante na arquitetura, enquanto as evidências empíricas foram caracterizadas a partir

das métricas e dos resultados relatados nos estudos. Os desafios de implementação foram sintetizados por recorrência temática, considerando aspectos de desempenho, escalabilidade, interoperabilidade, heterogeneidade dos dispositivos, gestão de identidade e complexidade operacional.

Essa estratégia permitiu relacionar as questões de pesquisa aos resultados da revisão e identificar tendências, concentrações temáticas e lacunas na literatura analisada.

3.7 SÍNTESE DAS EVIDÊNCIAS E ANÁLISE QUALITATIVA

Os dados extraídos dos estudos incluídos foram submetidos a uma síntese qualitativa descritiva e à categorização temática. A análise buscou identificar padrões recorrentes relacionados aos mecanismos da Arquitetura Zero Trust, aos contextos de implementação, às formas de avaliação e aos desafios relatados pelos estudos.

Como ferramenta auxiliar à organização e à consulta do corpus documental, utilizou-se a plataforma NotebookLM. A ferramenta apoiou a recuperação de informações e a consulta cruzada dos documentos analisados. Entretanto, a definição das categorias temáticas, a codificação dos achados e a interpretação das evidências foram realizadas pelos pesquisadores, mediante conferência das informações nos textos originais dos estudos. As respostas produzidas pela ferramenta não foram consideradas evidências independentes nem incorporadas aos resultados sem verificação na respectiva fonte primária.

A síntese dos dados foi organizada em quatro eixos analíticos. O primeiro eixo, denominado Mecanismos e componentes da ZTA, reuniu as abordagens técnicas empregadas na implementação dos princípios Zero Trust, incluindo microsegmentação, componentes de decisão e execução de políticas (PDP/PEP), controle de acesso baseado em identidade, princípio do menor privilégio e mecanismos de verificação contínua. Tecnologias utilizadas como suporte à implementação, como Redes Definidas por Software (SDN), aprendizado de máquina, identidades descentralizadas e mecanismos criptográficos adaptados a ambientes restritos, também foram categorizadas nesse eixo.

O segundo eixo, Contextos e ambientes de implementação, caracterizou as infraestruturas investigadas nos estudos. Foram considerados ambientes de computação em nuvem, computação de borda, Internet das Coisas (IoT), redes móveis e infraestruturas corporativas distribuídas. Essa categorização permitiu identificar diferenças nos requisitos e nas limitações associadas à aplicação da ZTA em ambientes com distintas capacidades computacionais e características de comunicação.

O terceiro eixo, Evidências e métricas de avaliação, reuniu os indicadores utilizados pelos estudos para avaliar segurança e desempenho. Foram registradas métricas relacionadas à latência, ao custo computacional, ao consumo energético, à sobrecarga de comunicação, ao desempenho dos

mecanismos de detecção e aos resultados associados à mitigação de ameaças. Os resultados quantitativos foram preservados conforme as definições e unidades apresentadas nos estudos originais, evitando comparações diretas entre métricas ou contextos experimentais não equivalentes.

O quarto eixo, Desafios e limitações de implementação, agrupou os obstáculos técnicos e operacionais relatados pelos estudos. Foram considerados aspectos relacionados à escalabilidade, à interoperabilidade, à heterogeneidade dos dispositivos, ao custo computacional, à integração com infraestruturas existentes, à gestão de identidades e à complexidade operacional.

A categorização foi utilizada como estrutura para a síntese narrativa dos achados. As ameaças abordadas pelos estudos, incluindo movimentação lateral, acessos não autorizados, ataques de negação de serviço e ataques do tipo *Man-in-the-Middle*, foram relacionadas aos respectivos mecanismos investigados e às métricas utilizadas na avaliação. Não foi realizada agregação estatística dos resultados, em razão da heterogeneidade dos ambientes experimentais, das arquiteturas e dos indicadores empregados nos estudos.

A Tabela 2 apresenta a síntese dos 15 artigos selecionados para compor o corpus desta revisão, detalhando o título de cada estudo, seu domínio de aplicação, os principais mecanismos ou componentes da Arquitetura Zero Trust investigados e as métricas de sucesso utilizadas pelos autores.

Tabela 2. Mapeamento técnico

Artigo	***Domínio***	***Mecanismo Principal***		***Principal Métrica de Sucesso***
Título	***Domínio de Aplicação***	***Componentes Analisados***		***Métricas Utilizadas***
UAV-Based Privacy-Preserved Trustworthy Seamless Service Agility for NextG Cellular Networks;	*Telecomunicações e Redes de Próxima Geração (NextG), com foco em situações de desastre ou falhas de rede*	*Autenticação mútua de todas as partes, delegação de autoridade (via assinatura de proxy, agindo como um PDP/PEP delegado no UAV) e gestão de identidades ocultas (ICAM/Privacidade através de CIDs)*	*IoT (UAVs) integrada a Redes Celulares NextG (4G/5G)*	*Latência (tempo total de configuração da conexão) e Escalabilidade (contagem total de mensagens transmitidas/recebidas)*
Future Industry Internet of Things with Zero-trust Security	*Industrial (Industrial IoT - IIoT)*	*PE (Policy Engine), PA (Policy Administrator), PEP (Policy Enforcement Point), SDP (Software Defined Perimeter) e ICAM (mecanismo de autenticação e identidade via BasIoT/Blockchain)*	*IoT (especificamente IIoT habilitada por 5G/6G) e Edge Computing*	*TPS (transações por segundo), uso de CPU e uso de memória*
Secure Enrollment Token Delivery Mechanism for Zero Trust Networks Using Blockchain	*Corporativo/Enterprise (focado em recursos organizacionais distribuídos)*	*ICAM (Gestão de Identidade, JWT e certificados X.509), PEP e PDP (representados pelo controlador e roteadores da rede overlay OpenZiti)*	*Nuvem e Híbrida (menciona infraestruturas locais, sites remotos e serviços em nuvem IaaS)*	*Latência (tempo total de conclusão - TCt) e estabilidade do sistema (tamanho da fila de transações por nó)*
Extension mechanism of overlay network	*Sistemas de Internet das*	*ICAM (gestão de identidade e credenciais via*	*IoT e Nuvem (Cloud)*	*Latência (overhead de processamento em ms),*

protocol to support digital authenticates	*Coisas (IoT) com foco em comunicações peer-to-peer seguras*	*PKI/certificados digitais) e autenticação mútua contínua através do protocolo CYPHONIC*		*Vazão (Throughput em Mbps) e Jitter*
Implementing Zero Trust Model for SSH Security with kerberos and OpenLDAP	*Administração de Sistemas e Segurança de Servidores*	*ICAM (Gerenciamento de Identidade e Acesso via Kerberos e OpenLDAP), mecanismos de autenticação e autorização (PDP/PEP funcional) e isolamento de rede*	*Corporativa local (utilizando servidores Debian 11 e ambientes de rede interna/externa)*	*Taxa de sucesso de autenticação (100% de êxito) e latência/tempo de resposta (duração média da autenticação em segundos)*
Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication	*Segurança de redes e gerenciamento de identidade digital em redes Zero Trust*	*Gerenciamento de Identidade, Credenciais e Acesso (ICAM), verificação contínua de confiança e tokens de autenticação*	*Corporativa local (testbed experimental em servidor Linux dedicado com Hyperledger Besu)*	*Tempo de execução/conclusão do processo MFA (latência) e custo de gás (gas costs) para operações em blockchain*
Decentralised Identity Management solution for zero-trust multi-domain Computing Continuum frameworks	*Compartilhamento de recursos e colaboração em cenários de computação multi-domínio (ex: projeto FLUIDOS)*	*PDP (Policy Decision Point), PEP (Policy Enforcement Point) e ICAM (Gerenciamento de Identidade Descentralizada via DIDs e Credenciais Verificáveis)*	*Computing Continuum (integrando Nuvem, Edge e IoT)*	*Latência (tempo de execução para geração de DID, emissão de credenciais e verificação) e overhead de comunicação (tamanho da mensagem em bytes)*
ZTA-IoT: A Novel Architecture for Zero-Trust in IoT Systems and an Ensuing Usage Control Model	*IoT em geral, demonstrado com casos de uso nos setores industrial (fábrica inteligente) e de saúde (smart healthcare)*	*PDP (Policy Decision Point), PEP (Policy Enforcement Point), Policy Engine (PE), Policy Administrator (PA) e fontes de dados como CDM, SIEM e Gerenciamento de Identidade*	*IoT habilitada para nuvem (cloud-enabled IoT), incluindo camadas de Objeto, Virtual-Objeto, Edge e Nuvem Pública*	*Latência (tempo médio de transmissão), tempo de processamento da função Lambda e tempo de resposta de consultas no DynamoDB*
Analysis of Azure Zero Trust Architecture Implementation for Mid-Size Organizations	*Corporativo (focado em organizações de médio porte)*	*PDP (Policy Decision Points), PEP (Policy Enforcement Points), Microsegmentação, e ICAM (utilizando Entra ID, MFA, Conditional Access, PIM e JIT)*	*Nuvem e Híbrida*	*Redução de incidentes de acesso privilegiado (30%), redução de tickets de suporte (20%) e taxa de alinhamento de permissões ao princípio de menor privilégio (98%)*
ZT-SDN: An ML-Powered Zero-Trust Architecture for Software-Defined Networks	*Redes organizacionais e corporativas*	*PDP (Ponto de Decisão de Política), PEP (Ponto de Execução de Política), PE (Motor de Política) e PA (Administração de Política)*	*Redes Definidas por Software (SDN), integrando aplicações e dispositivos IoT*	*Matriz de confusão (TP, TN, FP, FN), erro RMSE, distância DTW, throughput (vazão), contagem de mensagens Packet-In e tempo de processamento*
Zero-trust based dynamic access control for cloud computing	*Computação em nuvem e centros de dados em nuvem*	*PDP (Policy Decision Point), PEP (Policy Enforcement Point) e Avaliação de Confiança Dinâmica (Trust Assessment)*	*Nuvem (Cloud Computing), especificamente utilizando a plataforma OpenStack*	*Acurácia de autorização, Precisão, Recall, F1-score, curva ROC (AUC), erro de diferença temporal (TD) e pontuação CPE*
5G defense network using commercial gNodeB with zero trust architecture	*Militar/Defesa*	*Perímetro Definido por Software (SDP), incluindo os componentes SDP Controller (ZT Manager), SDP Initiating Host (IH) e SDP Accepting Host (AH)*	*Híbrida, integrando infraestrutura de rádio (gNodeB) comercial com uma rede de núcleo (Core*	*Throughput (vazão de dados), tempo de configuração de conexão (latência de acesso) e número de hosts visíveis na rede*

			Network) de defesa privada	
A lightweight zero-trust authentication architecture for IoT via unified enhanced FAST-SM9 and dynamic re-authentication	*Internet das Coisas (IoT) em sistemas distribuídos e heterogêneos*	*Re-autenticação dinâmica (zero-trust-DRA), mecanismo de gerenciamento de falhas (FMM), políticas de segurança multicamadas (MLSP) e gestão de identidade e tokens (DITGM/ICAM)*	*Cloud-Edge-End (Nuvem-Borda-Terminal) para IoT*	*Latência de autenticação, consumo de energia (mJ), sobrecarga de comunicação (bytes), taxa de falha e tempo de recuperação (segundos)*
Hybrid Machine Learning Anomaly Detection and Lightweight Zero Trust Authentication for LoRaWAN Networks	*Cidades inteligentes (estacionamento inteligente), agricultura de precisão e gestão de infraestrutura urbana*	*Autenticação Zero Trust baseada em Blockchain (ICAM), Avaliação Contínua de Confiança (Trust Score) e Resposta Adaptativa*	*IoT (redes LoRaWAN)*	*Acurácia (95.3%), AUC-ROC (0.973), latência de autenticação (187ms), consumo de energia (mJ), vida útil da bateria (anos) e disponibilidade do sistema*

Fonte: Elaborado pelos autores (2026).

3.8 CONSISTÊNCIA E INTERPRETAÇÃO DAS EVIDÊNCIAS

Considerando a finalidade de mapeamento característica das revisões de escopo, não foi realizada avaliação formal do risco de viés ou classificação da qualidade metodológica individual dos estudos incluídos. Essa decisão foi considerada na interpretação dos achados, evitando a atribuição de níveis de evidência ou a formulação de conclusões comparativas sobre a superioridade dos mecanismos analisados.

Para ampliar a consistência da síntese, os resultados relatados pelos estudos foram examinados em seus respectivos contextos de implementação e avaliação. Foram consideradas as características do ambiente experimental, a natureza da evidência produzida, os mecanismos Zero Trust investigados e as métricas utilizadas pelos autores. Resultados provenientes de simulações, protótipos, *testbeds* e estudos de caso foram preservados em suas categorias de origem, evitando a comparação direta entre evidências produzidas sob condições metodológicas distintas.

As evidências empíricas identificadas no corpus foram interpretadas em articulação com os princípios e componentes arquiteturais descritos no NIST SP 800-207. O documento normativo foi utilizado como referência conceitual para examinar a correspondência entre os mecanismos implementados nos estudos e os princípios da Arquitetura Zero Trust, não sendo tratado como estudo empírico ou incorporado ao corpus de artigos selecionados.

Durante a síntese, foi realizada a conferência das informações extraídas nos textos originais dos estudos. Os resultados quantitativos foram registrados de acordo com as métricas, unidades e condições experimentais descritas pelos respectivos autores. Quando identificadas limitações, desafios operacionais ou divergências entre os benefícios esperados da ZTA e os resultados observados nos

ambientes avaliados, essas informações foram registradas e categorizadas no eixo referente aos desafios e às limitações de implementação.

Esses procedimentos buscaram assegurar maior rastreabilidade à síntese e reduzir interpretações descontextualizadas dos resultados. Em razão da heterogeneidade dos desenhos experimentais e das métricas identificadas, as conclusões foram formuladas em caráter descritivo e interpretativo, considerando os limites do corpus e do delineamento adotado.

4 RESULTADOS E ANÁLISE

Esta seção apresenta a síntese dos dados extraídos dos 15 estudos científicos incluídos na revisão. Os resultados foram organizados de acordo com os eixos analíticos definidos na metodologia: mecanismos e componentes da Arquitetura Zero Trust (ZTA), contextos e ambientes de implementação, evidências e métricas de avaliação e desafios e limitações de implementação.

As diretrizes do NIST SP 800-207 foram utilizadas como referência conceitual para a interpretação dos mecanismos identificados, sem integrar o corpus de estudos empíricos. Considerando a heterogeneidade dos ambientes experimentais, das arquiteturas e das métricas empregadas, os resultados quantitativos são apresentados em seus respectivos contextos de origem, não sendo realizada agregação estatística ou comparação direta entre indicadores não equivalentes.

4.1 CARACTERIZAÇÃO DO CORPUS E CONTEXTOS DE IMPLEMENTAÇÃO

Os 15 estudos incluídos foram publicados entre 2022 e 2026. A distribuição temporal identificou dois estudos publicados em 2022 (13,3%), três em 2023 (20,0%), três em 2024 (20,0%), cinco em 2025 (33,3%) e dois em 2026 (13,3%). Observou-se maior concentração de publicações no biênio 2024–2025, que reuniu 53,3% do corpus analisado.

Os contextos de implementação mostraram-se heterogêneos, abrangendo Internet das Coisas (IoT), Internet das Coisas Industrial (IIoT), redes móveis 5G e de próxima geração, computação em nuvem, computação de borda e redes corporativas. Essa diversidade permitiu identificar diferentes formas de operacionalização dos princípios Zero Trust em infraestruturas com requisitos distintos de conectividade, desempenho e capacidade computacional.

Nos ambientes IoT, IIoT e de redes móveis, os estudos concentraram-se principalmente nas restrições de processamento, memória, consumo energético e mobilidade dos dispositivos. Em ambientes de nuvem e infraestruturas híbridas, predominaram investigações relacionadas à gestão de identidades, à aplicação dinâmica de políticas e ao controle de acesso. Nos contextos de redes

corporativas, destacaram-se a microsegmentação, o controle de fluxos e a limitação da movimentação lateral.

A natureza das evidências também apresentou variação. O corpus incluiu estudos baseados em simulações, protótipos, *testbeds* e estudos de caso. Essa característica possibilitou mapear diferentes abordagens de experimentação das soluções, embora as diferenças entre os ambientes e protocolos de avaliação limitem comparações diretas entre os resultados.

Tabela 3. Caracterização dos estudos incluídos na revisão

Ano	**Estudo**	**Contexto de implementação**	Mecanismo ou abordagem investigada	Natureza da evidência
2022	Abdel-Malek et al.	NextG / UAVs (Drones)	ZTA aplicada a redes móveis	Protótipo (srsRAN e USRPs)
2022	Li et al.	IIoT	Autenticação e criptografia leve	Protótipo e Simulação
2023	Rivera et al.	Redes distribuídas	Identidade e blockchain	Protótipo
2023	Matama et al.	Redes Overlay	Controle de comunicação Zero Trust	Protótipo
2023	Mediana et al.	Infraestrutura SSH	Autenticação e controle de acesso	Estudo de caso/Protótipo
2024	Rivera et al.	Gestão de Identidade Digital	MAF, ZKP e identidade descentralizada	Protótipo
2024	Murcia et al.	Cloud-Edge-IoT	Orquestração Zero Trust	Ambiente experimental
2024	Ameer et al.	IoT Habilitados para Nuvem	Controle de uso e políticas	Implementação
2025	Dakić et al.	Nuvem Corporativa	Identidade e menor privilégio	Estudo de caso
2025	Katsis & Bertino	SDN	Decisao dinâmica e política	Simulação e Protótipo
2025	Wang et al.	Computação em Nuvem	ML e aprendizado por reforco	Simulação
2025	Kim et al.	Redes 5G	SDP e controle de acesso	Simulação e *Testbed*
2025	Ma et al.	Cloud-Edge-End	Gestão dinâmica de confiança	Simulação e Protótipo
2026	Abdelhady et al.	LoRaWAN/IoT	Deteccao de anomalias	Simulação calibrada

2026	Hari N.N. et al.	Redes Corporativas	Microsegmentação	Estudo de Caso/Protótipo

Fonte: Elaborado pelo autor (2026).

4.2 MECANISMOS E COMPONENTES DA ARQUITETURA ZERO TRUST

A análise do corpus identificou diferentes mecanismos empregados na operacionalização dos princípios da ZTA. Entre as abordagens investigadas, destacaram-se a microsegmentação, o controle de acesso orientado por identidade, a aplicação dinâmica de políticas, a avaliação contínua das condições de acesso e os mecanismos de autenticação adaptados às características dos ambientes analisados.

Os estudos apresentaram componentes funcionalmente relacionados aos processos de decisão e aplicação de políticas descritos no NIST SP 800-207. Entretanto, nem todas as implementações adotaram explicitamente a nomenclatura *Policy Decision Point* (PDP) e *Policy Enforcement Point* (PEP). Em diferentes arquiteturas, controladores SDN, mecanismos de avaliação de confiança e serviços de gerenciamento de políticas desempenharam funções relacionadas à decisão de acesso, enquanto *gateways*, *switches*, agentes e elementos de borda atuaram na aplicação das decisões.

Além dos mecanismos estruturantes da ZTA, foram identificadas tecnologias de suporte destinadas a adaptar a arquitetura aos requisitos dos diferentes ambientes. Redes Definidas por Software (SDN) foram utilizadas para a aplicação programável de políticas; mecanismos baseados em blockchain e identidade descentralizada foram investigados nos processos de gestão de credenciais; técnicas de aprendizado de máquina foram empregadas na detecção de anomalias e avaliação dinâmica de confiança; e mecanismos criptográficos leves foram analisados em dispositivos com restrições de processamento e energia.

4.2.1 Microsegmentação e limitação da movimentação lateral

A microsegmentação foi investigada principalmente em redes corporativas e infraestruturas distribuídas. Hari N.N. et al. (2026) avaliaram uma abordagem de segmentação orientada por identidade em ambientes hospitalar e acadêmico. No cenário analisado, os autores relataram redução superior a 99% na métrica de Exposição de Conectividade Interna da Rede (ENICE) e redução de 99,7% no número de caminhos potenciais de ataque.

Os resultados foram associados à redução das relações de comunicação implicitamente permitidas entre os recursos da infraestrutura. A utilização de políticas vinculadas à identidade das cargas de trabalho restringiu a conectividade disponível entre segmentos e aumentou o número de decisões de acesso necessárias para alcançar recursos localizados em diferentes zonas da rede.

Esses resultados correspondem às topologias e às condições experimentais avaliadas pelo estudo. Dessa forma, os percentuais relatados não constituem estimativas gerais de redução da superfície de ataque aplicáveis a qualquer implementação de microsegmentação.

4.2.2 Orquestração de políticas e Redes Definidas por Software

As Redes Definidas por Software foram utilizadas como tecnologia de suporte à aplicação dinâmica das políticas de acesso. Katsis e Bertino (2025) investigaram uma arquitetura na qual o controlador SDN desempenha funções relacionadas à avaliação das condições de acesso e à atualização das regras de fluxo.

Nesse modelo, as regras podem ser modificadas a partir de informações relacionadas à identidade, ao comportamento observado e às políticas associadas aos recursos. Os elementos de encaminhamento da rede atuam na aplicação das decisões produzidas pelo plano de controle, desempenhando funções comparáveis às atribuídas aos PEPs no modelo abstrato do NIST.

Os estudos que empregaram SDN destacaram a programabilidade da infraestrutura e a possibilidade de atualização dinâmica das políticas. Entretanto, também foram identificados desafios relacionados à escalabilidade e à integração com equipamentos e sistemas que não oferecem suporte nativo aos mecanismos de controle programável.

4.2.3 Identidade descentralizada e mecanismos baseados em blockchain

Nos estudos relacionados à gestão de identidade, mecanismos baseados em blockchain foram empregados como suporte à distribuição, integridade e validação de credenciais. Diaz Rivera et al. (2023) e Rivera et al. (2024) investigaram abordagens que incorporaram identificadores descentralizados, contratos inteligentes e mecanismos criptográficos aos processos de autenticação.

As propostas buscaram reduzir a dependência de componentes centralizados de identidade e ampliar a rastreabilidade dos processos de distribuição e validação de credenciais. Em cenários experimentais controlados, foram avaliadas tentativas de interceptação e reutilização indevida de tokens, incluindo ataques do tipo *Man-in-the-Middle* e *Replay*.

Os resultados de segurança relatados foram acompanhados por variações no tempo necessário para os processos de validação. A latência mostrou-se dependente das características da arquitetura distribuída, do número de componentes envolvidos e dos procedimentos de confirmação utilizados.

4.2.4 Aprendizado de máquina e avaliação dinâmica de confiança

O aprendizado de máquina foi empregado em estudos voltados à detecção de comportamentos anômalos e à avaliação dinâmica das condições de confiança. Wang et al. (2025), Ma et al. (2025) e Abdelhady et al. (2026) investigaram diferentes abordagens computacionais destinadas a analisar padrões de tráfego, identificar alterações comportamentais e apoiar decisões de acesso.

Em ambiente LoRaWAN, Abdelhady et al. (2026) avaliaram modelos de detecção de anomalias adaptados às restrições dos dispositivos. A implementação relatada apresentou ocupação de memória de aproximadamente 59 KB, indicando viabilidade computacional no cenário experimental analisado.

Outros estudos investigaram mecanismos de pontuação dinâmica de confiança. Nos cenários avaliados, alterações nos padrões de acesso produziram redução dos escores atribuídos aos dispositivos, possibilitando a aplicação automática de políticas restritivas quando determinados limites de confiança eram alcançados.

Os resultados demonstram diferentes estratégias para incorporar informações comportamentais aos processos de decisão. Entretanto, os estudos utilizaram modelos, conjuntos de dados e critérios de avaliação distintos, limitando a comparação direta entre as abordagens.

4.2.5 Mecanismos criptográficos leves em dispositivos restritos

As restrições de energia, processamento e comunicação presentes em ambientes IoT motivaram a investigação de mecanismos criptográficos adaptados a dispositivos com recursos limitados. Li et al. (2022) avaliaram o FAST-SM9 em contexto de IIoT e redes 5G.

No cenário experimental relatado, o mecanismo apresentou redução de 63% no consumo energético em comparação a uma abordagem baseada em infraestrutura de chave pública com RSA-2048. Os autores relacionaram o resultado à redução das interações de comunicação e à integração de operações criptográficas durante os processos de autenticação.

Esse achado demonstra a relevância do consumo energético como dimensão de avaliação da ZTA em ambientes IoT. Entretanto, o resultado corresponde à configuração experimental específica e ao mecanismo comparador utilizado no estudo.

4.3 EVIDÊNCIAS E MÉTRICAS DE SEGURANÇA

Os estudos utilizaram diferentes indicadores para avaliar os efeitos dos mecanismos Zero Trust sobre a segurança das infraestruturas. Foram identificadas métricas relacionadas à exposição da conectividade interna, ao número de caminhos potenciais de ataque, ao comportamento da rede durante

ataques de negação de serviço, à adequação dos privilégios e à capacidade de detecção de comportamentos anômalos.

A Tabela 4 sintetiza resultados quantitativos selecionados. Os valores são apresentados conforme relatados nos estudos originais e devem ser interpretados considerando os respectivos ambientes, métricas e protocolos experimentais.

Tabela 4. Evidências e métricas de segurança relatadas nos estudos

Estudo	Contexto	Mecanismo	Métrica avaliada	Resultado relatado
Hari N.N. et al. (2026)	Redes hospitalar e acadêmica	Microsegmentação	ENICE	Redução superior a 99%
Hari N.N. et al. (2026)	Redes hospitalar e acadêmica	Microsegmentação	Caminhos potenciais de ataque	Redução de 99,7%
Kim et al. (2025)	Rede 5G	SDP	Throughput sob ataque	Manutenção acima de 65%
Dakić et al. (2025)	Nuvem corporativa	Menor privilégio	Alinhamento de permissões	98%
Mediana et al. (2023)	Infraestrutura SSH	Kerberos/OpenLDAP	Tentativas de força bruta	Bloqueio das tentativas avaliadas
Abdelhady et al. (2026)	LoRaWAN	Detecção de anomalias	Memória do modelo	Aproximadamente 59 KB

Fonte: Elaborado pelos autores (2026).

Os resultados evidenciam a diversidade dos desfechos utilizados na avaliação das implementações. Enquanto alguns estudos mensuraram alterações na topologia de exposição e nos caminhos de ataque, outros priorizaram indicadores relacionados à disponibilidade da rede, adequação de privilégios ou capacidade de detecção.

Nos cenários de microsegmentação, os indicadores foram direcionados à mensuração da conectividade potencialmente disponível entre os recursos. Em redes móveis, o comportamento do *throughput* durante ataques foi utilizado para analisar a capacidade de manutenção das comunicações. Nos estudos relacionados à identidade e ao controle de privilégios, foram empregadas métricas associadas à adequação das permissões e à prevenção de tentativas de acesso.

A heterogeneidade das métricas constitui uma característica relevante do corpus. Percentuais de redução de caminhos de ataque, indicadores de desempenho sob ataques e taxas de adequação de privilégios representam dimensões distintas da segurança. Consequentemente, esses valores não devem ser interpretados como medidas equivalentes de eficácia nem utilizados para estabelecer uma classificação direta entre os mecanismos analisados.

4.4 DESEMPENHO E IMPACTOS OPERACIONAIS

A implementação de mecanismos Zero Trust gerou impactos mensuráveis no desempenho, destacando-se latência, throughput, consumo energético e uso de memória. Na autenticação, a latência

variou conforme a complexidade: o estabelecimento de túneis foi mais rápido que o uso de certificados digitais ou identidades distribuídas, as quais dependem das características da rede e dos procedimentos de validação. Em testes corporativos com 1.000 usuários, a avaliação de políticas acrescentou cerca de 130 ms, reforçando que os custos operacionais dependem das condições experimentais específicas.

Nas redes móveis, mecanismos SDP (Kim et al., 2025) reduziram a transmissão inicial, mas garantiram resiliência em ataques de negação de serviço, mantendo o throughput superior a 65%. No contexto de IoT, a eficiência energética e de memória foi prioritária: o FAST-SM9 (Li et al., 2022) reduziu o consumo em 63% comparado ao RSA-2048, enquanto modelos para LoRaWAN demonstraram viabilidade com baixíssima ocupação de memória.

Em suma, os impactos operacionais variam conforme o contexto e o mecanismo. Soluções para dispositivos restritos focam em eficiência energética e memória, enquanto ambientes corporativos e distribuídos priorizam a latência e a capacidade de transmissão durante a aplicação das políticas.

4.5 DESAFIOS E LIMITAÇÕES DE IMPLEMENTAÇÃO

Os desafios da ZTA agrupam-se em quatro categorias: escalabilidade, heterogeneidade tecnológica, interoperabilidade e impacto operacional. A escalabilidade foi focada em mecanismos centralizados e avaliação contínua; contudo, apesar da viabilidade em protótipos, ainda faltam evidências em infraestruturas operacionais de grande escala por períodos prolongados.

A heterogeneidade tecnológica destaca-se em ambientes IoT e Edge, onde restrições de hardware exigem protocolos criptográficos leves e modelos de detecção com baixo consumo de recursos. A interoperabilidade é o principal desafio em ambientes híbridos com sistemas legados, muitas vezes requerendo intermediários como gateways ou proxies para integrar recursos sem suporte nativo. Além disso, a diversidade de tecnologias para gerir identidades e políticas demonstra uma padronização ainda limitada no setor.

Quanto ao impacto operacional, a experiência do usuário foi pouco investigada. Embora estudos em nuvem apontem dificuldades com MFA e autenticações recorrentes, a falta de dados centrados no usuário impede conclusões generalizadas sobre fadiga de autenticação ou redução da produtividade.

4.6 SÍNTESE DOS RESULTADOS

Esta revisão evidenciou uma grande diversidade de mecanismos, contextos e métricas na avaliação da Arquitetura Zero Trust (ZTA), abrangendo ambientes IoT, redes móveis, nuvem e redes corporativas com requisitos distintos de segurança e desempenho. Entre os principais mecanismos

destacam-se a microsegmentação, o controle de acesso orientado por identidade e a aplicação dinâmica de políticas, operacionalizados por tecnologias como SDN, blockchain, aprendizado de máquina e criptografia leve.

Os resultados quantitativos indicam benefícios claros na redução da exposição de recursos e na limitação da movimentação lateral. Entretanto, a implementação desses controles introduz impactos operacionais em latência, throughput e consumo energético, demonstrando que as características da infraestrutura influenciam diretamente a configuração dos mecanismos escolhidos.

A predominância de protótipos e simulações indica que ainda faltam avaliações em infraestruturas operacionais de grande escala, persistindo desafios de interoperabilidade e integração com sistemas legados. O achado central da revisão é a heterogeneidade das métricas de avaliação: a ausência de indicadores padronizados dificulta a comparação entre propostas e a consolidação de evidências sobre a eficácia da ZTA, configurando uma lacuna metodológica relevante para o avanço da área.

5 DISCUSSÃO

Os resultados desta revisão de escopo demonstram que a implementação da Arquitetura Zero Trust (ZTA) ocorre de maneira heterogênea e é diretamente influenciada pelas características das infraestruturas nas quais seus princípios são operacionalizados. Embora o NIST SP 800-207 estabeleça uma arquitetura abstrata e tecnologicamente agnóstica, os estudos analisados evidenciam diferentes estratégias para implementar mecanismos de decisão, execução de políticas, monitoramento e avaliação contínua das condições de acesso.

A diversidade das soluções identificadas reforça que a ZTA não corresponde a uma arquitetura tecnológica única ou a um conjunto fixo de ferramentas. Microsegmentação, Redes Definidas por Software (SDN), mecanismos de identidade descentralizada, aprendizado de máquina e protocolos criptográficos leves foram empregados para responder a requisitos específicos de segurança e desempenho. Nesse sentido, os achados indicam que a implementação da ZTA depende da adaptação dos princípios de verificação explícita, menor privilégio e avaliação contínua às características operacionais de cada ambiente.

5.1 DOS COMPONENTES ABSTRATOS À OPERACIONALIZAÇÃO DAS POLÍTICAS ZERO TRUST

A análise dos estudos revela que as implementações de Arquitetura Zero Trust (ZTA) utilizam diversos mecanismos para desempenhar as funções de Ponto de Decisão de Política (PDP) e Ponto de

Execução de Política (PEP) descritos no NIST SP 800-207. Enquanto controladores SDN e serviços de gestão de confiança atuam na decisão, elementos como switches e gateways aplicam as restrições de acesso. Como o modelo do NIST é abstrato, cabe a cada arquitetura definir como coletar e transformar dados de identidade, estado do dispositivo e contexto em decisões reais de acesso.

Nesse cenário, o aprendizado de máquina desempenha um papel central ao converter telemetria e padrões de tráfego em escores de confiança e detecção de anomalias, permitindo ajustes dinâmicos nas permissões. A eficácia dessas implementações adaptativas depende diretamente da disponibilidade e qualidade dos dados utilizados. Contudo, o uso de algoritmos introduz desafios críticos, como a necessidade de dados de treinamento representativos e o risco de falsos positivos, áreas que ainda demandam investigações futuras mais aprofundadas.

5.2 SEGURANÇA E DESEMPENHO COMO DIMENSÕES INTERDEPENDENTES

A revisão identifica uma relação direta entre o fortalecimento dos mecanismos de controle e os impactos no desempenho operacional. Processos como autenticação adicional, validação criptográfica e aplicação dinâmica de políticas podem introduzir latência, sobrecarga de comunicação e maior consumo de recursos computacionais. Em redes móveis, o uso de Perímetro Definido por Software (SDP) resultou em menor *throughput* em condições normais, mas garantiu maior resiliência e manutenção do tráfego durante ataques de negação de serviço.

Esses resultados reforçam que as métricas de desempenho não devem ser analisadas isoladamente, mas em conjunto com os objetivos de segurança. A relevância de uma redução na taxa de transmissão depende do nível de proteção alcançado e das necessidades da aplicação. Da mesma forma, a latência adicional gerada por certificados digitais ou identidades distribuídas pode ser aceitável em redes corporativas, mas inviável em sistemas sensíveis ao tempo ou comunicações críticas. Assim, o projeto de uma ZTA exige que segurança, latência e capacidade de processamento sejam tratadas como dimensões interdependentes, avaliando-se os custos operacionais em relação aos riscos que se pretende mitigar.

5.3 RESTRIÇÕES DE RECURSOS E ADAPTAÇÃO DA ZTA AOS AMBIENTES IOT

Os estudos sobre a Internet das Coisas (IoT) demonstram que a aplicação dos princípios Zero Trust em dispositivos com recursos restritos exige adaptações arquiteturais e computacionais. Sensores e dispositivos de borda possuem limitações de processamento, memória e energia que dificultam a utilização direta de mecanismos projetados para infraestruturas de nuvem. Nesse cenário, mecanismos

criptográficos leves surgem como alternativa: o uso do FAST-SM9, por exemplo, reduziu o consumo energético em 63% comparado ao RSA-2048, devido à otimização das operações e comunicações.

A detecção de anomalias também precisou ser adequada, utilizando modelos de baixa ocupação de memória (como 59 KB em redes LoRaWAN) para permitir análises comportamentais em hardware limitado. Entretanto, a viabilidade experimental não elimina desafios práticos como a atualização de modelos e a coleta de telemetria em redes distribuídas.

A análise reforça que mecanismos para alta capacidade computacional são inapropriados para dispositivos IoT, pois processos complexos de validação geram custos de processamento incompatíveis com sensores a bateria. Assim, os resultados indicam a necessidade de distribuir as funções de decisão e execução de políticas entre nuvem, borda e dispositivos finais. O uso de arquiteturas hierárquicas ou distribuídas permite preservar os princípios Zero Trust sem transferir integralmente o custo computacional aos dispositivos restritos.

5.4 MICROSEGMENTAÇÃO E CONTENÇÃO DA MOVIMENTAÇÃO LATERAL

A microsegmentação reduziu significativamente a exposição entre recursos e a movimentação lateral. No estudo de Hari N.N. et al. (2026), observou-se uma redução superior a 99% na exposição de conectividade interna (ENICE) e de 99,7% nos caminhos potenciais de ataque. Embora esses resultados dependam de topologias e condições experimentais específicas, eles provam que limitar comunicações implicitamente autorizadas restringe drasticamente o alcance de ativos comprometidos.

A principal contribuição da microsegmentação não é eliminar o risco, mas conter o impacto de um comprometimento, exigindo novas validações de acesso ao longo da infraestrutura. Isso converge com os princípios de menor privilégio e autorização explícita. Entretanto, a aplicação de políticas granulares pode ser dificultada por dependências entre sistemas, fluxos pouco documentados e equipamentos legados. Assim, os benefícios reais dependem da capacidade organizacional de identificar ativos e manter o mapeamento de fluxos rigorosamente atualizado.

5.5 IDENTIDADE DESCENTRALIZADA E OS CUSTOS DA VALIDAÇÃO DISTRIBUÍDA

Estudos sobre blockchain e identidade descentralizada utilizam identificadores descentralizados e contratos inteligentes para garantir a integridade de credenciais sem depender de órgãos centrais. Embora eficazes contra interceptações e o uso indevido de tokens, esses métodos enfrentam uma tensão entre descentralização e velocidade, apresentando latências que podem dificultar a autorização em tempo real.

A solução sugerida é a separação funcional: o blockchain atuaria na governança e manutenção da integridade da identidade, enquanto componentes posicionados próximos aos recursos processariam decisões de acesso sensíveis à latência. Pesquisas futuras devem focar em arquiteturas híbridas para determinar sob quais condições experimentais essa combinação de controle local e identidade descentralizada oferece os melhores benefícios.

5.6 INTEROPERABILIDADE E INTEGRAÇÃO COM INFRAESTRUTURAS LEGADAS

A integração da ZTA com infraestruturas existentes é um desafio recorrente, pois muitos ambientes organizacionais possuem sistemas legados que não suportam nativamente tecnologias como SDN e funções de rede virtualizadas. Para contornar isso, a aplicação dos princípios Zero Trust exige camadas intermediárias, como agentes, gateways ou proxies, para mediar o acesso aos recursos antigos. Embora viabilizem a integração, esses componentes aumentam a complexidade operacional, introduzem latência e demandam monitoramento constante.

A heterogeneidade das arquiteturas e a falta de padronização em interfaces e métricas dificultam a interoperabilidade entre mecanismos de decisão e aplicação de políticas de diferentes ecossistemas. Consequentemente, os achados indicam que a adoção da ZTA tende a ser incremental, com a incorporação progressiva de mecanismos de identidade e segmentação sobre o ambiente heterogêneo, em vez de uma substituição imediata de toda a infraestrutura.

Esse processo exige um planejamento arquitetural rigoroso e o mapeamento detalhado dos fluxos e dependências entre sistemas. A implementação de políticas granulares sem esse conhecimento prévio pode causar interrupções operacionais ou exigir exceções que reduzam a consistência e a eficácia dos controles de acesso.

5.7 EXPERIÊNCIA DO USUÁRIO COMO DIMENSÃO AINDA POUCO INVESTIGADA

Embora a verificação contínua seja central na ZTA, a experiência do usuário foi pouco examinada no corpus analisado. Os estudos focaram em métricas técnicas de segurança e desempenho, negligenciando indicadores de usabilidade e percepção do usuário. Um estudo em nuvem relatou desafios com autenticações recorrentes e MFA, mas a escassez de avaliações centradas no usuário impede generalizações sobre fadiga de autenticação ou perda de produtividade.

Esta ausência de evidências é uma lacuna relevante, pois a eficácia da segurança depende de como os controles são incorporados à rotina dos usuários. Processos muito intrusivos podem prejudicar a adoção, exigindo mecanismos de menor fricção que mantenham o rigor da autorização. Assim, pesquisas futuras devem integrar métricas de experiência do usuário e impacto organizacional,

investigando autenticação contextual, estratégias adaptativas e mecanismos *passwordless* com a participação efetiva dos usuários.

5.8 LIMITAÇÕES DAS EVIDÊNCIAS E DESAFIOS DE GENERALIZAÇÃO

A predominância de protótipos e simulações limita a generalização dos achados para infraestruturas reais de grande escala e longo prazo. Resultados quantitativos expressivos obtidos em ambientes controlados podem variar diante de mudanças no tráfego ou eventos legítimos não previstos nos modelos iniciais.

A heterogeneidade das métricas de segurança e desempenho é identificada como a principal lacuna da área, pois a diversidade de indicadores impede a comparação direta entre diferentes arquiteturas e a consolidação das evidências. Para avançar, o texto sugere a padronização de métricas e cenários de referência que permitam avaliações mais comparáveis, reproduzíveis e integradas.

5.9 SÍNTESE DA DISCUSSÃO

Esta revisão indica que as implementações de ZTA dependem estritamente do contexto tecnológico, não havendo uma configuração única para ambientes corporativos, nuvem ou IoT. Enquanto redes corporativas focam em microsegmentação para conter movimentos laterais, ambientes IoT priorizam a eficiência energética e a baixa sobrecarga de comunicação.

Segurança e desempenho são dimensões interdependentes, onde o fortalecimento da verificação introduz custos operacionais e desafios de integração com sistemas legados. Assim, a ZTA deve ser vista como um conjunto de mecanismos adaptáveis que equilibram identidade, desempenho e interoperabilidade, em vez de uma solução de superioridade universal.

Persiste uma lacuna entre a viabilidade experimental e a aplicação em infraestruturas operacionais de larga escala, dificultada pela falta de métricas padronizadas para comparação. O avanço da área requer a padronização de indicadores, a ampliação de estudos longitudinais e a incorporação de fatores como usabilidade e impacto organizacional.

6 CONCLUSÃO

Esta revisão de escopo mapeou os mecanismos, as evidências empíricas e os desafios relacionados à implementação da Arquitetura Zero Trust (ZTA) em infraestruturas de redes, considerando 15 estudos científicos publicados entre 2022 e 2026. Os achados demonstraram que a operacionalização dos princípios Zero Trust assume diferentes configurações conforme o contexto tecnológico, os requisitos de segurança e as limitações de desempenho das infraestruturas investigadas.

Os estudos analisados concentraram-se em mecanismos relacionados à microsegmentação, ao controle de acesso orientado por identidade, à aplicação dinâmica de políticas e à avaliação contínua das condições de acesso. Foram identificados componentes funcionalmente associados aos processos de decisão e execução de políticas descritos no NIST SP 800-207, embora nem todas as implementações adotassem explicitamente a terminologia *Policy Decision Point* (PDP) e *Policy Enforcement Point* (PEP). Tecnologias como Redes Definidas por Software (SDN), blockchain, aprendizado de máquina e mecanismos criptográficos leves foram empregadas como recursos de suporte à operacionalização da ZTA em ambientes de nuvem, redes corporativas, Internet das Coisas (IoT), computação de borda e redes móveis.

Em relação às evidências de segurança, os estudos relataram resultados associados à redução da exposição entre recursos, à limitação dos caminhos potenciais de movimentação lateral, ao controle de privilégios e à identificação de comportamentos anômalos. Entre os resultados quantitativos mapeados, destacaram-se reduções superiores a 99% na exposição da conectividade interna e de 99,7% no número de caminhos potenciais de ataque em um cenário específico de microsegmentação. Esses valores, entretanto, correspondem às topologias, métricas e condições experimentais dos respectivos estudos e não devem ser interpretados como estimativas gerais de eficácia aplicáveis a todas as implementações Zero Trust.

As métricas utilizadas na avaliação das soluções apresentaram elevada heterogeneidade. Foram identificados indicadores relacionados à exposição da infraestrutura, aos caminhos de ataque, à detecção de anomalias, ao controle de privilégios, à latência, ao *throughput*, ao consumo energético e à utilização de recursos computacionais. Essa diversidade evidencia a natureza multidimensional da avaliação de arquiteturas Zero Trust, mas também limita a comparação direta entre propostas e dificulta a consolidação de estimativas agregadas sobre sua efetividade.

Os resultados também demonstraram que a ampliação dos mecanismos de verificação e controle pode introduzir impactos operacionais. Processos adicionais de autenticação, validação criptográfica, análise contextual e aplicação dinâmica de políticas apresentaram efeitos sobre a latência, a sobrecarga de comunicação e o consumo de recursos. Em ambientes IoT e dispositivos com capacidade computacional restrita, a eficiência energética assumiu particular relevância, favorecendo a investigação de mecanismos criptográficos leves e modelos de detecção adaptados às limitações de hardware. Em infraestruturas corporativas e distribuídas, destacaram-se desafios relacionados à interoperabilidade, à integração com sistemas legados e à gestão de políticas.

Dessa forma, os achados indicam que a ZTA não deve ser compreendida como uma solução tecnológica única ou como um modelo de implantação uniforme. Sua implementação depende da

seleção e da adaptação de mecanismos de identidade, segmentação, decisão e execução de políticas às características de cada infraestrutura. As evidências mapeadas apresentam resultados favoráveis em contextos específicos, mas permanecem fragmentadas entre diferentes mecanismos, ambientes experimentais e métricas de avaliação.

A predominância de protótipos, simulações e *testbeds* constitui uma limitação relevante do conjunto de evidências analisado. Permanecem reduzidas as avaliações longitudinais conduzidas em infraestruturas operacionais de grande escala, assim como estudos que examinem conjuntamente segurança, desempenho, interoperabilidade e experiência do usuário. Adicionalmente, a utilização exclusiva da base IEEE Xplore delimita o alcance do corpus desta revisão e deve ser considerada na interpretação e na generalização dos achados.

Como direcionamento para pesquisas futuras, destaca-se a necessidade de desenvolver conjuntos padronizados de métricas e cenários de referência para a avaliação de implementações Zero Trust, possibilitando a análise integrada de segurança, desempenho e impacto operacional. Estudos conduzidos em infraestruturas de grande escala e durante períodos prolongados podem ampliar a compreensão sobre escalabilidade, estabilidade e integração com sistemas legados. Também se mostram relevantes investigações sobre mecanismos adaptativos de avaliação de confiança, detecção distribuída de anomalias e abordagens de autenticação contextual capazes de reduzir a fricção para os usuários sem comprometer os requisitos de segurança.

Conclui-se que a literatura analisada apresenta avanços relevantes na operacionalização dos princípios da Arquitetura Zero Trust em diferentes infraestruturas de redes. Entretanto, o estado atual das evidências ainda não permite estabelecer uma configuração universalmente superior ou estimar, de forma agregada, a efetividade da ZTA. O principal desafio científico identificado reside na transição de resultados obtidos em ambientes experimentais heterogêneos para evidências comparáveis, reproduzíveis e produzidas em infraestruturas operacionais de maior escala. Nesse sentido, a consolidação da ZTA como abordagem de segurança depende não apenas do desenvolvimento de novos mecanismos tecnológicos, mas também do avanço de métodos padronizados de avaliação capazes de demonstrar, em condições operacionais, seus benefícios, custos e limitações.

REFERÊNCIAS

ABDEL-MALEK, M. A.; SAYED, M. M.; AZAB, M. UAV-Based Privacy-Preserved Trustworthy Seamless Service Agility for NextG Cellular Networks. **Sensors**, [S. l.], v. 22, n. 2756, p. 1-19, 2022.

ABDELHADY, G. et al. Hybrid Machine Learning Anomaly Detection and Lightweight Zero Trust Authentication for LoRaWAN Networks. **IEEE Access**, [S. l.], v. 14, p. 1-15, 2026.

AMEER, S. et al. ZTA-IoT: A Novel Architecture for Zero-Trust in IoT Systems and an Ensuing Usage Control Model. **ACM Transactions on Privacy and Security**, [S. l.], v. 27, n. 3, art. 22, p. 1-36, ago. 2024.

DOKIĆ, V. et al. Analysis of Azure Zero Trust Architecture Implementation for Mid-Size Organizations. **Journal of Cybersecurity and Privacy**, [S. l.], v. 5, n. 2, p. 1-41, 2025.

HARI, N. N. et al. A three-tier microsegmentation framework for enterprise networks under Zero Trust Architecture. **Alexandria Engineering Journal**, [S. l.], v. 141, p. 150–164, 2026.

KATSIS, C.; BERTINO, E. ZT-SDN: An ML-Powered Zero-Trust Architecture for Software-Defined Networks. **ACM Transactions on Privacy and Security**, [S. l.], v. 28, n. 2, art. 23, p. 1-35, fev. 2025.

KIM, W. et al. 5G defense network using commercial gNodeB with zero trust architecture. **ETRI Journal**, [S. l.], v. 47, p. 445–458, 2025.

LI, S.; IQBAL, M.; SAXENA, N. Future Industry Internet of Things with Zero-trust Security. **Information Systems Frontiers**, [S. l.], v. 26, p. 1653–1666, 2024.

MA, Z. et al. A lightweight zero-trust authentication architecture for IoT via unified enhanced FAST-SM9 and dynamic re-authentication. **PLoS ONE**, [S. l.], v. 20, n. 10, p. 1-25, 2025.

MATAMA, K. et al. Extension Mechanism of Overlay Network Protocol to Support Digital Authenticates. [S. l.: s. n.], 2023.

MEDIANA, S. D.; LINDAWATI; FADHLI, M. Implementing Zero Trust Model for SSH Security with kerberos and OpenLDAP. **Sistemasi: Jurnal Sistem Informasi**, [S. l.], v. 12, n. 3, p. 981-995, set. 2023.

MURCIA, J. M. B. et al. Decentralised Identity Management solution for zero-trust multi-domain Computing Continuum frameworks. **Future Generation Computer Systems**, [S. l.], v. 162, p. 1-18, 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Zero Trust Architecture**. Gaithersburg: NIST, 2020. (NIST Special Publication 800-207).

RIVERA, J. J. D. et al. Secure Enrollment Token Delivery Mechanism for Zero Trust Networks Using Blockchain. **IEICE Transactions on Communications**, [S. l.], v. E106–B, n. 12, p. 1293-1301, dez. 2023..

RIVERA, J. J. D.; MUHAMMAD, A.; SONG, W.-C. Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication. **IEEE Open Journal of the Communications Society**, [S. l.], v. 5, p. 2509-2525, 2024.

SANTOS, Wilker José Caminha dos; CAMARGO, Franco Feitosa Corrêa de; PICANÇO, Ailson Renan Santos; CONTE, Thiago Nicolau Magalhães de Souza; LOPES, Rogério Santiago; COUTINHO, Rosemary Maria Pimentel; SEIXAS, Vitória Nazaré Costa; SILVA, Elzelis Muller da; LIMA, Patrícia Danielle Lima de. MODELO INTELIGENTE BASEADO EM APRENDIZADO FEDERADO E VISÃO COMPUTACIONAL COM DADOS SIMULADOS PARA O DIAGNÓSTICO DISTRIBUÍDO DE DOENÇAS DO CACAUEIRO EM COOPERATIVAS DA AMAZÔNIA LEGAL. Veredas do Direito, *[S. l.]*, v. 23, n. 11, p. e237511, 2026. DOI: 10.18623/rvd.v23.7511. Disponível em: https://revista.domhelder.edu.br/index.php/veredas/article/view/7511. Acesso em: 19 jul. 2026.

WANG, R. et al. Zero-trust based dynamic access control for cloud computing. **Cybersecurity**, [S. l.], v. 8, n. 12, p. 1-16, 2025..