ARQUITETURA ZERO TRUST: UMA REVISÃO INTEGRATIVA SOBRE PRINCÍPIOS, COMPONENTES E APLICAÇÕES NA SEGURANÇA DE REDES CONTEMPORÂNEAS

Rafael Braga Monteiro Dos Santos[1]

[1]*Universidade de Uberaba (Uniube), Uberaba–MG, Brasil (rafaelbms@edu.uniube.br)*

Resumo: A arquitetura Zero Trust emerge como paradigma central de segurança de redes contemporâneas, substituindo modelos baseados em perímetro. Este trabalho apresenta revisão integrativa sobre o tema, abordando origem do conceito, princípios fundamentais, componentes definidos pelo NIST SP 800-207 e aplicações modernas. Conclui-se que Zero Trust representa evolução necessária à proteção de ambientes híbridos, em nuvem e com forte mobilidade de usuários.

Palavras-chave: Zero Trust; segurança de redes; cibersegurança; NIST SP 800-207; controle de acesso.

INTRODUÇÃO

A crescente complexidade dos ambientes computacionais corporativos, marcada pela adoção massiva de computação em nuvem, dispositivos móveis, trabalho remoto e Internet das Coisas (IoT), evidenciou as limitações dos modelos tradicionais de segurança de redes. O paradigma clássico de proteção, fundamentado na metáfora do castelo e fosso — em que se presume que tudo que se encontra dentro do perímetro corporativo é confiável e tudo que está fora é potencialmente malicioso — mostra-se insuficiente diante das ameaças contemporâneas, especialmente aquelas oriundas de movimentação lateral de atacantes e de comprometimento de credenciais legítimas (Nakamura; Geus, 2007; Stallings, 2015).

Nesse contexto, o conceito de Zero Trust — formulado inicialmente por John Kindervag, em 2010 (Kindervag, 2010), e posteriormente sistematizado pelo National Institute of Standards and Technology (NIST) na publicação SP 800-207 (Rose et al., 2020) — propõe uma mudança paradigmática: em vez de confiar implicitamente em usuários, dispositivos ou recursos com base em sua localização na rede, todo acesso deve ser continuamente verificado, autenticado e autorizado, independentemente da origem da requisição. O lema “nunca confiar, sempre verificar” sintetiza essa filosofia, fundamentada no princípio do menor privilégio e na verificação contínua de atributos relativos à identidade, ao dispositivo e ao contexto da requisição (Buck et al., 2021; Syed et al., 2022).

Diante desse panorama, o presente trabalho tem como objetivo apresentar uma revisão integrativa sobre a arquitetura Zero Trust, contemplando: (i) a origem e a evolução histórica do conceito; (ii) os princípios fundamentais que sustentam o modelo; (iii) os componentes lógicos e funcionais definidos pelo NIST SP 800-207; e (iv) os principais cenários de aplicação, desafios e tendências contemporâneas. Espera-se contribuir para a sistematização do conhecimento sobre o tema e para a reflexão sobre sua relevância na formação acadêmica em engenharia de computação, engenharia de telecomunicações, engenharia elétrica e engenharia eletrônica, áreas frequentemente envolvidas no projeto e na operação de redes seguras.

MATERIAL E MÉTODOS

O presente estudo caracteriza-se como uma revisão integrativa da literatura, abordagem metodológica que possibilita reunir, sintetizar e avaliar criticamente produções acadêmicas, técnicas e normativas sobre um determinado tema, sustentando inferências consistentes acerca do estado da arte. A pesquisa foi conduzida entre janeiro e maio de 2026, mediante consulta às bases Google Scholar, IEEE Xplore, ACM Digital Library e SciELO, além da documentação técnica oficial do NIST e da Cybersecurity and Infrastructure Security Agency (CISA). Os descritores empregados, em português e em inglês, incluíram: “Zero Trust”, “Zero Trust Architecture”, “confiança zero”, “segurança de redes” e “NIST SP 800-207”, combinados por meio dos operadores booleanos AND e OR. Foram considerados, como critérios de inclusão, obras publicadas preferencialmente entre 2018 e 2025, com ênfase em revisões sistemáticas, surveys e publicações normativas de referência, admitindo-se ainda obras clássicas da área de segurança de redes,

independentemente do ano de publicação. A seleção dos estudos seguiu as etapas de (i) identificação por meio das buscas nas bases; (ii) triagem por título, resumo e palavras-chave; (iii) leitura integral dos textos elegíveis; e (iv) síntese qualitativa dos achados quanto à fundamentação teórica, à descrição dos componentes da arquitetura e às aplicações relatadas, organizada nos quatro eixos discutidos a seguir.

RESULTADOS E DISCUSSÃO

A revisão da literatura permitiu organizar a discussão em quatro eixos complementares: (i) origem e evolução do conceito Zero Trust; (ii) princípios fundamentais; (iii) componentes da arquitetura conforme o NIST SP 800-207; e (iv) aplicações, desafios e tendências contemporâneas.

Origem e evolução do conceito Zero Trust. As raízes do Zero Trust remontam ao início dos anos 2000, com as discussões sobre desperimetrização promovidas pelo Jericho Forum, grupo que defendia a redução da dependência da segurança baseada em fronteiras de rede (Stallings, 2015). O termo "Zero Trust" foi cunhado, em 2010, pelo analista John Kindervag, então pesquisador da Forrester Research, em resposta às limitações observadas no modelo tradicional de segurança perimetral (Kindervag, 2010). Em 2014, a Google publicou o modelo BeyondCorp (Ward; Beyer, 2014), considerado a primeira implementação corporativa em larga escala dos princípios Zero Trust e que demonstrou ser viável fornecer acesso seguro a aplicações internas sem o uso de redes privadas virtuais (VPN) tradicionais. Posteriormente, em agosto de 2020, a publicação do documento NIST SP 800-207 — Zero Trust Architecture consolidou a base conceitual e arquitetural do modelo, transformando-o em referência para órgãos governamentais e organizações privadas em escala global (Rose et al., 2020). Em paralelo, esforços normativos complementares, como o Zero Trust Maturity Model da CISA (2023) e o guia de implementação NIST SP 1800-35 (Kerman et al., 2025), ampliaram o arcabouço de orientação prática para a adoção do modelo.

Princípios fundamentais. Conforme estabelecido pela publicação do NIST (Rose et al., 2020), o Zero Trust fundamenta-se em sete princípios centrais, sintetizados no Quadro 1. Esses princípios orientam o desenho de arquiteturas seguras independentemente da topologia de rede ou da localização dos recursos.

Quadro 1. Princípios fundamentais da arquitetura Zero Trust.

Princípio	Descrição sintética
Recursos como dados	Todos os ativos digitais são tratados como recursos a proteger
Comunicação segura	Toda comunicação é protegida independentemente da rede
Acesso por sessão	O acesso a recursos é concedido por sessão, com privilégio mínimo
Política dinâmica	Decisões consideram identidade, dispositivo, contexto e comportamento
Monitoramento de ativos	A organização monitora a postura de segurança de seus ativos
Autenticação contínua	Autenticação e autorização são reavaliadas continuamente
Coleta de informações	Dados sobre estado, comunicação e ameaças melhoram a postura de segurança

Componentes da arquitetura conforme o NIST SP 800-207. Em termos funcionais, a arquitetura Zero Trust organiza-se em torno de três componentes lógicos principais (Rose et al., 2020). O Policy Engine (PE) é responsável pela decisão final sobre a concessão de acesso a um recurso, considerando políticas previamente estabelecidas e sinais contextuais em tempo real. O Policy Administrator (PA) executa a decisão tomada pelo PE, estabelecendo ou encerrando a sessão entre o sujeito e o recurso. O Policy Enforcement Point (PEP), por sua vez, atua como o ponto de aplicação da política, sendo responsável por habilitar, monitorar e, eventualmente, encerrar a conexão. Esses componentes operam de forma articulada, alimentados por fontes de dados externas que incluem sistemas de gestão de identidades e acessos (IAM), repositórios de inteligência de ameaças, sistemas de gerenciamento de eventos e informações de segurança (SIEM), bem como ferramentas de análise comportamental e de avaliação de postura de dispositivos (Syed et al., 2022). Em complemento, o guia de implementação NIST SP 1800-35 (Kerman et al., 2025) operacionaliza essa arquitetura de

referência por meio de dezenove cenários demonstrativos desenvolvidos em colaboração com a indústria, fornecendo modelos replicáveis para diferentes níveis de maturidade.

Aplicações, desafios e tendências. A literatura especializada aponta a aplicação da arquitetura Zero Trust em diversos cenários, com destaque para a proteção de ambientes em nuvem híbrida, o suporte ao trabalho remoto seguro, o controle de acesso a aplicações corporativas, a segurança em ambientes de Internet das Coisas (IoT) e a proteção de infraestruturas críticas (Syed et al., 2022; CISA, 2023). A microsegmentação — isto é, o particionamento lógico da rede em zonas menores, cada uma com políticas de acesso independentes — figura como técnica central para a contenção da movimentação lateral de atacantes. Entre os principais desafios destacam-se a complexidade de implementação em ambientes legados, a necessidade de integração entre múltiplas ferramentas, a maturidade do gerenciamento de identidades e o impacto sobre a experiência do usuário (Sêmola, 2014). Revisões recentes ressaltam, ainda, que persistem lacunas de pesquisa relevantes, sobretudo quanto à mensuração empírica dos ganhos efetivos de segurança proporcionados pela adoção do modelo e à padronização de métricas de maturidade comparáveis entre organizações (Buck et al., 2021). Tendências contemporâneas apontam para a integração entre Zero Trust e tecnologias emergentes, como a inteligência artificial aplicada à análise comportamental, a automação de políticas de segurança e os modelos Secure Access Service Edge (SASE), que convergem capacidades de rede e segurança em uma única solução baseada em nuvem.

CONCLUSÃO

A revisão integrativa permitiu identificar a arquitetura Zero Trust como uma resposta consistente às limitações dos modelos tradicionais de segurança baseados em perímetro, especialmente diante de ambientes corporativos caracterizados pela computação em nuvem, mobilidade e proliferação de dispositivos. Os sete princípios consolidados pelo NIST SP 800-207, os componentes lógicos da arquitetura (Policy Engine, Policy Administrator e Policy Enforcement Point) e a ênfase na verificação contínua de identidade e contexto representam pilares fundamentais para o desenho de redes mais resilientes. Cabe ressaltar, contudo, que a adoção do Zero Trust não constitui um produto isolado, mas uma estratégia de longo prazo, dependente de governança, integração tecnológica e maturidade organizacional, conforme reforçam os arcabouços normativos mais recentes (Kerman et al., 2025; CISA, 2023). Como direções para trabalhos futuros, sugere-se a investigação empírica de implementações em diferentes contextos organizacionais brasileiros, o desenvolvimento de métricas comparáveis de maturidade Zero Trust e o estudo da integração entre o modelo, a computação em borda e a inteligência artificial aplicada à cibersegurança.

AGRADECIMENTOS

Agradeço à Universidade de Uberaba (Uniube) pelo apoio acadêmico que tornou possível a realização deste trabalho.

REFERÊNCIAS

BUCK, C.; OLENBERGER, C.; SCHWEIZER, A.; VÖLTER, F.; EYMANN, T. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. Computers & Security, v. 110, 102436, 2021. Disponível em: https://doi.org/10.1016/j.cose.2021.102436.

CISA — CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. Zero Trust Maturity Model: Version 2.0. Washington, DC: U.S. Department of Homeland Security, 2023. Disponível em: https://www.cisa.gov/zero-trust-maturity-model.

KERMAN, A.; SOUPPAYA, M.; GRAYELI, P.; SYMINGTON, S. Implementing a Zero Trust Architecture. NIST Special Publication 1800-35. Gaithersburg: National Institute of Standards and Technology, 2025. Disponível em: https://doi.org/10.6028/NIST.SP.1800-35.

KINDERVAG, J. No more chewy centers: Introducing the Zero Trust Model of information security. Forrester Research, Cambridge, 2010.

NAKAMURA, E. T.; GEUS, P. L. de. Segurança de redes em ambientes cooperativos. São Paulo: Novatec, 2007.

ROSE, S.; BORCHERT, O.; MITCHELL, S.; CONNELLY, S. Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg: National Institute of Standards and Technology, 2020. Disponível em: https://doi.org/10.6028/NIST.SP.800-207.

SÊMOLA, M. Gestão da segurança da informação: uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2014.

STALLINGS, W. Criptografia e segurança de redes: princípios e práticas. 6. ed. São Paulo: Pearson, 2015.

SYED, N. F.; SHAH, S. W.; SHAGHAGHI, A.; ANWAR, A.; BAIG, Z.; DOSS, R. Zero Trust Architecture (ZTA): A comprehensive survey. IEEE Access, v. 10, p. 57143-57179, 2022.

Disponível em: https://doi.org/10.1109/ACCESS.2022.3174679.

WARD, R.; BEYER, B. BeyondCorp: A new approach to enterprise security. ;login: USENIX Magazine, v. 39, n. 6, p. 6-11, 2014.