GOVERNANÇA DE RISCOS SOCIOTÉCNICOS EM INSTITUIÇÕES DE INTELIGÊNCIA: ARQUITETURA ZERO TRUST COMO ESTRATÉGIA ORGANIZACIONAL CONTRA AMEAÇAS INTERNAS

Socio-technical Risk Governance in Intelligence Agencies: Zero Trust Architecture as an Organizational Strategy Against Insider Threats

EMERSON EIKITI MATSUKAWA
UNINOVE – UNIVERSIDADE NOVE DE JULHO

GISLAINE DA MOTTA BASTOS MATSUKAWA
ESCOLA SUPERIOR DE PROPAGANDA E MARKETING - ESPM

THIAGO YOKOYAMA MATSUMOTO
UNINOVE – UNIVERSIDADE NOVE DE JULHO

ALEXANDRE RODRIGUES PINTO
UNINOVE – UNIVERSIDADE NOVE DE JULHO

Comunicação:
O XIV SINGEP foi realizado em conjunto com a 14th Conferência Internacional do CIK (CYRUS Institute of Knowledge) e com a SPARK (Society for Promoting Academic Research and Knowledge), em formato híbrido, com sede presencial na UNINOVE - Universidade Nove de Julho, no Brasil.

Agradecimento à orgão de fomento:
Agradecimentos ao Fundo de Apoio à Pesquisa - FAP UNINOVE e à CAPES.

GOVERNANÇA DE RISCOS SOCIOTÉCNICOS EM INSTITUIÇÕES DE INTELIGÊNCIA: ARQUITETURA ZERO TRUST COMO ESTRATÉGIA ORGANIZACIONAL CONTRA AMEAÇAS INTERNAS

Objetivo do estudo
Analisar as contribuições da governança baseada na verificação contínua da arquitetura Zero Trust para mitigar o risco de vazamento de informações sigilosas por ameaças internas em instituições de inteligência, mapeando taxonomias comportamentais, pilares técnicos de acesso e impactos na resiliência operacional.

Relevância/originalidade
Preenche lacunas ao integrar dimensões sociotécnicas, fatores culturais e inteligência artificial à governança Zero Trust, superando limitações perimetrais tradicionais e modelos puramente técnicos para mitigar riscos de agentes internos e assegurar a soberania informacional em instituições de inteligência e infraestruturas públicas.

Metodologia/abordagem
Revisão integrativa estruturada nos cinco estágios de Whittemore e Knafl (2005). Realizou buscas sem limite temporal nas bases Scopus e Web of Science, selecionando e sintetizando quatorze artigos de alto impacto em quatro eixos temáticos fundamentais.

Principais resultados
Demonstra que a governança Zero Trust reduz vazamentos por agentes internos e restringe movimentos laterais através do privilégio mínimo e monitoramento contínuo. Prova que a resiliência institucional exige integrar defesas ativas com inteligência artificial, conformidade regulatória e cultura de segurança consolidada.

Contribuições teóricas/metodológicas
Propõe um modelo conceitual integrativo conectando arquitetura técnica, governança regulatória e fatores sociotécnicos na gestão de ameaças internas. Metodologicamente, valida a aplicação de revisões integrativas em segurança cibernética estratégica, estabelecendo diretrizes estruturadas e proposições teóricas para futuras investigações empíricas em inteligência institucional.

Contribuições sociais/para a gestão
Oferece aos gestores públicos diretrizes para implementar controle de acesso centrado no dado e superar resistências culturais. Socialmente, fortalece a salvaguarda de infraestruturas críticas e a soberania nacional, prevenindo vazamentos de segredos de Estado e protegendo a confiança da sociedade nas instituições.

Palavras-chave: Governança Sociotécnica de Riscos, Arquitetura Zero Trust (ZTA), Instituições de Inteligência, Ameaças Internas, Revisão Integrativa

Socio-technical Risk Governance in Intelligence Agencies: Zero Trust Architecture as an Organizational Strategy Against Insider Threats

Study purpose
Analyze the strategic contributions of continuous verification governance within Zero Trust Architecture to mitigate the risk of classified information leaks from insider threats across intelligence institutions, mapping behavioral taxonomies, technical access control mechanisms, and organizational impacts on mission resilience and critical operations.

Relevance / originality
Fills critical knowledge gaps by integrating sociotechnical, cultural, and artificial intelligence dimensions into Zero Trust governance, transcending traditional perimeter defenses and purely technical models to systematically mitigate insider threat risks and safeguard national information sovereignty within intelligence agencies and state infrastructures.

Methodology / approach
Integrative review methodology structured around the five stages of Whittemore and Knafl (2005). Conducted comprehensive searches in Scopus and Web of Science databases without temporal limits, systematically selecting and synthesizing fourteen high-impact studies across four core analytical thematic axes.

Main results
It demonstrates that Zero Trust governance reduces insider-driven data leaks and restricts lateral movement through the principle of least privilege and continuous monitoring. It proves that institutional resilience requires integrating active defenses with artificial intelligence, regulatory compliance, and a robust security culture.

Theoretical / methodological contributions
Proposes an integrative conceptual framework linking technical architecture, regulatory governance, and sociotechnical factors in insider threat mitigation. Methodologically, it validates integrative review approaches within strategic cybersecurity research, providing structured actionable guidelines and theoretical propositions for future empirical investigations across national intelligence institutions.

Social / management contributions
It offers public sector managers guidelines for implementing data-centric access control and overcoming cultural resistance. From a societal perspective, it strengthens the safeguarding of critical infrastructure and national sovereignty, preventing the leakage of state secrets and protecting public trust in institutions.

Keywords: Sociotechnical Risk Governance, Zero Trust Architecture (ZTA), Intelligence Agencies, Insider Threats, Integrative Review