SEGURANÇA DA INFORMAÇÃO NA ERA DIGITAL: PILARES, NORMAS E DESAFIOS CONTEMPORÂNEOS

Eduardo de Lima Toledo[1], Fabiano De Oliveira Wonzoski[2]

1. Discente do curso de graduação em Ciência da Computação, Unoesc, Videira, SC
2. Docente do curso de graduação em Ciência da Computação, Unoesc, Videira, SC

Autor correspondente: Eduardo de Lima Toledo, eduardolimatoledo@icloud.com

Área: Ciências Exatas e Tecnológicas

Introdução: A transformação digital intensificou a interconectividade entre sistemas, usuários e fornecedores, elevando a criticidade da proteção de ativos informacionais e exigindo abordagens integradas que articulem os pilares Confidencialidade, Integridade e Disponibilidade com normas de governança e marcos regulatórios para assegurar resiliência, continuidade operacional e confiança institucional no ambiente digital contemporâneo. **Objetivo:** Analisar, por meio de revisão sistemática da literatura e análise documental, como os pilares da segurança da informação, frameworks de gestão e legislações de proteção de dados estruturam práticas eficazes de prevenção, detecção e resposta a incidentes. **Método:** Pesquisa qualitativa-exploratória baseada em revisão sistemática de literatura e análise documental, com busca nas bases IEEE Xplore, Scopus, ScienceDirect e Google Scholar, recorte temporal nos últimos dez anos até agosto de 2025 e descritores incluindo segurança da informação, confidencialidade, integridade, disponibilidade, ISO/IEC 27001, NIST, LGPD, GDPR, computação em nuvem e inteligência artificial; a triagem seguiu etapas de identificação, seleção por títulos e resumos, leitura integral e extração padronizada de dados; critérios de inclusão contemplaram estudos revisados por pares e relatórios técnicos com metodologia explícita, sendo excluídos comentários de opinião e trabalhos sem descrição metodológica; do total de 1.042 registros identificados, 64 atenderam aos critérios de inclusão e foram analisados em profundidade. **Resultados:** Os achados indicam que a adoção articulada dos pilares CID em conjunto com estruturas normativas e frameworks operacionais reduz a ocorrência de incidentes e melhora a capacidade de recuperação organizacional; evidências empíricas associam certificação ou adoção de controles formais à menor frequência de falhas sistêmicas, enquanto revisões destacam desafios emergentes relacionados à migração para nuvem, ao uso de inteligência artificial e às lacunas na capacitação humana e na governança; observou-se, ademais, que a conformidade legal contribui para a confiança de stakeholders e para a coordenação de respostas a incidentes. **Conclusão:** Conclui-se que a efetividade da segurança da informação depende da integração entre fundamentos técnicos, governança normativa e desenvolvimento cultural organizacional; recomenda-se priorizar políticas de capacitação contínua, adoção pragmática de frameworks como ISO/IEC 27001 e NIST, e direcionar pesquisas futuras à aplicação de inteligência artificial para detecção precoce de ameaças, automação de controles e práticas DevSecOps.

Palavras-chave: Segurança Computacional; Privacidade; Computação em Nuvem; Inteligência Artificial.