VIII ENCONTRO INTERNACIONAL DE GESTÃO, DESENVOLVIMENTO E INOVAÇÃO
NOVOS CONTEXTOS PARA O AGRONEGÓCIO
ISSN: 2594-8083
VIII EIGEDIN
25 a 27 de Maio de 2026
Totalmente Online e Gratuito

( ) Graduação (X) Pós-Graduação
( ) Artigo completo ( ) Relato de prática (X) Resumo expandido

CIBERSEGURANÇA COMO FATOR ESTRATÉGICO NA TRANSFORMAÇÃO DIGITAL: O PAPEL DA CULTURA ORGANIZACIONAL

Orlando Oliveira Rodrigues
Universidade Tecnológica Federal do Paraná
orlandorodrigues@alunos.utfpr.edu.br

Kauterine de Lima Dallanol
Universidade Tecnológica Federal do Paraná
kauterinedallanol@alunos.utfpr.edu.br

Juliana Sampaio Do Carmo
Universidade Tecnológica Federal do Paraná
julianadocarmoeng@hotmail.com

Flavio Trojan
Universidade Tecnológica Federal do Paraná
trojan@utfpr.edu.br

Sérgio Luiz Ribas Pessa
Universidade Tecnológica Federal do Paraná
slpessa@utfpr.edu.br

Sérgio Eduardo Gouvêa da Costa
Universidade Tecnológica Federal do Paraná
gouvea@utfpr.edu.br

RESUMO

A Transformação Digital intensifica a dependência de tecnologias e amplia a exposição a riscos cibernéticos, exigindo que a cibersegurança seja tratada como um fator estratégico. Nesse contexto, este artigo tem como objetivo analisar como a cibersegurança se consolida como um fator estratégico no processo de Transformação Digital das organizações, considerando a influência da cultura organizacional. Metodologicamente, foi realizada uma Revisão Sistemática da Literatura, com base no método PRISMA, a partir de estudos indexados nas bases *Scopus* e *Web of Science* no período de 2019 a 2025. Os resultados evidenciam que a efetividade das práticas de cibersegurança está fortemente associada a fatores culturais, como valores organizacionais, comprometimento da liderança e responsabilidade compartilhada, que influenciam diretamente a adoção de comportamentos seguros. Observa-se que organizações que incorporam a segurança da informação como valor institucional apresentam maior aderência às políticas e maior consistência nas práticas de proteção. Conclui-se que a consolidação da cibersegurança como fator estratégico depende da integração entre tecnologia, processos e, sobretudo, cultura organizacional.

Palavras-chave: Cibersegurança; Transformação Digital; Cultura Organizacional.

ISSN: 2594-8083

1 INTRODUÇÃO

A Transformação Digital tem se consolidado como um imperativo estratégico para as organizações contemporâneas, caracterizada pela integração de tecnologias digitais aos processos organizacionais e pela intensificação do uso de dados em ambientes interconectados (Li et al., 2023; Chotia et al., 2025). Nesse cenário, embora a digitalização amplie eficiência e inovação, também aumenta os riscos cibernéticos, tornando a cibersegurança um elemento estratégico para a continuidade dos negócios (Jonathan et al., 2024; Chotia et al., 2025).

Apesar dos avanços tecnológicos, a efetividade das práticas de cibersegurança não depende exclusivamente de soluções técnicas, estando fortemente condicionada a fatores organizacionais e humanos (Harper, 2023; Maulidar et al., 2025). Nesse sentido, Harper (2023) ressalta que o fator humano constitui um dos principais pontos de vulnerabilidade, enquanto Alshaikh (2020) destaca que a cultura organizacional exerce influência direta sobre a adoção de comportamentos seguros. Dessa forma, organizações que promovem valores orientados à segurança da informação e à responsabilidade compartilhada tendem a apresentar maior adesão a comportamentos seguros, enquanto ambientes em que a segurança é restrita à área técnica apresentam maiores vulnerabilidades (Mikuletič et al., 2024).

Diante desse contexto, este artigo tem como objetivo analisar como a cibersegurança se consolida como um fator estratégico no processo de Transformação Digital das organizações, considerando a influência da cultura organizacional. Para isso, foi realizada uma Revisão Sistemática da Literatura, com base no método PRISMA, utilizando estudos indexados nas bases *Scopus* e *Web of Science* no período de 2019 a 2025, visando compreender o papel dos fatores culturais na adoção de práticas de cibersegurança.

2 DISCUSSÃO E ANÁLISE DOS DADOS

A análise dos estudos selecionados evidencia que a cibersegurança, no contexto da Transformação Digital, transcende a dimensão técnica, sendo influenciada por fatores organizacionais e estratégicos. De forma recorrente, os estudos apontam que a cibersegurança atua como elemento mediador da resiliência organizacional, da continuidade dos negócios e da sustentabilidade das iniciativas digitais (Li et al., 2023; Arafah et al., 2025). Esses achados indicam que organizações com maior alinhamento entre estratégias digitais e práticas de segurança apresentam maior capacidade de resposta a riscos cibernéticos.

No que se refere às abordagens analíticas identificadas, os resultados demonstram a predominância de três linhas principais: a perspectiva estratégica, a cultura de segurança da

ISSN: 2594-8083

informação e o fator humano. A dimensão cultural se destaca como elemento estruturante, na medida em que valores organizacionais, normas compartilhadas e o comprometimento da liderança influenciam diretamente a institucionalização das práticas de cibersegurança (Alshaikh, 2020; Tejay; Mohammed, 2023). Complementarmente, Estudos voltados à governança reforçam que a efetividade das estratégias depende da integração entre diretrizes organizacionais e mecanismos de controle (Haleem et al., 2022).

Os resultados também evidenciam o papel central do fator humano, uma vez que comportamentos individuais, percepção de risco e níveis de conscientização influenciam diretamente a adesão às políticas de segurança (Harper, 2023; Mikuletič et al., 2024; Maulidar et al., 2025). Nesse sentido, estratégias como treinamentos contínuos e programas de conscientização emergem como mecanismos fundamentais para alinhar comportamento individual e diretrizes institucionais (Armas; Taherdoost, 2025). Além disso, a literatura aponta que a promoção de uma cultura baseada na responsabilidade compartilhada contribui para a redução de vulnerabilidades associadas a falhas humanas.

Em síntese, os estudos indicam que a consolidação da cibersegurança como fator estratégico está associada a um processo evolutivo, no qual organizações avançam de abordagens reativas para práticas proativas e culturalmente internalizadas. Esse processo depende da articulação entre cultura organizacional, governança e comportamento individual, sustentado por estratégias de integração da segurança à governança e fortalecimento da liderança (Chotia et al., 2025; Arafah et al., 2025). Porém, persistem limitações na mensuração de fatores culturais e comportamentais, indicando a necessidade de abordagens mais integradas.

3 CONCLUSÕES

Com base neste estudo, a cibersegurança se consolida como um fator estratégico no contexto da Transformação Digital ao ultrapassar a dimensão técnica e depender da integração entre tecnologia, processos e cultura organizacional. A análise da literatura evidenciou que a efetividade das práticas de segurança está fortemente condicionada a fatores culturais, como valores compartilhados, comprometimento da liderança e responsabilidade coletiva, que influenciam diretamente a adoção de comportamentos seguros. Somado a isso, a cibersegurança deve ser compreendida como um processo evolutivo, no qual as organizações avançam de abordagens reativas para posturas proativas e alinhadas à estratégia. Contudo, persistem limitações na mensuração de aspectos culturais e comportamentais, evidenciando a necessidade de abordagens mais integradas. Nesse sentido, a consolidação da cibersegurança como

elemento estratégico depende do alinhamento entre dimensões técnicas e humanas, sendo a cultura organizacional um fator determinante para a sustentabilidade da Transformação Digital.

AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de financiamento 001.

REFERÊNCIAS

ALSHAIKH, Mohammed. Developing cybersecurity culture to influence employees' compliance behavior. **Computers & Security**, v. 98, art. 102003, 2020. DOI: 10.1016/j.cose.2020.102003.

ARAFah, Ayman et al. Cybersecurity challenges in digital transformation: a strategic perspective. **Information & Computer Security**, v. 33, n. 1, p. 1–17, 2025. DOI: 10.1108/ICS-08-2024-0132.

CHOTIA, Varun; KHOUALDI, Kamel; BROCCARDO, Laura; YAQUB, Muhammad Zafar. The role of cyber security and digital transformation in gaining competitive advantage through Strategic Management Accounting. **Technology in Society**, [s. l.], v. 81, art. 102851, 2025. DOI: 10.1016/j.techsoc.2025.102851.

HARPER, Jimmy W. Cybersecurity: a review of human-based behavior and best practices to mitigate risk. **Issues in Information Systems**, v. 24, n. 3, p. 119–128, 2023. DOI: 10.48009/4_iis_2023_119.

HALEEM, Abid et al. Perspectives of cybersecurity for ameliorative Industry 4.0 era: a review-based framework. **Industrial Management & Data Systems**, v. 122, n. 6, p. 1110–1136, 2022. DOI: 10.1108/IMDS-10-2021-0627.

JONATHAN, Samuel et al. Cybersecurity as a strategic enabler of digital transformation. **Journal of Strategic Information Systems**, v. 33, n. 1, art. 101783, 2024. DOI: 10.1016/j.jsis.2023.101783.

LI, Fang et al. Digital transformation, data governance and cybersecurity. **Information Systems Frontiers**, v. 25, n. 2, p. 473–488, 2023. DOI: 10.1007/s10796-022-10258-4.

MAULIDAR, Rahma et al. Human error and cybersecurity incidents: organizational implications. **Computers & Security**, v. 138, art. 103660, 2025. DOI: 10.1016/j.cose.2024.103660.

MIKULETIČ, Samanta et al. IT professionals' understanding of the implications of LGPD on information security. **Revista de Gestão Organizacional**, v. 18, n. 2, p. 1–19, 2024. DOI: 10.22277/rgo.v18i2.8355.