SemeAd 2025
XXVIII Seminários em Administração

10, 11, 12, 13 e 14 de novembro de 2025
ISSN 2177-3866

DESIGNING AGAINST SYSTEMIC EXCLUSION: A FRAMEWORK FOR EMANCIPATORY INFORMATION SECURITY SYSTEMS

ANGELICA PIGOLA
UNIVERSIDADE ESTADUAL DE CAMPINAS (UNICAMP)

Agradecimento à orgão de fomento:
This research was funded by Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), Brazil, grant number 88887.946533/2024-00

10, 11, 12, 13 e 14 de novembro de 2025
ISSN 2177-3866

Introdução
Information security has become a foundational infrastructure mediating access to education, mobility, healthcare, and democratic participation. However, conventional security approaches often prioritize institutional control and efficiency, marginalizing vulnerable users. This paper calls for a reorientation of information security as a space not only for protection but also for social justice and user empowerment.

Problema de Pesquisa e Objetivo
Security mechanisms frequently reinforce exclusion, surveillance, and epistemic inequality, limiting autonomy and deepening digital divides. This study proposes the Emancipatory Information Security Framework as a theoretical and design-based response, offering new pathways for building digital systems that support equity, participation, and agency, especially for those historically excluded from technological governance.

Fundamentação Teórica
The framework draws on structuration theory, critical theory, and design science. Structuration theory reveals how security infrastructures are shaped by and shape social practices; critical theory uncovers the ideological dimensions of InfoSec; and design science offers practical tools for constructing alternative, justice-oriented systems. This interdisciplinary integration enables both diagnosis and transformation

Discussão
The Emancipatory Information Security Framework is composed of seven key mechanisms: agency, voice, inclusion, rationality, reflexivity, reparative justice, and plurality. Each mechanism is operationalized through design principles and InfoSec actions, such as inclusive authentication, pseudonymity, multilingual encryption, transparent auditing, and participatory governance. These components aim to resist domination and reconfigure power relations embedded in digital infrastructures.

Conclusão
Repositioning InfoSec as an emancipatory infrastructure requires a shift from threat mitigation to enabling collective agency. Rather than protecting systems from users, security should be designed with and for users, particularly those affected by systemic inequities. EISF supports ethical, inclusive, and transparent digital practices that promote meaningful participation and self-determination.

Contribuição / Impacto
This framework contributes to critical IS and InfoSec scholarship by offering a values-based model that integrates justice, user agency, and plural epistemologies into the core of digital system design. It also provides a practical foundation for developers and policymakers seeking to build secure systems that are democratic, accountable, and aligned with human rights.

Referências Bibliográficas
Tingelhoff, F., & Marga, J. J. (2025). Avoiding virtual dystopia: A design theory for emancipatory participatory immersive platforms. The Journal of Strategic Information Systems, 34(4), 101910. https://doi.org/10.1016/j.jsis.2025.101910
Young, A. G., Shuva, S., Roth, T., Zhu, Y., & Hevner, A. R. (2025). Ethical design through grounding and evaluation: The EDGE method for designing information systems for social impact. Journal of Information Technology, 40(2), 164–179. https://doi.org/10.1177/02683962241289598