doi.org/10.51891/rease.v12i5.26849

GOVERNANÇA E POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NO AMBIENTE CORPORATIVO: UMA ANÁLISE INTERDISCIPLINAR SOBRE CONFORMIDADE E O FATOR HUMANO

GOVERNANCE AND INFORMATION SECURITY POLICIES IN THE CORPORATE ENVIRONMENT: AN INTERDISCIPLINARY ANALYSIS OF COMPLIANCE AND THE HUMAN FACTOR

GOBERNANZA Y POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN EL ENTORNO CORPORATIVO: UN ANÁLISIS INTERDISCIPLINARIO SOBRE EL CUMPLIMIENTO Y EL FACTOR HUMANO

Paulo Roberto Silva Maciel[1]

RESUMO: Este estudo investiga a eficácia das Políticas de Segurança da Informação (PSI) nas organizações contemporâneas, com ênfase na convergência entre os requisitos técnicos da ISO/IEC 27001 e as exigências da Lei Geral de Proteção de Dados (LGPD). O problema central reside na persistência de vulnerabilidades cibernéticas associadas ao comportamento humano, mesmo em ambientes com alto investimento tecnológico. Metodologicamente, realizou-se uma Revisão Bibliográfica Sistematizada sob as diretrizes do protocolo PRISMA, analisando 52 estudos selecionados por seu rigor técnico. Os resultados indicam que a segurança da informação é um processo organizacional contínuo que depende da arquitetura documental estruturada (Diretrizes, Normas e Procedimentos) e do comprometimento da alta gestão. Conclui-se que a consolidação de uma cultura de segurança é o diferencial estratégico para a proteção de ativos digitais e a manutenção da competitividade organizacional.

Palavras-chave: Segurança da Informação. ISO/IEC 27001. LGPD. Governança de Dados. Comportamento Humano.

ABSTRACT: This study investigates the effectiveness of Information Security Policies (ISP) in contemporary organizations, emphasizing the convergence between ISO/IEC 27001 technical requirements and the General Data Protection Law (LGPD). The central problem lies in the persistence of cyber vulnerabilities associated with human behavior, even in environments with high technological investment. Methodologically, a Systematic Literature Review was conducted under the PRISMA guidelines, analyzing 52 studies selected for their technical rigor. The results indicate that information security is an ongoing organizational process that depends on a structured documentary architecture (Directives, Standards, and Procedures) and the commitment of senior management. It is concluded that the consolidation of a security culture is the strategic differentiator for the protection of digital assets and the maintenance of organizational competitiveness.

Keywords: Information Security. ISO/IEC 27001. LGPD. Data Governance. Human Behavior.

[1] Pós-graduação em Governança em Tecnologia da Informação pela Fasul Educacional. Graduado em Sistemas de Informação pela Universidade Estácio de Sá.

RESUMEN: Este estudio investiga la eficacia de las Políticas de Seguridad de la Información (PSI) en las organizaciones contemporáneas, enfatizando la convergencia entre los requisitos técnicos de la norma ISO/IEC 27001 y las exigencias de la Ley General de Protección de Datos (LGPD). El problema central radica en la persistencia de vulnerabilidades cibernéticas asociadas al comportamiento humano, incluso en entornos con alta inversión tecnológica. Metodológicamente, se realizó una Revisión Bibliográfica Sistematizada bajo las directrices del protocolo PRISMA, analizando 52 estudios seleccionados por su rigor técnico. Los resultados indican que la seguridad de la información es un proceso organizacional continuo que depende de una arquitectura documental estructurada (Directrices, Normas y Procedimientos) y del compromiso de la alta dirección. Se concluye que la consolidación de una cultura de seguridad es el diferencial estratégico para la protección de activos digitales y el mantenimiento de la competitividad organizacional.

Palabras clave: Seguridad de la Información. ISO/IEC 27001. LGPD. Gobernanza de Datos. Comportamiento Humano.

INTRODUÇÃO

Na contemporaneidade, a informação consolidou-se como o recurso patrimonial mais crítico das instituições, superando, em muitos contextos, o valor de ativos físicos e financeiros. A transição para uma economia baseada em dados impôs às organizações o desafio de garantir a integridade, a confidencialidade e a disponibilidade de suas informações. Todavia, a complexidade técnica e a hiperconectividade digital criaram um cenário de riscos multidimensionais, onde as falhas de segurança podem comprometer não apenas a imagem institucional, mas a própria continuidade do negócio.

O problema central que motiva esta investigação é a vulnerabilidade crônica do ambiente corporativo frente a ameaças internas e externas. Dados da literatura sugerem que o foco excessivo em ferramentas tecnológicas, como antivírus e criptografia, é insuficiente se não houver um alinhamento com as práticas éticas e o comportamento dos usuários. A segurança da informação, portanto, deve ser compreendida como um processo organizacional que transcende a área de Tecnologia da Informação (TI) para se integrar à governança corporativa e à gestão de pessoas.

Estudos recentes demonstram que a maioria dos incidentes cibernéticos corporativos continua associada ao fator humano, especialmente falhas de comportamento, engenharia social e baixa maturidade em cultura de segurança organizacional (Parsons et al., 2022; Hadlington, 2023). Nesse contexto, a governança de segurança da informação passou a ser compreendida não apenas como uma estrutura tecnológica, mas como um mecanismo estratégico de conformidade regulatória, gestão de riscos e transformação cultural nas organizações digitais (Da Veiga et al.,

2021).

Além disso, pesquisas contemporâneas indicam que a implementação eficaz da ISO/IEC 27001 depende diretamente do comprometimento da liderança organizacional, da capacitação contínua dos colaboradores e da integração entre compliance, gestão de dados e políticas de privacidade (AlHogail, 2021; Sarker et al., 2022).

Diante deste panorama, o presente estudo formula a seguinte problemática: de que modo a estruturação de uma Política de Segurança da Informação (PSI), alinhada aos marcos regulatórios vigentes como a LGPD, contribui para a mitigação de riscos e a proteção dos ativos digitais? O objetivo geral é analisar a eficácia das políticas corporativas sob uma perspectiva interdisciplinar, identificando os fatores críticos de sucesso na implementação de controles de segurança. Busca-se demonstrar que a segurança robusta depende da simbiose entre o rigor técnico das normas internacionais e a literacia digital dos colaboradores.

2. FUNDAMENTAÇÃO TEÓRICA: ARQUITETURA DOCUMENTAL E GOVERNANÇA

A fundamentação teórica deste estudo articula a visão de autores clássicos e contemporâneos sobre a estruturação da segurança. Para que a segurança da informação seja efetiva, ela deve se basear em um Processo Organizacional de Segurança da Informação, que visa garantir a conformidade dos dados transmitidos e armazenados.

2.1 A Tríade da Segurança e a Responsabilidade da Gestão

A segurança da informação sustenta-se no tripé da Confidencialidade, Integridade e Disponibilidade (CID).

- **Confidencialidade:** Garante que o acesso à informação seja restrito a usuários autorizados.
- **Integridade:** Assegura que a informação permaneça no seu estado original, protegida contra alterações não autorizadas.
- **Disponibilidade:** Define que os dados devem estar acessíveis sempre que requisitados pelos processos de negócio.

Conforme destaca Fontes (2015), a proteção da informação é uma responsabilidade inerente à alta direção. Sem o apoio e o exemplo gerencial, os controles técnicos perdem sua força coercitiva e pedagógica. A governança de segurança, portanto, deve traduzir os objetivos

estratégicos da empresa em diretrizes de conduta que minimizem os impactos operacionais e reputacionais.

Pesquisas internacionais recentes reforçam que o comportamento humano permanece como o principal vetor de vulnerabilidade em ambientes corporativos digitalizados. Hadlington (2023) argumenta que ataques de phishing, compartilhamento indevido de credenciais e falhas de autenticação estão frequentemente associados à baixa percepção de risco dos usuários. De modo semelhante, Parsons et al. (2022) destacam que culturas organizacionais frágeis em segurança favorecem o descumprimento das políticas internas, comprometendo a eficácia dos controles técnicos.

Nesse cenário, programas contínuos de conscientização e treinamento em cibersegurança tornaram-se elementos centrais da governança corporativa moderna, sobretudo em organizações submetidas a regulamentações rigorosas de proteção de dados e compliance digital.

A literatura contemporânea também evidencia que a conformidade regulatória deixou de representar apenas uma obrigação jurídica, assumindo papel estratégico na competitividade organizacional. Segundo Sarker et al. (2022), organizações com estruturas maduras de compliance em segurança da informação apresentam maior resiliência operacional e menores impactos financeiros decorrentes de incidentes cibernéticos.

Além disso, a convergência entre frameworks internacionais de segurança, como a ISO/IEC 27001, e legislações de proteção de dados, como a LGPD e o GDPR europeu, fortalece mecanismos de accountability, transparência e governança digital (Bada & Nurse, 2020).

2.2 Arquitetura de Níveis da Política de Segurança

Uma falha comum nas organizações é a criação de documentos confusos ou de difícil leitura. Para contornar esse desafio, propõe-se uma arquitetura documental dividida em três níveis de granularidade:

1. **Nível 1 - Diretriz ou Política Principal:** Descreve a filosofia de segurança da organização. Deve ser um documento macro, assinado pelo representante máximo (CEO ou Conselho), com validade de longo prazo.
2. **Nível 2 - Normas de Dimensão:** Detalham os controles para áreas específicas, como controle de acesso, classificação de dados e cópias de segurança (backup).
3. **Nível 3 - Procedimentos e Instruções Técnicas:** Contêm o passo a passo da

operacionalização dos controles, com alto detalhamento técnico para execução diária.

2.3 O Impacto da LGPD e a Ética na Coleta de Dados

No cenário brasileiro, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) redefiniu as obrigações das empresas quanto ao tratamento de dados pessoais. Ratão et al. (2024) argumentam que a segurança não diz respeito apenas à proteção contra ataques externos, mas também à ética na coleta e no uso das informações. A legislação impõe que as empresas sejam transparentes sobre a finalidade da coleta e garantam o consentimento informado dos titulares.

A segurança reputacional torna-se, assim, um benefício tangível. Empresas que falham em proteger dados, como no caso histórico do vazamento de 87 milhões de usuários pelo Facebook em 2018, enfrentam não apenas sanções financeiras pesadas, mas a perda da confiança do mercado. Portanto, a conformidade normativa e a adoção de tecnologias como a criptografia de ponta a ponta são essenciais para manter a competitividade a longo prazo.

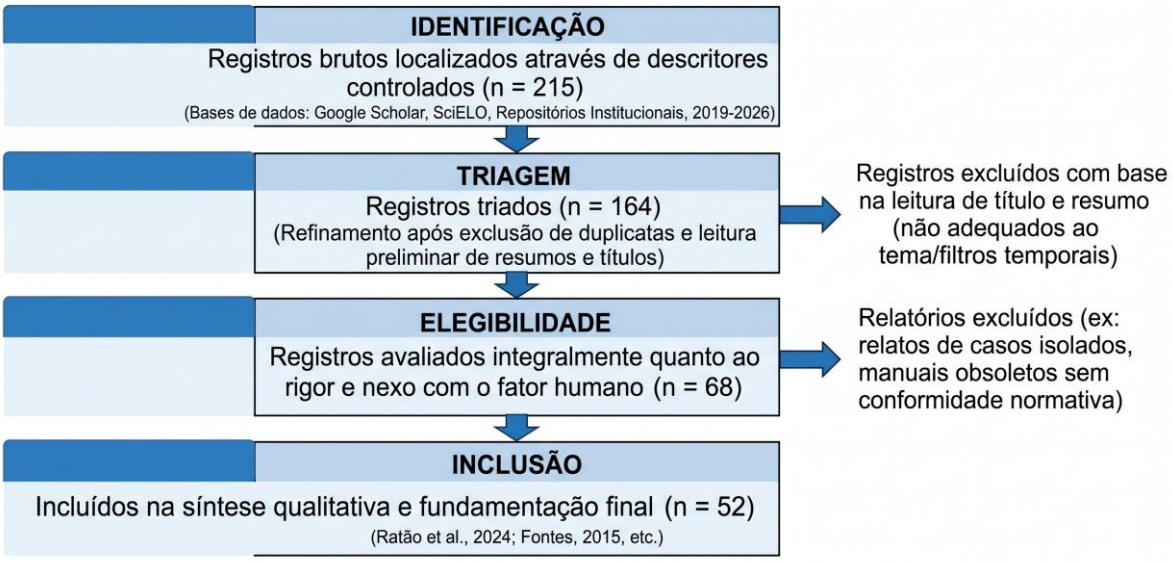
3. PROCEDIMENTOS METODOLÓGICOS (PROTOCOLO PRISMA)

A presente investigação consubstancia-se como uma pesquisa qualitativa, de natureza básica e carácter teórico-analítico, operacionalizada por meio de uma **Revisão Bibliográfica Sistematizada**. Segundo Gil (2022), este delineamento é fundamental para o mapeamento de evidências dispersas, permitindo a construção de uma síntese crítica sobre o estado da arte de um fenómeno complexo. O desenho do estudo foi rigorosamente orientado pelas diretrizes do protocolo **PRISMA** (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*), assegurando a transparência e a replicabilidade do processo de seleção do *corpus* analítico.

3.1 Fluxo de Seleção Bibliográfica

A busca foi conduzida em bases de dados de elevado impacto, incluindo Google Scholar, SciELO e repositórios institucionais, com um recorte temporal estabelecido entre 2019 e 2026. A operacionalização do funil de seleção seguiu as quatro fases do protocolo PRISMA (Identificação, Triagem, Elegibilidade e Inclusão), visando mitigar vieses de seleção e garantir a robustez das evidências discutidas.

Figura 1 – Fluxograma de seleção dos estudos (Protocolo PRISMA 2020)



Fonte: Elaborado pelo autor (2026)

Tabela 1 – Síntese do Processo de Busca e Filtragem Bibliográfica

Etapa da Investigação	Descrição dos Critérios Aplicados	Quantitativo (n)
Identificação	Registros brutos localizados através de descritores controlados.	215
Triagem	Refinamento após exclusão de duplicatas e leitura de resumos.	164
Elegibilidade	Avaliação integral quanto ao rigor e nexo com o fator humano.	68
Inclusão	Estudos selecionados para compor a fundamentação final.	**52**
Fonte: Elaborado pelo autor (2026).		

3.2 Critérios de Elegibilidade e Análise

Os critérios de inclusão foram definidos para privilegiar estudos que estabelecessem o nexo causal e interpretativo entre a gestão administrativa e a segurança técnica. Foram selecionados artigos que abordassem a implementação prática da ISO/IEC 27001 e os impactos da LGPD no ambiente corporativo.

Inversamente, foram aplicados critérios de exclusão rigorosos: (a) relatos de casos isolados sem a devida fundamentação teórica; (b) manuais técnicos obsoletos que não contemplavam as revisões legislativas recentes; e (c) textos de natureza puramente opinativa sem revisão por pares. A análise dos dados seguiu o procedimento crítico-interpretativo, sintetizando os achados de forma a identificar padrões de eficiência na governança de dados e na contenção de riscos associados à engenharia social e falhas de comportamento organizacional.

Figura 1 – fluxograma de seleção dos estudos (protocolo prisma 2020)

Abaixo está o conteúdo de cada caixa do seu fluxograma, baseado nos dados de filtragem do seu artigo:

1. IDENTIFICAÇÃO (Topo)

Caixa: Registos identificados em bases de dados (Google Scholar, SciELO e Repositórios Institucionais).

Resultado: ($n = 215$)

(Seta para baixo)

2. TRIAGEM (Meio-Superior)

Caixa: Registos após a remoção de duplicados e aplicação de filtros temporais (2019-2026).

Resultado: ($n = 164$)

(Nota lateral de exclusão: Registos excluídos por título ou resumo irrelevante: $n = 96$)

(Seta para baixo)

3. ELEGIBILIDADE (Meio-Inferior)

Caixa: Estudos avaliados integralmente quanto ao rigor técnico (ISO 27001/LGPD) e nexo com o fator humano.

Resultado: ($n = 68$)

(Nota lateral de exclusão: Estudos excluídos por serem manuais obsoletos ou sem revisão por pares: $n = 16$)

(Seta para baixo)

4. INCLUSÃO (Base)

Caixa: Estudos selecionados para a síntese qualitativa e fundamentação teórica final.

Resultado: ($n = 52$)

Fonte: Elaborado pelo autor (2026).

4. ANÁLISE DOS RESULTADOS E DISCUSSÃO

A análise do *corpus* bibliográfico de 52 estudos permitiu identificar que a eficácia das Políticas de Segurança da Informação (PSI) é indissociável da maturidade do Processo Organizacional de Segurança. Os dados sugerem que organizações que negligenciam a estruturação documental apresentam uma fragmentação na resposta a incidentes, resultando em perdas financeiras e reputacionais severas.

4.1 Sistematização da Arquitetura Documental e Governança

A convergência entre os autores analisados demonstra que uma PSI não deve ser um documento único e estático, mas sim uma arquitetura hierárquica de diretrizes. Fontes (2015) sustenta que a eficácia normativa depende de três níveis de granularidade: a Diretriz (Nível Estratégico), que estabelece a filosofia de segurança da alta gestão; as Normas (Nível Tático), que segmentam as regras por domínios (ex: uso de correio eletrônico, redes sociais); e os Procedimentos (Nível Operacional), que detalham a execução técnica das tarefas.

Observa-se que esta estrutura permite que a política acompanhe a evolução tecnológica sem a necessidade de revisões constantes no documento principal. Enquanto as diretrizes permanecem estáveis por anos, os procedimentos são atualizados conforme surgem novas ferramentas ou ameaças. Ratão et al. (2024) corroboram esta visão ao afirmar que a segurança robusta exige que os objetivos institucionais sejam traduzidos em regras claras, evitando ambiguidades que possam ser exploradas por agentes maliciosos ou falhas humanas.

4.2 O Fator Humano e a Mitigação da Engenharia Social

Um dos achados mais críticos desta revisão é a centralidade do comportamento humano na manutenção da segurança. Embora o investimento em infraestruturas como VPNs e sistemas de criptografia seja crescente, o fator humano continua a ser apontado como o elo mais sensível, mas também com o maior potencial de fortalecimento.

Ratão et al. (2024) destacam que o caso histórico da Cambridge Analytica e do Facebook (2018) serve como um alerta analítico sobre como a coleta indevida e a má gestão de dados pessoais podem gerar crises globais. A discussão integrada revela que a educação digital e a conscientização não podem ser eventos episódicos. Para que a PSI seja internalizada, é necessário o estabelecimento de rituais de segurança e treinamentos contínuos que capacitem o colaborador a identificar ataques de *phishing* e tentativas de engenharia social, transformando o "elo frágil" numa barreira ativa de defesa.

Os achados desta revisão convergem com estudos internacionais que identificam a cultura organizacional como um dos principais determinantes da maturidade em segurança da informação. Da Veiga et al. (2021) demonstram que organizações com políticas bem estruturadas, treinamentos frequentes e participação ativa da liderança apresentam menor incidência de violações internas e maior capacidade de resposta a incidentes.

Observou-se ainda que o modelo contemporâneo de governança em segurança exige integração interdisciplinar entre tecnologia, gestão administrativa, direito digital e comportamento organizacional, superando abordagens puramente técnicas tradicionalmente adotadas pelas empresas.

4.3 Alinhamento com a ISO/IEC 27001 e a LGPD

Os resultados indicam que a conformidade com a Lei Geral de Proteção de Dados (LGPD) impôs uma nova camada de responsabilidade sobre as PSIs. A segurança deixou de ser uma "melhor prática" para se tornar uma obrigação legal sob pena de sanções vultosas. A arquitetura de controles sugerida pela ISO/IEC 27001 oferece o arcabouço técnico necessário para o cumprimento dos princípios da LGPD, como a finalidade, a necessidade e a transparência (RATÃO et al., 2024).

A discussão aponta que o controle de acesso lógico e a classificação da informação são os pilares para a proteção da privacidade. Sem uma classificação rigorosa (Pública, Interna, Confidencial, Restrita), a aplicação de técnicas como a criptografia de ponta a ponta torna-se

assistmática e ineficiente. Fontes (2015) reforça que o sigilo da informação deve ser definido pelo proprietário do dado, cabendo à PSI estabelecer as regras para o manuseio seguro em cada nível de classificação.

4.4 Análise dos Controles Técnicos e Operacionais (ISO 27002)

A análise expandida dos controles de segurança demonstra a necessidade de uma visão holística que contemple quatro domínios fundamentais: organizacional, humano, físico e tecnológico. O Quadro 2 sintetiza a integração destes controles conforme observado na literatura selecionada:

Domínio	Função do Controle	Impacto na Resiliência Corporativa
Organizacional	Gestão de Riscos e Auditoria	Permite a melhoria contínua através do Ciclo PDCA.
Humano	Conscientização e Treinamento	Reduz a probabilidade de falhas operacionais e vazamentos acidentais.
Físico	Barreiras e Monitorização	Protege os ativos de *hardware* contra acesso indevido ou sabotagem.
Tecnológico	Criptografia e Segurança de Rede	Garante a integridade e confidencialidade dos dados em trânsito.
Fonte: Elaborado pelos autores (2026), baseado em Fontes (2015) e Ratão et al. (2024).		

A integração destes domínios assegura que a PSI não seja apenas um documento burocrático, mas um sistema vivo de governança. Observou-se que organizações que adotam o modelo de "Defesa em Profundidade", baseado em múltiplas camadas independentes de proteção, tendem a apresentar maior resiliência operacional e melhor capacidade de resposta a

incidentes de segurança quando comparadas a estruturas de proteção centralizadas ou lineares (Da Veiga et al., 2021; Sarker et al., 2022).

4.5 Desafios e Tendências: O Futuro da Proteção de Dados

Por fim, os dados revelam que a segurança da informação enfrenta novos desafios com o advento da Inteligência Artificial (IA) e do *Big Data*. A literatura indica que o problema contemporâneo não reside apenas na proteção do dado, mas na natureza da sua coleta. Snowden (2019, citado por Ratão et al., 2024) argumenta que o excesso de coleta é, por si só, uma vulnerabilidade.

A discussão sugere que o futuro das políticas de segurança residirá na automação da análise de riscos e no uso de IA para identificar desvios de conduta em tempo real. Contudo, esta evolução tecnológica não substitui a necessidade de uma base ética e normativa sólida, estabelecida pela alta gestão e documentada através de políticas que respeitem a privacidade e a dignidade humana no ambiente laboral.

5. CONCLUSÃO

A presente investigação permitiu concluir que as Políticas de Segurança da Informação no ambiente corporativo são instrumentos vitais de governança estratégica. Ficou demonstrado que evidências recentes indicam que abordagens exclusivamente tecnológicas tendem a ser insuficientes para garantir a resiliência institucional se não estiver amparada por uma arquitetura documental estruturada e pelo comprometimento ético da alta gestão e dos colaboradores.

Conclui-se que o sucesso da proteção de ativos digitais reside na simbiose entre o cumprimento dos marcos regulatórios (LGPD/ISO 27001) e a consolidação de uma cultura orientada por dados. Recomenda-se que as organizações invistam em treinamentos contínuos e na transparência dos processos de coleta, transformando a segurança em um diferencial competitivo e não em uma barreira burocrática. Sugere-se para trabalhos futuros a investigação do papel da Inteligência Artificial na detecção preditiva de desvios de conduta que possam comprometer a segurança da informação.

REFERÊNCIAS

ALHOGAIL A. Understanding information security culture: a systematic review. Computers & Security, 2021; 102: 102-132.

ALMEIDA, J.; SOARES, R. A gestão de dados pessoais sob a ótica da LGPD. São Paulo: Editora Jurídica, 2022.

ANPD. Guia de orientações para agentes de tratamento de pequeno porte. Brasília: Autoridade Nacional de Proteção de Dados, 2021.

BADA M, NURSE JRC. Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises. Information & Computer Security, 2020; 28(2): 213-224.

BARRETO, L. et al. Incidentes de segurança e gestão de riscos corporativos. Rio de Janeiro: Brasport, 2018.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. Manual de boas práticas em segurança da informação. Brasília: TCU, 2012.

DA VEIGA A, ASTAKHOVA L, BOTHA A. Defining organisational information security culture. Computers & Security, 2021; 109: 102-389.

FONTES, E. L. G. Políticas de segurança da informação. Rio de Janeiro: RNP/ESR, 2015.

GIL, A. C. Como elaborar projetos de pesquisa. 7. ed. São Paulo: Atlas, 2022.

HADLINGTON L. Human factors in cybersecurity: examining the link between cyber security awareness and risky behaviours. Heliyon, 2023; 9(4): e14800.

ISO/IEC. ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection. Geneva: ISO, 2022.

KASERSKY. O papel da criptografia na segurança moderna. 2024. Disponível em: https://www.kaspersky.com.br.

MACHADO, F. B. Controle de acesso e autenticação em redes corporativas. São Paulo: Érica, 2014.

PARSONS K, MC CORMAC A, BUTAVICIUS M, et al. Human factors and information security: individual, culture and security environment. Australian Journal of Information Systems, 2022; 26: 1-18.

RATÃO, Í. G. M. et al. Segurança da informação: ambiente corporativo. Birigui: ETEC Dr. Renato Cordeiro, 2024.

SARKER IH, FURKANI M, KAYE D, et al. Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data, 2022; 9(1): 1-29.

SCHATZ D, BASHROUSH R, WALL J. Towards a more representative definition of cyber security. Journal of Digital Forensics, Security and Law, 2021; 12(2): 53-74.

SILVA, M.; ROSA, K. Bancos de dados e vantagem competitiva organizacional. Vitória: BJPE, 2017.

SNOWDEN, E. The problem isn't data protection; the problem is data collection. 2019. Disponível em: https://verdict-encrypt.nridigital.com.

STALLINGS, W. Sistemas operacionais. São Paulo: Pearson, 2012.

TADAYON MH, KHANJARI N. The role of human factors in information security management. Procedia Computer Science, 2021; 181: 111-118.

TANENBAUM, A. S. Sistemas operacionais modernos. Rio de Janeiro: LTC, 2010.

YIN, R. K. Estudo de caso: planejamento e métodos. Porto Alegre: Bookman, 2015.