Privacidade em Risco na Assistência Estudantil: Uma Análise Multidimensional sob a Lei Geral de Proteção de Dados (LGPD)

Fabiana Ferreira Cardoso
Universidade Federal de Pernambuco – UFPE
https://orcid.org/0009-0003-3700-1912

Eloisa Gonçalves da Silva Torlig
Universidade de Brasília – UnB
https://orcid.org/0000-0003-2519-9805

Virginia de Melo Dantas Trinks
Universidade de Brasília – UnB
https://orcid.org/0000-0003-0123-3458

Rafael Rabelo Nunes
Universidade de Brasília – UnB
https://orcid.org/0009-0001-9446-9306

Resumo

Objetivo: Analisar de forma multidimensional os riscos de privacidade associados ao tratamento de dados pessoais nos processos de assistência estudantil em uma Instituição Federal de Ensino (IFE).

Metodologia: Pesquisa aplicada de abordagem qualitativa e exploratória, com triangulação de dados por meio de entrevistas semiestruturadas, análise documental e grupo focal. A análise de conteúdo foi realizada com a técnica *Bow-Tie* como núcleo analítico para modelagem causal.

Originalidade/Relevância: O estudo preenche uma lacuna na literatura sobre a implementação da LGPD em IFEs, ao aplicar a técnica *Bow-Tie* para análise causal e multidimensional de riscos de privacidade, integrando dimensões técnica, organizacional, jurídica e humana.

Principais resultados: Os riscos mostraram-se sistêmicos e multidimensionais. A aplicação da técnica *Bow-Tie* identificou 15 riscos primários e 25 cadeias causais, evidenciando a dimensão técnico-operacional como amplificador sistêmico do risco. As 28 consequências identificadas atuam em múltiplos níveis. Para os titulares, verificam-se danos psicossociais e riscos de discriminação e estigmatização. Para a instituição, há exposição a sanções administrativas e danos reputacionais. Os 22 controles propostos visam a uma governança orientada a risco.

Contribuições: Os resultados validam a técnica *Bow-Tie* como instrumento analítico para examinar as inter-relações técnicas e sociais que afetam a privacidade, ao propor uma matriz de controles integrados e alinhada ao Programa de Privacidade e Segurança da Informação (PPSI). Conclui-se que a mitigação eficaz dos riscos exige uma governança coordenada nas quatro dimensões, reafirmando a privacidade como base da confiança no ambiente educacional digital.

Palavras-chave: governança de privacidade, proteção de dados, conformidade regulatória

Abstract

Objective: To conduct a multidimensional analysis of the privacy risks associated with the processing of personal data in student assistance processes at a Federal Educational Institution.

Methodology: Applied research with a qualitative and exploratory approach, using data triangulation through semi-structured interviews, document analysis, and focus groups. Content analysis was performed using the Bow-Tie technique as the analytical core for causal modeling.

Originality/Relevance: The study addresses a gap in the literature on the implementation of the LGPD in Federal Educational Institutions (IFE) by applying the Bow-Tie technique for causal and multidimensional privacy risk analysis, integrating technical, organizational, legal, and human dimensions.

Main Results: The risks proved to be systemic and multidimensional. The application of the Bow-Tie technique identified 15 primary risks and 25 causal chains, highlighting the technical-operational dimension as a systemic risk amplifier. The 28 consequences operate on multiple levels: psychosocial harm and risks of discrimination and stigmatization for the data subjects; exposure to administrative sanctions and reputational damage for the institution. The 22 proposed controls aim to establish risk-oriented governance.

Contributions: The results validate the Bow-Tie technique as an analytical tool for examining the technical and social interrelationships that affect privacy, by proposing an integrated control matrix aligned with the Information Security and Privacy Program (PPSI). It is concluded that effective risk mitigation requires coordinated governance across the four dimensions, reaffirming privacy as the foundation of trust in the digital educational environment.

Keywords: privacy governance, data protection, regulatory compliance

1. Introdução

A transformação digital intensificou o tratamento de dados pessoais sensíveis no ecossistema educacional, ampliando de forma expressiva os riscos de exposição a incidentes de privacidade (OECD, 2026). No Brasil, a LGPD estabeleceu um marco regulatório abrangente. Contudo, segundo Dantas e Dodt (2025), sua implementação efetiva no setor público educacional enfrenta obstáculos substanciais. Esses desafios são particularmente evidentes na avaliação proativa de riscos em instituições de ensino, que deve considerar as particularidades do contexto pedagógico e a proteção reforçada de crianças e adolescentes (Souza et al., 2025; UNESCO, 2022).

Essas dificuldades tornam-se especialmente evidentes durante a avaliação proativa de riscos à privacidade. Tal avaliação exige uma abordagem que considere, de forma integrada, as especificidades do contexto pedagógico e a proteção reforçada destinada a crianças e adolescentes, grupos com salvaguardas legais especiais (Souza et al., 2025; UNESCO, 2022). Contudo, a persistência dessa lacuna analítica, conforme alerta Nascimento et al. (2025), mantém em estado de vulnerabilidade justamente os dados mais sensíveis e os titulares que a lei busca proteger com maior rigor.

Embora a literatura sobre riscos de privacidade e segurança da informação tenha avançado, persiste uma insuficiência analítica crítica, especialmente no que se refere à compreensão integrada das causas organizacionais, técnicas e humanas que levam às violações de privacidade no contexto educacional. Estudos recentes têm focado em riscos cibernéticos e de continuidade de negócio ou em aspectos jurídicos isolados da LGPD (Tomaz, Nunes & Silva, 2025; Gonçalves et al., 2025).

Apesar dos avanços na literatura, permanecem escassas análises empíricas integradas dos riscos à privacidade em Instituições Federais de Ensino (IFEs), o que revela a limitação de métodos capazes de articular, simultaneamente, suas dimensões técnica, organizacional, jurídica e humana. Para superar essa limitação metodológica e operacionalizar os princípios da privacidade desde a concepção (*privacy by design)* e prestação de contas (*accountability)*, este estudo adota a técnica *Bow-Tie* como ferramenta central de investigação.

Diante desse cenário, este estudo objetiva aplicar a técnica *Bow-Tie* para identificar e analisar as cadeias causais multidimensionais dos riscos à privacidade em uma IFE. Especificamente, busca-se: (i) mapear as consequências desses riscos; (ii) propor controles integrados para sua mitigação.

O foco deste estudo é analisar, sob uma perspectiva holística, os riscos de privacidade associados às operações de tratamento de dados pessoais envolvendo os processos de assistência estudantil de uma IFE. Especificamente, busca-se: (i) preencher a lacuna empírica mediante uma análise detalhada de riscos; (ii) oferecer e testar um instrumento metodológico replicável para análise de riscos, baseado na técnica *Bow-Tie*; e (iii) apresentar controles preventivos e mitigatórios baseados na criticidade das cadeias causais identificadas, subsidiando a governança orientada a risco.

A pesquisa se diferencia aos demais estudos publicados no Brasil ao aplicar a técnica *Bow-Tie* à análise de riscos de privacidade no setor educacional público. Essa abordagem permite examinar, de forma integrada, as interações entre causas técnicas, organizacionais, jurídicas e humanas no tratamento de dados sensíveis de estudantes. A aplicação desta ferramenta em uma Instituição Federal de Ensino representa uma inovação metodológica capaz de subsidiar a governança orientada a risco e a conformidade com a LGPD em contextos educacionais reais.

Espera-se que os resultados deste estudo contribuam teoricamente ao validar e expandir a aplicação de um método de análise causal ao domínio da privacidade educacional. Na prática, fornece um diagnóstico e instrumentos para que gestores e Encarregados de Tratamento de Dados Pessoais, possam manter a proteção de dados e ter condições para a sustentabilidade da confiança no ambiente educacional digital.

O artigo está organizado em seis seções. Após esta introdução, a Seção 2 revisa o referencial teórico sobre LGPD, particularidades do contexto educacional, *frameworks* de risco e a fragmentação no campo de estudo. A Seção 3 detalha a metodologia aplicada. A Seção 4

apresenta e discute os resultados da modelagem *Bow-Tie*. A Seção 5 conclui com as contribuições do estudo e pesquisas futuras. Por fim, listam-se as referências.

2. Referencial Teórico

Esta seção fundamenta o estudo ao revisar conceitos-chave, o contexto específico da educação, os principais *frameworks* de avaliação de riscos e, de forma crítica, as contribuições e limitações da literatura existente. O objetivo é situar a pesquisa dentro do debate teórico sobre privacidade, demonstrando como o estudo responde a carência de pesquisa identificada.

2.1. O Marco Normativo da LGPD

A LGPD (Lei nº 13.709/2018) consolida o marco regulatório brasileiro (Brasil, 2018). Seu conceito amplo de tratamento abrange todas as operações desde a coleta até a eliminação (Art. 5º, X), evidenciando que as vulnerabilidades se distribuem ao longo de todo o ciclo de vida dos dados (Dantas & Dodt, 2025; Reis et al., 2024). Portanto, a proteção de dados configura-se não como uma ação pontual, mas como um processo contínuo e integrado (Candiani & Pereira, 2024).

Nesse contexto, princípios como finalidade determinada, adequação, necessidade e prevenção (Art. 6º) constituem a base normativa para a identificação proativa de riscos. Barros e Vilela (2025) destacam que a efetiva aplicação da LGPD no setor educacional enfrenta diversos desafios de maturidade institucional. Essas dificuldades reforçam a necessidade de avaliações de risco sistemáticas e contextualizadas, essenciais para transformar a *accountability* em realidade prática (Doneda, 2021).

Segundo dados divulgados pelo TCU, cerca de 76,7% das organizações públicas federais encontram-se nos níveis inexpressivo ou inicial de adequação à LGPD (Brasil, 2025). Diante dessa constatação, a conformidade com esta Lei exige uma visão holística do fluxo informacional. Nessa perspectiva, cada fase do ciclo de vida dos dados demanda salvaguardas específicas. Portanto, essa compreensão é fundamental para qualquer análise de risco que pretenda ser efetiva e alinhada ao espírito da LGPD.

2.2. A Privacidade no Contexto Educacional

A privacidade consolida-se como um direito fundamental indissociável da dignidade humana, da autonomia individual e do exercício pleno da cidadania em sociedades democráticas (Doneda, 2021). Na esteira da transformação digital, sua proteção transcende a esfera pessoal para configurar-se como condição essencial para a liberdade de expressão, o desenvolvimento psicossocial e a construção de relações de confiança no ambiente educacional, especialmente quando envolvem grupos em situação de vulnerabilidade, como crianças e adolescentes, cuja proteção reforçada é prevista no Art. 14 da LGPD (Brasil, 2018; UNESCO, 2022).

Neste contexto, o ambiente educacional contemporâneo configura-se como um ecossistema digital heterogêneo. Ele integra sistemas acadêmicos, ambientes virtuais de aprendizagem e ferramentas analíticas (Barros & Vilela, 2025). Este cenário gera uma produção massiva de dados não apenas acadêmicos, mas também sensíveis, criando um perfil íntimo do indivíduo em formação, o que tem dificultado cada vez mais a governança de privacidade dentro das instituições de ensino (UNESCO, 2022).

A adoção crescente de tecnologias *data-driven*, como a inteligência artificial educacional, introduz complexidades adicionais (UNESCO, 2022). Questões relacionadas à opacidade algorítmica e ao consentimento informado tornam-se prementes (Khalil, Shakya & Liu, 2025). Um aspecto crítico, regulado pelo Art. 14 da LGPD, é a condição peculiar de desenvolvimento de crianças e adolescentes (Brasil, 2018). Para este grupo, incidentes de privacidade podem ter impactos psicossociais profundos e duradouros (UNICEF, 2021).

O cenário educacional não apenas concentra dados sensíveis, mas o faz junto a uma população titular com vulnerabilidades específicas (Araújo, 2021). Tal conjuntura demanda salvaguardas proporcionais e reforçadas. Nesse sentido, iniciativas internacionais como o *Student Privacy Pledge* (*Future of Privacy Forum*, 2021) buscam estabelecer compromissos éticos para provedores de tecnologia educacional, que se comprometem a limitar a coleta de dados e a proibir seu uso para publicidade direcionada. Portanto, a conformidade com a LGPD no contexto educacional deve ser reinterpretada como um processo pedagógico contínuo, que protege os dados ao mesmo tempo em que educa para a privacidade.

2.3. Riscos dos processos de tratamento de dados pessoais

Segundo Alves (2025), o ambiente digital na educação apresenta riscos significativos que vão além da segurança técnica, encontrando um paralelo preocupante na ineficiência estrutural do setor público no tratamento de dados pessoais, o que amplia a vulnerabilidade de titulares em todos os contextos. Para Freitas (2022) essa vulnerabilidade sistêmica, que expõe desde o aluno em formação até o cidadão em sua relação com o Estado, evidencia que o principal desafio não é tecnológico, mas sim de governança e de implementação efetiva de uma cultura de proteção de dados.

Conforme demonstram auditorias do Tribunal de Contas da União nos últimos anos, os riscos nos processos de tratamento de dados pessoais na esfera pública ainda são sistêmicos e graves. Dados de 2025 evidenciam que os órgãos federais fiscalizados apresentavam inconformidades com a Lei Geral de Proteção de Dados Pessoais (Brasil, 2022; Brasil, 2025).

Essa realidade coloca em risco a privacidade de milhões de cidadãos. As principais fragilidades identificadas são a carência de um mapeamento completo dos fluxos de dados, a ausência de indicadores para avaliar a eficácia dos controles e a insuficiência de capacitação específica para os servidores (Brasil, 2022; Brasil, 2025). Tais deficiências elevam consideravelmente a probabilidade de incidentes de segurança da informação.

Como agravante, o relatório de não conformidade do TCU destaca que várias instituições auditadas não dispõem de protocolos definidos para comunicar violações à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados (Brasil, 2025). A manutenção de processos nessas condições configura descumprimento legal. Ademais, compromete a confiança da sociedade no Estado e gera exposição a danos reputacionais e à imagem da administração pública.

2.4. Abordagens Metodológicas para Avaliação de Riscos de Privacidade

A avaliação sistemática de riscos constitui um pilar central da governança em privacidade (ABNT, 2023). Diversos *frameworks* oferecem orientações, cada qual com uma ênfase distinta. Entre eles destacam-se:

A norma ABNT NBR ISO/IEC 27701 estabelece requisitos para um sistema de gestão de informação privada, sendo uma extensão das normas de segurança da informação (ABNT, 2022). O objetivo desta norma é auxiliar as organizações a gerenciarem dados pessoais em conformidade com leis como a LGPD.

Paralelamente, a ABNT NBR ISO/IEC 29134 (ABNT, 2023) fornece diretrizes para a realização de Relatórios de Impacto à Proteção de Dados (RIPD). A ABNT NBR ISO/IEC 27005, por sua vez é um guia para a identificação, análise, avaliação e tratamento de riscos relacionados à segurança da informação e privacidade (ABNT, 2022). A ABNT NBR ISO/IEC 27557 estabelece o *framework* e diretrizes para a aplicação prática dos princípios da ABNT NBR ISO 31000:2018 (Gestão de Riscos) especificamente ao contexto da proteção da privacidade dentro de uma organização, integrando a gestão de riscos de privacidade ao processo de governança organizacional mais amplo.

No âmbito federal, o Programa de Privacidade e Segurança da Informação institucionaliza a gestão de riscos como uma ferramenta de governança de estado (Brasil, 2025). Internacionalmente, o *NIST Privacy Framework* propõe uma estrutura flexível para integrar a gestão de riscos aos processos organizacionais (NIST, 2020).

No contexto internacional, estudos recentes têm destacado as limitações de abordagens tradicionais de avaliação de riscos quando aplicadas a ambientes educacionais *data-driven*, especialmente no setor público, onde coexistem assimetrias de poder, dependência tecnológica e fragilidades institucionais (Selwyn, 2020; Khalil et al., 2025). Pesquisas conduzidas em universidades europeias e norte-americanas indicam que a proteção da privacidade estudantil exige instrumentos capazes de articular dimensões técnicas, organizacionais e normativas, sob pena de se reduzir a conformidade regulatória a um exercício meramente formal (UNESCO, 2022; NIST, 2020). Nesse sentido, a presente pesquisa dialoga com esse debate internacional ao propor e testar empiricamente um modelo analítico multidimensional, adaptado à realidade das Instituições Federais de Ensino.

2.5. A técnica *Bow-Tie* como Ferramenta de Modelagem Causal

Para além dos *frameworks* apresentados neste estudo, a técnica *Bow-Tie* destaca-se como uma ferramenta para modelagem causal (ABNT, 2021). Esta técnica permite visualizar de forma integrada as relações entre causas, eventos centrais indesejados, consequências e os controles preventivos e mitigatórios.

A capacidade de mapear cadeias causais desta técnica oferece uma vantagem analítica sobre abordagens puramente enumerativas. O estudo posiciona a *Bow-Tie* como uma ferramenta capaz de operacionalizar a visão sociotécnica da privacidade proposta por Nissenbaum (2009). A técnica força a análise simultânea de falhas técnicas, processos organizacionais, relações contratuais e fatores humanos. Dessa forma, trata o risco como um fenômeno emergente da interação entre essas dimensões.

2.6. Abordagens Críticas sobre Vigilância e Governança de Dados

Para além do marco normativo e dos *frameworks* de gestão, este estudo fundamenta-se em abordagens críticas que problematizam a vigilância digital e a governança de dados. Autores como Zuboff (2019) e Lyon (2001) alertam para a naturalização do monitoramento contínuo em âmbitos sociais, incluindo o educacional.

A noção de integridade contextual, proposta por Nissenbaum (2009), oferece um parâmetro ético-normativo para avaliar a pertinência dos fluxos de dados no ecossistema pedagógico. Paralelamente, perspectivas como o colonialismo de dados (Couldry & Mejias, 2019) e os algoritmos de opressão (Noble, 2018) ajudam a desvendar as assimetrias de poder e os riscos de discriminação sistêmica.

Esta base crítica permite interpretar os riscos de privacidade não apenas como ausências de conformidade, mas como manifestações de dinâmicas estruturais de vigilância e desequilíbrio informacional. Consequentemente, a mitigação efetiva demanda intervenções que atuem simultaneamente nas dimensões técnica, judicial e cultural, desafiando a normalização da vigilância e reafirmando o espaço educativo como ambiente protegido.

2.7. Trabalhos Relacionados e Identificação da Limitação Analítica

A literatura científica recente avança na compreensão dos riscos no setor público federal, porém com focos específicos que deixam uma carência analítica para a privacidade no contexto educacional. Para evidenciar essa limitação, a Tabela 1 sintetiza e compara estudos relevantes, destacando seus escopos principais e suas insuficiências em relação aos objetivos desta pesquisa.

Tabela 1

Análise comparativa de estudos sobre gestão de riscos no setor público federal

Estudo	Ano	Foco Principal	Contexto/Setor	Limitação relativa a esta pesquisa
Kruse, Smith, Vanderlinden & Nealand	2017	Revisão sistemática analisa 270 artigos sobre cibersegurança na saúde, identificando as principais vulnerabilidades, ameaças e tendências no setor.	Saúde	Ênfase em controles de cibersegurança.
Araújo & Gomes	2021	Desafios na implantação da gestão de riscos.	Universidades Federais (geral)	Objetivo genérico na gestão de riscos, não na privacidade.
Araújo & Callado	2022	Compreender como as práticas de gestão de riscos implementadas no contexto de uma universidade federal brasileira se configuraram às recomendações dos *frameworks* internacionais, e seu alcance como mecanismo de controle de governança pública.	Universidade Federal	Destaque para práticas de gestão de riscos.
Alves, Georg & Nunes	2022	Riscos de negócio de tribunais.	Poder Judiciário	Foco em riscos de negócio em segurança cibernética em tribunais judiciários.
Zottmann et al.	2023	Avaliação de riscos de privacidade.	Poder Judiciário	Destaque setorial no judiciário; não aborda as particularidades pedagógicas.
Tomaz, Nunes & Silva	2025	Riscos de negócio para segurança cibernética em um instituto federal de educação.	Instituição Federal de Ensino	Propósito em segurança da informação e continuidade de negócio, não nos riscos substantivos à privacidade.
Gonçalves et al.	2025	Riscos cibernéticos para universidades.	Universidades	Concentra-se em ameaças externas e disponibilidade e não nos riscos internos e de processos.

Estudos como Araújo e Gomes (2021) identificam barreiras organizacionais na gestão de riscos em universidades federais, mas com um enfoque genérico que não aborda os riscos específicos da LGPD. Araújo e Callado (2022) apresentam práticas de gestão de riscos no contexto de uma universidade. Zottmann et al. (2023) integram riscos da norma ABNT NBR ISO/IEC 29134 com controles de segurança no Poder Judiciário. Alves, Georg & Nunes (2022) apresentam riscos de negócio em cibersegurança em tribunais judiciários utilizando o método *Bow-Tie*.

Outras pesquisas concentram-se em ameaças cibernéticas e continuidade de negócios. Tomaz, Nunes & Silva (2025) aplicam a técnica *Bow-Tie* ao contexto educacional, mas com ênfase em segurança da informação e continuidade de negócio, não nos riscos substantivos à privacidade. Gonçalves et al. (2025) mapeiam causas e consequências de ataques cibernéticos em universidades, porém não abordam os riscos internos e de processos que caracterizam violações de privacidade, como o uso indevido ou o compartilhamento inadequado de dados pessoais.

Como demonstrado, os estudos convergem para a importância da gestão de riscos, porém possuem escopos limitados. Falta uma investigação que, no contexto específico das IFEs, integre em um único modelo analítico os requisitos da LGPD, a dimensão contratual crítica, os fatores humanos e as cadeias causais que os conectam. Esta pesquisa preenche essa questão em aberto ao empregar a técnica *Bow-Tie* para desvendar essas interações multidimensionais.

3. Metodologia

Trata-se de uma pesquisa de natureza aplicada, pois tem como finalidade gerar conhecimentos orientados à solução de problemas concretos e atuais, com foco no aprimoramento de práticas institucionais e no suporte à tomada de decisão (Gil, 2019). Os resultados são direcionados à aplicação prática, especialmente no fortalecimento da governança, dos processos e dos controles organizacionais relacionados ao fenômeno investigado.

Quanto aos objetivos, a pesquisa caracteriza-se como exploratória e descritiva. É exploratória por buscar maior familiaridade com o problema, ainda pouco investigado no contexto estudado, permitindo a identificação de variáveis, riscos, relações causais e limitações na literatura existente. Simultaneamente, é descritiva, uma vez que se propõe a caracterizar, sistematizar e analisar os fenômenos observados, descrevendo suas características, causas, consequências, controles e inter-relações de forma estruturada e analítica.

O estudo adota a abordagem qualitativa, adequada à compreensão aprofundada de fenômenos complexos, sociotécnicos e organizacionais do mundo real, cuja natureza subjetiva nem sempre é passível de quantificação direta. Essa estratégia possibilita captar percepções, experiências, práticas e significados atribuídos pelos participantes, bem como compreender o contexto institucional no qual os processos analisados estão inseridos.

O método de pesquisa baseia-se no estudo empírico, com ênfase na análise interpretativa dos dados. Para garantir maior robustez analítica, emprega-se a triangulação de dados, combinando diferentes fontes e técnicas de coleta de dados, o que contribui para a validação dos achados e para a redução de vieses.

A análise dos dados é realizada por meio da análise de conteúdo, seguindo as etapas propostas por Bardin (2016), envolvendo pré-análise, exploração do material e tratamento e interpretação dos resultados. Essa técnica possibilita a categorização sistemática dos dados e a identificação de padrões, relações e significados relevantes ao objetivo do estudo.

De forma complementar, foram utilizados instrumentos analíticos estruturantes, como modelos causais e matriz de risco, com o propósito de organizar os achados, evidenciar relações entre causas, eventos e consequências e apoiar a proposição de recomendações práticas (ABNT, 2021).

3.1. Desenho da Pesquisa

A pesquisa foi conduzida em uma IFE de médio porte na região norte do país que oferece cursos nas modalidades de ensino: médio, técnico subsequente, formação inicial e continuada, graduação e pós-graduação. Esta instituição tem 7530 estudantes matriculados, 810 docentes e 632 técnicos administrativos divididos em 12 campus. O estudo foi dividido em três etapas: planejamento, execução e divulgação dos resultados.

Na primeira etapa realizou-se pesquisa bibliográfica (artigos científicos, leis, decretos, instruções normativas, guias, normas internas, nacionais e internacionais, bem como documentos (políticas, normas, relatórios, processos e procedimentos). Também foram definidos o tipo de pesquisa (qualitativa), a população (intencional - IFE) e a amostra (estudantes, docentes e técnicos administrativos da IFE), os instrumentos de coleta (roteiros de entrevistas e grupo focal) e procedimentos de análise (análise de conteúdo temática).

Na segunda etapa “execução” foram realizadas a coleta e análise de dados. Para garantir o rigor e a validade do constructo, adotou-se uma estratégia de triangulação de fontes e técnicas. A coleta de dados ocorreu entre outubro de 2025 e janeiro de 2026 e envolveu três técnicas complementares: entrevistas, análise documental e grupo focal. Para este estudo adotaram-se os seguintes procedimentos:

- Entrevistas semiestruturadas: permitem explorar percepções, práticas e desafios vivenciados pelos atores envolvidos. Foram realizadas 48 entrevistas para captar a diversidade de perspectivas: gestores (n=8), docentes (n=9), técnicos administrativos (n=15) e estudantes (n=16). Para tal, utilizaram-se dois roteiros distintos (servidores e estudantes). A coleta foi interrompida ao atingir a saturação teórica (Saunders, Lewis & Thornhill, 2018);
- Análise documental: voltada ao exame de políticas, normas, processos, procedimentos, contratos, relatórios e registros institucionais relevantes. Procedeu-se à revisão

sistemática de 25 documentos institucionais, incluindo políticas de proteção de dados, privacidade e segurança da informação, contratos com fornecedores de tecnologia, termos de uso dos sistemas de informação e ambiente virtual de aprendizagem e registros de processos operacionais de assistência estudantil. Esta análise permitiu contrastar o discurso formal com as práticas relatadas;

- Grupo focal: utilizado para aprofundar discussões, confrontar percepções e identificar convergências e divergências entre os participantes Foram conduzidas 2 sessões com oito especialistas internos (Encarregado de Dados, Analista de Segurança, Assistente Social, Psicólogo, Coordenadora de Assistência ao Estudante, Técnica em Enfermagem, Gestor de Segurança da Informação e Diretora de Assistência ao Estudante) para validar os achados preliminares, discutir a plausibilidade das relações causais identificadas e refinar as recomendações.

Na terceira etapa "divulgação dos resultados" realizou-se a caracterização do contexto analisado, apresentando as categorias principais, diretamente relacionadas ao objetivo do estudo, as evidências empíricas, a interpretação dos achados e a articulação com referências utilizadas neste estudo.

3.2. Procedimentos de Análise

A análise dos dados qualitativos seguiu os preceitos da análise de conteúdo temática (Bardin, 2016). As transcrições e documentos foram codificados em categorias, alinhadas às quatro dimensões de risco pré-teorizadas: técnico-operacional, organizacional, jurídica-contratual e humana.

O núcleo analítico consistiu na aplicação estruturada da técnica *Bow-Tie*, adaptada da norma ABNT NBR ISO/IEC 31010 (ABNT, 2021). O protocolo de análise, executado iterativamente, compreendeu cinco etapas:

- Identificação dos *eventos centrais* de perda de privacidade;
- Mapeamento causal retrospectivo (*lado esquerdo*), identificando causas a partir dos dados triangulados;
- Mapeamento prospectivo de consequências (*lado direito*), catalogando impactos para titulares e para a instituição;
- Identificação e análise de controles preventivos e mitigatórios;
- Validação e refinamento dos diagramas *Bow-Tie* preliminares no grupo focal.

Para auxiliar na organização e análise, utilizou-se o software Excel em uma planilha denominada "Análise *Bow-tie"*, disponibilizada no repositório digital desta pesquisa[1]. As ferramentas de Inteligência Artificial (IA), "perplexity" e "deepseek" foram empregadas estritamente para suporte na síntese de literatura e organização de ideias, não para análise interpretativa dos dados primários, garantindo a centralidade do juízo dos pesquisadores. Os

[1] https://zenodo.org/uploads/18493392

autores revisaram criticamente e validaram todo o conteúdo gerado ou auxiliado por IA mantendo a responsabilidade intelectual última sobre o trabalho.

3.3. Considerações Éticas

A pesquisa não envolveu coleta de dados sensíveis de seres humanos de forma a configurar intervenção que exija apreciação por Comitê de Ética, conforme Resolução do Conselho Nacional da Saúde nº 510/2016, limitando-se a análise documental e entrevistas com estudantes, docentes e técnicos administrativos sobre processos institucionais de assistência estudantil (Brasil, 2016). O estudo foi conduzido em conformidade com preceitos éticos para pesquisas sociais. Na realização das entrevistas garantiu-se o anonimato dos participantes, a confidencialidade das informações e o uso dos dados exclusivamente para fins acadêmicos. Também foram adotadas salvaguardas técnicas para o manuseio dos dados coletados, alinhadas aos princípios da LGPD (Brasil, 2018).

4. Apresentação e Discussão dos Resultados

A aplicação da técnica *Bow-Tie* como núcleo metodológico permitiu alcançar o objetivo central deste estudo: analisar, de forma integrada e causal, os riscos de privacidade associados ao tratamento de dados pessoais nos processos de assistência estudantil de uma IFE. Os resultados revelam um cenário de complexidade sistêmica, no qual vulnerabilidades técnicas, organizacionais, jurídicas e humanas interagem de forma sinérgica, potencializando riscos e comprometendo a efetividade da proteção de dados. Esta seção apresenta e discute criticamente os achados empíricos disponibilizados no repositório de dados da pesquisa articulando-os com o referencial teórico e destacando suas implicações práticas e teóricas.

4.1. Modelagem Causal com a Técnica *Bow-Tie*: Uma Taxonomia de Riscos Multidimensionais

A análise qualitativa dos dados triangulados (entrevistas, documentos, grupo focal) permitiu inicialmente identificar um amplo espectro de preocupações. Após consolidação e validação com especialistas, essas apreensões foram sintetizadas em quinze riscos primários, categorizados conforme suas dimensões predominantes. A Tabela 2 apresenta esta taxonomia, que evidencia a natureza transversal e inter-relacionada das principais ameaças à privacidade citadas nas entrevistas.

Tabela 2
Taxonomia dos riscos de privacidade na IFE investigada

Nº	Risco de Privacidade	Dimensão Predominante
1	Coleta excessiva de dados sensíveis de estudantes em processos de assistência estudantil.	Organizacional/Jurídica
2	Divulgação indevida de dados sensíveis de estudantes no âmbito da assistência estudantil.	Organizacional/Humana

3	Compartilhamento indevido ou irregular de dados sensíveis de estudantes com terceiros.	Organizacional/Jurídica/Contratual
4	Armazenamento inseguro de dados sensíveis de estudantes em sistemas e suporte da assistência estudantil.	Técnico-operacional/ Organizacional
5	Cláusulas abusivas ou desproporcionais em contratos com terceiros.	Jurídica/Humana
6	Uso secundário indevido de dados sensíveis coletados para assistência estudantil para outras finalidades não comunicadas, não autorizadas ou incompatíveis com o propósito original do tratamento.	Jurídica/Técnico-operacional
7	Cultura organizacional frágil e permissiva quanto ao sigilo e à proteção de dados sensíveis na assistência estudantil.	Humana/Organizacional
8	Acesso indevido a dados pessoais de estudantes em situação de vulnerabilidade socioeconômica, psicológica ou de saúde.	Técnico-operacional/Organizacional
9	Retenção excessiva de dados sensíveis de estudantes após o término do vínculo ou da necessidade assistencial.	Organizacional/Jurídica
10	Tratamento inadequado ou inseguro de dados sensíveis de estudantes por terceiros.	Contratual/Jurídica/Organizacional
11	Vazamento de dados pessoais sensíveis de estudantes em situação de vulnerabilidade.	Técnico-operacional
12	Capacitação insuficiente e inadequada em privacidade e proteção de dados para servidores da assistência estudantil.	Humana/Organizacional
13	Monitoramento não transparente de dados pessoais de estudantes no contexto da assistência estudantil.	Técnico-operacional/Jurídica
14	Descarte ou eliminação insegura de dados sensíveis de estudantes nos processos de assistência estudantil.	Técnico-operacional/Organizacional
15	Reidentificação de dados sensíveis de estudantes anonimizados ou pseudonimizados em resultados de seleção de estudantes, benefícios assistenciais, avaliações e pesquisas psicossociais e socioeconômicas.	Técnico-Operacional

É importante distinguir, na taxonomia proposta, os riscos que emanam de falhas procedimentais internas daqueles decorrentes de ameaças externas ou falhas de segurança técnica. Enquanto o 'Vazamento de dados pessoais sensíveis de estudantes' (Risco 11) refere-se a incidentes de segurança que comprometem a confidencialidade, frequentemente tratados sob a ótica da Segurança da Informação, a ‘Divulgação indevida de dados sensíveis de estudantes' (Risco 2) identificada neste estudo possui natureza organizacional e humana. Ela ocorre quando o acesso legítimo aos dados é mal gerenciado internamente, resultando na exposição de informações sensíveis de estudantes por falta de *Privacy by Design* nos processos de trabalho, e não necessariamente por falha tecnológica.

A taxonomia vai além de uma listagem, demonstrando que os riscos não são técnicos isolados, mas frequentemente estão enraizados em falhas de governança (riscos 1, 3, 9, 14), cultura organizacional (7, 12) e na gestão da relação com terceiros (3, 10). Essa visão corrobora

a perspectiva sociotécnica da privacidade (Nissenbaum, 2009), indicando que a solução exigirá uma transformação que aborde simultaneamente tecnologias, processos, contratos e pessoas.

A análise dos riscos identificados neste estudo, especialmente aqueles relacionados ao monitoramento não transparente e à coleta e retenção excessiva de dados sensíveis (Riscos 13, 1 e 9), corrobora a teoria do 'Excedente Comportamental' de Zuboff (2019). No contexto da assistência estudantil, observa-se que a coleta de dados frequentemente excede a estrita necessidade para concessão de benefícios, gerando um acúmulo informacional que, sem governança adequada, pode transformar o ambiente de cuidado em mecanismo de vigilância.

4.2. Análise Retrospectiva de Padrões e Cadeias Causais Sistêmicas

A aplicação da técnica *Bow-Tie* possibilitou um mergulho analítico retrospectivo, mapeando as 25 causas por trás dos riscos identificados. A Tabela 3 condensa as principais causas citadas pelos participantes deste estudo e sua associação com os riscos da Tabela 2.

Tabela 3
Análise causal retrospectiva

Nº	Causa	Riscos relacionados
C1	Cultura organizacional negligente com a privacidade.	Todos, em especial 2, 5, 7, 12
C2	Uso de ferramentas não oficiais para a comunicação (e-mail pessoal, WhatsApp, nuvem pública).	2, 3, 6, 11
C3	Falta de sistemas integrados e adequados.	14
C4	Orçamento insuficiente para a implementação de controles de privacidade e segurança da informação.	4, 10, 12
C5	Falta de pessoas qualificadas e sobrecarga de trabalho.	1, 2, 3, 4, 6, 9, 10, 14
C6	Falta de transparência e consentimento inadequado no tratamento de dados pessoais.	1, 9, 14
C7	Treinamentos genéricos e desconectados da realidade da instituição.	1, 2, 3, 4, 6, 9, 10, 14

A análise *Bow-Tie* disponibilizada no repositório digital deste estudo revela que as vulnerabilidades não emanam de eventos estanques, mas de cadeias causais sistêmicas. Por exemplo, a fragilidade contratual com fornecedores (causa implícita em (C3) gera dependência tecnológica e perda de controle sobre dados (Risco 10), o que, associado a treinamentos genéricos e desconectados da realidade da instituição (C7, C5, Risco 12), leva a práticas operacionais inseguras (Riscos 2, 8, 14).

A cultura organizacional negligente com a privacidade (C1) resulta em decisões e controles descoordenados, criando brechas exploradas por ameaças técnicas e humanas. Este achado ressalta a insuficiência de abordagens que tratam os riscos de forma isolada, demandando uma visão holística e integrada da governança.

4.3. Consequências em Múltiplos Níveis: Impactos Diferenciados e Estratificados

A modelagem prospectiva do lado direito da *Bow-Tie* permitiu categorizar 28 consequências, operando em dois níveis principais: impactos sobre os titulares (estudantes) e sobre a instituição. A Tabela 4 sintetiza as principais consequências citadas pelos participantes desse estudo, evidenciando a assimetria dos impactos.

Tabela 4
Consequências diretas para titulares e instituição

Consequências para os Titulares (Estudantes)	**Riscos Relacionados**
Impactos Psicossociais e de Direitos Fundamentais	
• Sensação de vigilância, constrangimento e invasão da intimidade.	13
• Discriminação, estigmatização e rotulação (ex.: "vulnerável", "deficiente").	2, 3, 8, 10, 11, 13, 15
• Danos à imagem, honra e vida acadêmica (bullying, exclusão).	2, 3, 8, 10, 11, 13, 15
• Danos psicológicos, morais e emocionais.	2, 3, 8, 10, 11, 13, 15
Impactos Materiais e Sociais	
• Prejuízos educacionais e profissionais	2, 3, 8, 10, 11
• Vulnerabilidade a chantagem, fraudes, golpes e roubo de identidade.	2, 3, 8, 10, 11, 14
Consequências para a Instituição (IFE)	**Riscos Relacionados**
Impactos Jurídicos e Regulatórios	
• Violação da LGPD.	1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 13, 14, 15
• Exposição a sanções da ANPD.	1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 13, 14, 15
• Ações judiciais individuais e coletivas.	2, 3, 6, 8, 10, 11
• Corresponsabilização por incidentes com terceiros.	5, 10
Impactos Reputacionais e de Confiança	
• Dano à reputação e credibilidade institucional.	2, 3, 8, 10, 11, 15

• Erosão do espaço educativo como ambiente de confiança.	2, 3, 8, 10, 11, 13, 15
• Campanhas de difamação em redes sociais.	2, 3, 8, 10, 11, 15
Impactos Operacionais e Estruturais	
• Sobrecarga operacional para gestão de incidentes e respostas.	2, 3, 8, 10, 11, 14
• Reforço de desigualdades e discriminação algorítmica.	2, 3, 8, 10, 11, 13

Os achados deste estudo mostram que a materialização dos riscos não é homogênea. Para os estudantes, em especial crianças e adolescentes, grupo com proteção reforçada pela LGPD (Art. 14), os impactos são profundamente pessoais e psicossociais, afetando seu desenvolvimento, dignidade e confiança na instituição. Para a IFE, os impactos são predominantemente institucionais: jurídicos, reputacionais e operacionais.

Esta assimetria pode gerar uma percepção diferente do risco entre gestores e titulares, em que os danos concretos aos indivíduos são subestimados em favor de preocupações com compliance e imagem. Os resultados apontam para uma incoerência ética fundamental: a instituição, ao falhar na proteção dos dados sensíveis que coleta no âmbito de sua missão de assistência e acolhimento, corrói a própria relação de confiança que é essencial para o sucesso dessa missão.

4.4. Discussão Integrada: Mecanismos de Interação e a Amplificação Sistêmica do Risco

A análise transcendeu a identificação de fatores, revelando padrões relacionais dinâmicos nos quais falhas em uma dimensão ativa e amplificam riscos em outras. O diagrama *Bow-Tie* da (Figura 1), disponível no repositório digital desta pesquisa, ilustra sinteticamente esse fenômeno. Conforme ilustrado na Figura 1, o lado esquerdo do diagrama ilustra as ameaças e barreiras preventivas identificadas durante as entrevistas e grupos focais. O centro representa o evento indesejado (Coleta excessiva de dados sensíveis de estudantes). O lado direito projeta as medidas de recuperação e as consequências potenciais para os discentes e para a imagem institucional, evidenciando a necessidade de uma abordagem preventiva baseada em *Privacy by Design*.

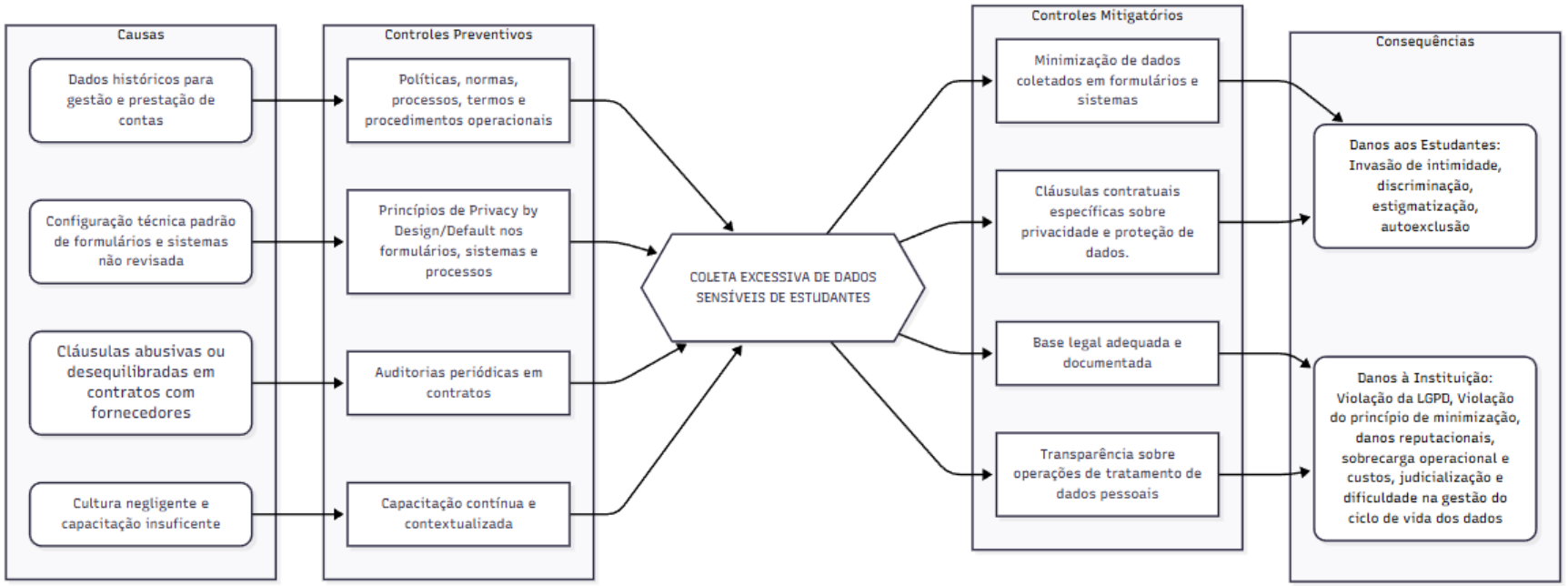

Figura 1: Diagrama *Bow-Tie* para coleta excessiva de dados sensíveis de estudantes.

Neste diagrama, causas como " Cláusulas abusivas ou desequilibradas em contratos com fornecedores" (Dimensão Contratual) e "Cultura negligente e capacitação insuficiente" (Dimensão Organizacional e Humana) convergem para a "Configuração técnica padrão não revisada" (Dimensão Técnica), gerando o evento central do "Coleta excessiva de dados sensíveis de estudantes". As consequências se desdobram em invasão de intimidade (nível individual), violação da LGPD (nível jurídico), sobrecarga operacional (nível operacional), normalização da vigilância, erosão do espaço educativo (nível sistêmico) e danos reputacionais (nível organizacional).

Este modelo visual evidencia que a dimensão técnico-operacional atua como um nó crítico de amplificação sistêmica. Contratos mal elaborados e governança frágil criam as condições para que decisões técnicas inadequadas (configuração técnica padrão para coleta excessiva de dados em formulários e sistemas) se concretizem, escapando ao controle organizacional e gerando danos em cascata. Enquanto estudos como Tomaz et al. (2025) focam em riscos de disponibilidade (cibernéticos), nossos dados expõem um risco de subordinação pedagógica à lógica da datificação, onde ferramentas tecnológicas, mal configuradas e governadas, reconfiguram práticas e relações educacionais de maneira opaca e potencialmente danosa.

Portanto, a governança da privacidade nas IFEs revela-se como a governança de uma capacidade institucional crítica, que se constrói sobre um tripé fundamental: a cultura de proteção de dados, a estrutura organizacional adequada e a capacitação contínua de pessoas. Esta capacidade se materializa na competência de especificação, aquisição e controle de tecnologias, bem como na gestão eficiente de contratos. Proteger a privacidade significa, nesse contexto, assegurar o domínio técnico e humano sobre as escolhas que definem como os dados são coletados, processados e compartilhados, garantindo que processos, contratos e sistemas reflitam os valores éticos e os compromissos da instituição.

4.5. Lacunas Críticas e uma Matriz de Controles Integrados

A aplicação da *Bow-Tie* não apenas mapeou riscos, mas também expôs lacunas críticas na governança da IFE estudada:

- Ausência de avaliação de impacto à proteção de dados sistemática;
- Predomínio de uma abordagem reativa sobre a preventiva;
- Assimetria informacional com os titulares;
- Desconexão entre políticas formais e práticas operacionais;
- Proteção insuficiente para grupos vulneráveis.

Como produto analítico voltado à ação, o estudo propõe uma matriz de controles integrados, apresentada no apêndice A, com 22 medidas preventivas e mitigatórias distribuídas pelas quatro dimensões, conforme validação dos especialistas. Algumas medidas não são atendidas pelos controles do PPSI, dentre elas vale destacar: Política de gestão de dados com critérios de classificação e prazos de retenção e descarte de dados, norma para uso de tecnologias emergentes no setor de assistência estudantil, como por exemplo inteligência

artificial generativa, política de minimização/pseudonimização de dados pessoais e política de monitoramento digital. Nesta matriz também são apresentados controles transversais habilitadores, como gestão de riscos e conformidade proativa, programa de capacitação contínua e personalizada, minimização de coleta e retenção de dados. O grupo focal destacou que controles técnicos de segurança da informação (criptografia, MFA, RBAC, *backups* criptografados) só serão efetivos se ancorados por uma governança fortalecida (ex.: comitê institucional de privacidade com autoridade real e representação multissetorial) e por relações contratuais seguras através do fortalecimento da cultura de privacidade.

4.6. Síntese dos Achados e Transição para a Conclusão

Em síntese, os resultados apresentam um quadro de riscos sistêmicos e multidimensionais, em que disfunções na cultura, na governança e na gestão contratual criam um terreno fértil para que vulnerabilidades técnicas se materializem, gerando consequências severas e assimétricas. A aplicação da técnica Bow-Tie permitiu explicitar relações causais complexas, superando abordagens baseadas exclusivamente em *checklists* normativos.

Adicionalmente, à luz da teoria da integridade contextual de Nissenbaum (2009), percebe-se que o fluxo de informações dentro da IFE carece de normas contextuais claras. Quando dados de vulnerabilidade social de um estudante são acessíveis por setores administrativos sem finalidade direta na assistência, rompe-se a expectativa de privacidade daquele contexto específico, violando a confiança depositada na instituição e estigmatiza o estudante. O estudo demonstra que a mitigação efetiva de riscos exige romper com abordagens fragmentadas e adotar uma estratégia de governança coordenada e baseada em risco, que reforce simultaneamente a capacidade técnica, a estrutura organizacional, os instrumentos jurídico-contratuais e a conscientização humana.

4.7. Implicações Gerenciais e Práticas

Para mitigar os riscos mapeados, este estudo propõe controles específicos adaptados à realidade da IFE, indo além das medidas genéricas de segurança da informação. Destacam-se:

- Anonimização em relatórios de gestão: implementação de protocolos que obriguem a desidentificação de dados socioeconômicos em relatórios administrativos e pedagógicos que circulam fora da Pró-Reitoria de Assistência ao Estudante;
- Protocolos de sigilo contextual: criação de termos de confidencialidade específicos para servidores que lidam com dados de saúde e vulnerabilidade, reforçando o dever ético e legal de não cruzamento dessas informações com dados de desempenho acadêmico sem consentimento explícito;
- Transparência ativa focada: reformulação do portal institucional para incluir, em linguagem simples, exatamente quais dados são coletados para a assistência estudantil, por quanto tempo são retidos e quem possui acesso a eles, empoderando o titular dos dados.

Conclusão

Este estudo investigou os riscos de privacidade associados ao tratamento de dados pessoais nos processos de assistência estudantil de uma Instituição Federal de Ensino (IFE), mediante uma abordagem multidimensional fundamentada na técnica *Bow-Tie*. Os resultados confirmam a natureza sociotécnica e sistêmica desses riscos, os quais emergem da interação dinâmica e frequentemente sinérgica entre quatro dimensões inter-relacionadas: técnico-operacional, organizacional-governamental, jurídico-contratual e humano-cultural.

A análise revelou um cenário de vulnerabilidades profundas e interconectadas. A identificação de quinze riscos primários e de 25 cadeias causais demonstra que as falhas não são episódicas, mas se originam de disfunções estruturais. A dimensão técnico-operacional evidenciou-se como um amplificador sistêmico de risco: cláusulas contratuais genéricas com terceiros, a dependência de sistemas inadequados e a manutenção de configurações padrão não revisadas criam um ambiente no qual violações tornam-se prováveis, comprometendo a efetividade de outros controles. Esse achado avança a literatura ao reposicionar a competência para especificação técnica e jurídica como núcleo crítico da governança da privacidade, transcendendo a sua concepção como mero requisito técnico.

Os impactos identificados são multiníveis e assimétricos. Para os titulares, em especial estudantes em situação de vulnerabilidade, as consequências extrapolam a esfera digital, materializando-se em danos psicossociais, risco de estigmatização, autocensura e erosão da confiança nos mecanismos institucionais de apoio. Para a IFE, os riscos se materializam na forma de exposição a sanções administrativas, litígios judiciais, danos reputacionais severos, sobrecarga operacional e custos associados. Em última instância, a gestão inadequada da privacidade ameaça a própria missão educacional, podendo normalizar práticas de vigilância, amplificar desigualdades e corroer o espaço educativo como ambiente de confiança e experimentação.

Os achados não indicam inconformidades pontuais, mas revelam uma cultura organizacional disfuncional, na qual a busca por agilidade operacional, manifestada em práticas informais de aceleração processual, a fragmentação das decisões e a insuficiência de capacitação sistemática se sobrepõem ao dever ético e legal de proteção de dados. A instituição depara-se, assim, com uma grave incoerência: embora busque promover a formação integral e o bem-estar discente, falha em proteger os dados sensíveis inerentes a esse processo, minando a relação de confiança que deveria fundamentá-lo.

Diante desse diagnóstico, torna-se evidente que a solução transcende a implementação de controles técnicos isolados. A proteção efetiva da privacidade demanda uma transformação profunda na governança, migrando de uma abordagem reativa e fragmentada para um modelo integrado, proativo e orientado por risco. A matriz de 22 controles propostos, alinhada ao Programa de Privacidade e Segurança da Informação (PPSI) e distribuída pelas quatro dimensões analíticas, oferece um roteiro prático para essa mudança. Sua eficácia, contudo, está condicionada à adoção de ações estruturantes prioritárias:

- Fortalecimento da governança: criação de um Comitê de Privacidade com autoridade vinculante, agregando competências técnicas, jurídicas, pedagógicas e administrativas;

- Revisão do poder contratual: desenvolvimento e adoção obrigatória de cláusulas-padrão setoriais seguras em licitações de tecnologia educacional, assegurando controle efetivo sobre os operadores;

- Mudança cultural: substituição de treinamentos genéricos por programas contínuos e segmentados de capacitação, associados a campanhas de conscientização que reposicionem a privacidade como valor central da missão institucional e direito fundamental;

- Transparência ativa: implementação de mecanismos de comunicação clara e acessível, garantindo não apenas o cumprimento formal do direito à informação, mas o efetivo engajamento e controle dos titulares sobre seus dados.

As contribuições deste estudo operam em três planos complementares. Teoricamente, ele avança a literatura ao operacionalizar a perspectiva sociotécnica da privacidade mediante a técnica *Bow-Tie*, demonstrando empiricamente como os riscos em instituições educacionais públicas resultam de um processo de amplificação sociotécnica, no qual decisões organizacionais, contratuais e culturais se materializam como vulnerabilidades técnicas ao longo do ciclo de vida dos dados.

Essa análise reforça a necessidade de modelos capazes de capturar a natureza relacional e sistêmica da privacidade, superando abordagens normativas e fragmentadas. Metodologicamente, valida-se a *Bow-Tie* como um instrumento analítico eficiente e replicável para a análise causal de riscos em ecossistemas educacionais complexos, transcendendo avaliações estáticas baseadas em *checklists*. Prática e gerencialmente, o estudo oferece uma matriz integrada de controles, capaz de subsidiar gestores públicos, encarregados e formuladores de políticas na implementação de uma governança orientada por risco.

Do ponto de vista das políticas públicas, os achados indicam que a adequação das IFEs à LGPD não deve ser tratada apenas como um requisito de conformidade, mas como um componente estruturante da qualidade e da legitimidade da política educacional. A ausência de governança eficaz tende a gerar efeitos adversos, como a normalização da vigilância e a erosão da confiança institucional. Portanto, a incorporação sistemática de avaliações de impacto e o fortalecimento da capacidade contratual e técnica emergem como condições necessárias para uma transformação digital educacional socialmente responsável.

Embora o estudo apresente diversas contribuições reconhece-se como limitação o caráter singular do estudo, o que restringe a generalização estatística. No entanto, a profundidade analítica e a clareza metodológica conferem elevada transferibilidade para contextos institucionais análogos. Pesquisas futuras podem avançar por meio de estudos comparativos entre IFEs, investigações longitudinais sobre a efetividade dos controles propostos e análises

focadas em riscos emergentes associados à inteligência artificial generativa e aos *learning analytics* no setor público educacional.

Em síntese, a conformidade com a LGPD nas IFEs configura-se não como um mero imperativo regulatório, mas como uma oportunidade estratégica para realinhar práticas institucionais com valores éticos fundamentais. A digitalização da educação é irreversível, mas sua trajetória não está predeterminada.

Proteger os dados pessoais com rigor, sobretudo os de grupos vulneráveis, constitui um investimento indispensável na confiança, na dignidade e na integridade do ecossistema educacional público. Este estudo oferece, portanto, o método, o diagnóstico e as ferramentas para iniciar essa transformação necessária, reafirmando que a privacidade é alicerce, e não obstáculo, para uma educação de qualidade e para a formação de cidadãos autônomos em um mundo digital.

Referências

Associação Brasileira de Normas Técnicas. (2021). *ABNT NBR ISO/IEC 31010:2021: Gestão de riscos. Técnicas para o processo de avaliação de riscos*. Rio de Janeiro: ABNT, 2021.

Associação Brasileira de Normas Técnicas. (2023). *ABNT NBR ISO/IEC 29134:2023. Tecnologia da informação: Técnicas de segurança. Diretrizes para avaliação de impacto à privacidade.* Rio de Janeiro: ABNT, 2023.

Associação Brasileira de Normas Técnicas. (2022). *ABNT NBR ISO/IEC 27701:2022. Segurança da informação, segurança cibernética e proteção à privacidade. Sistemas de gestão da segurança da informação - Requisitos*. Rio de Janeiro: ABNT, 2022.

Associação Brasileira de Normas Técnicas. (2023a). *ABNT NBR ISO/IEC 27005:2023. Segurança da informação, segurança cibernética e proteção à privacidade. Orientações para gestão de riscos de segurança da informação.* Rio de Janeiro: ABNT, 2023.

Associação Brasileira de Normas Técnicas. (2023b). *ABNT NBR ISO/IEC 27557:2023. Segurança da informação, segurança cibernética e proteção à privacidade. Aplicação da ABNT NBR ISO 31000: 2018 para gestão de riscos de privacidade organizacional.* Rio de Janeiro: ABNT, 2023.

Alves, R. S., Georg, M. A. C., & Nunes, R. R. (2022). *Judiciário sob ataque hacker: Riscos de negócio para segurança cibernética em tribunais brasileiros.* Revista Ibérica de Sistemas e Tecnologias de Informação, 44, 344–357. https://doi.org/10.5281/zenodo.8032915

Alves, W. dos S. (2025). *Vantagens, benefícios e riscos do ambiente digital para a educação.* Revista Caderno Pedagógico, v. 22, n. 7. https://doi.org/10.54033/cadpedv22n7-175

Araújo, A., & Gomes, A. (2021). *Gestão de riscos no setor público: desafios na adoção pelas universidades federais brasileiras.* Revista Contabilidade & Finanças, São Paulo, v. 32, n. 86, p. 241-254, 2021. https://doi.org/10.1590/1808-057x202112300

Araújo, J. G. R. de & Callado, A. L. C. (2022). *Concepção e Implementação de Práticas de Gestão de Riscos: Uma Análise em uma Instituição Federal de Ensino Superior Brasileira.* Contabilidade, Gestão e Governança, vol. 25, special issue, pp. 308–330. https://doi.org/10.51341/cgg.v25iesp.2872

Bardin, L. (2016). *Análise de conteúdo*. Edição revista e ampliada. Lisboa: Edições 70.

Barros, P., & Vilela, A. (2025) *Privacy and Personal Data Protection in Educational Ecosystems: Challenges in the Application of the GDPR and LGPD*. In: *Proceedings of the*

17th International Conference on Digital Transformation. SCITEPRESS, 2025 https://www.scitepress.org/Papers/2025/134269/134269.pdf

BRASIL. (2016). Conselho Nacional de Saúde. *Resolução nº 510, de 07 de abril de 2016.* Brasília-DF.

BRASIL. (2018). Presidência da República. Secretaria-Geral. Subchefia para Assuntos Jurídicos. *Lei nº 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais (LGPD).* Brasília-DF.

BRASIL. (2022). TRIBUNAL DE CONTAS DA UNIÃO. *Acordão 1384/2022. Relatório de auditoria para avaliar as ações governamentais e os riscos à proteção de dados pessoais*.

BRASIL. (2025). Tribunal de Contas da União. *Acordão 1372/2025: Auditoria de conformidade nos controles implementados por organizações públicas federais para adequação à Lei Geral de Proteção de Dados Pessoais (LGPD).*

Candiani, I. F. & Pereira, O. J. (2024). *Lei Geral de Proteção de Dados (LGPD) nas instituições de ensino: desafios normativos para sua aplicação e gestão.* Cadernos da Fucamp, v. 27, p.31-52, 2024. https://revistas.fucamp.edu.br/index.php/cadernos/article/view/3405/2128

Couldry, M. & Mejias, U. A. (2019) *The costs of connection: how data is colonizing human life and appropriating it for capitalism*. Stanford: Stanford University Press. https://www.jstor.org/stable/26931941

Dantas, D. & Dodt, C. (2025). *Ciclo de vida dos dados pessoais de acordo com a LGPD*. Exame, 2025. https://exame.com/bussola/ciclo-de-vida-dos-dados-pessoais-de-acordo-com-a-lgpd/

Doneda, D. (2021). *Da privacidade à proteção de dados Pessoais.* (3ª ed.). Thomson Reuters Brasil.

Freitas, C. O. de A. (2022). *Riscos e proteção de dados pessoais*. Revista Rede de Direito Digital, Intelectual & Sociedade, Curitiba, v.2, n.4, p. 225-247, 2022. https://revistas.ufpr.br/rrddis/article/download/93531/50795

Gil, A. C. (2019). *Métodos e técnicas de pesquisa social.* 7ª edição. São Paulo: Atlas.

Gonçalves, E., Silva, I. R. B. da, Zottmann, C. E. M., Souza Neto, J., & Nunes, R. R. (2025). *Universidades sob ataque hacker: riscos de negócio para segurança cibernética em universidades brasileiras.* UNB. http://ppee.unb.br/wp-content/uploads/2025/04/Artigo_ataque_hacker_IES_UnB.pdf

Khalil, M., Shakya, R., & Liu, Q. (2025). *Towards privacy-preserving data-driven education: the potential of federated learning. Cornell University arXiv preprint*, 2503.13550. https://doi.org/10.48550/arXiv.2503.13550

Kruse, C. S., Smith, B., Vanderlinder, H. (2017). *Security techniques for the eletronic health records.* https://doi.org/10.1007/s10916-017-0778-4

Lyon, D. (2001). *Surveillance society: monitoring everyday life.* Buckingham: Open University Press.

Nascimento, E. A. do; Dantas, Ahirton, J. F., Sousa, R. L. de; Elias, V. F., Menezes, T. L. P., Costa, M. do N. da; Silva, Denise, B. da., & Nascimento, T. do. (2024). *Educação digital: riscos e desafios nas instituições escolares.* Revista Tópicos. https://doi.org/10.5281/zenodo.11516675

National Institute of Standards and Technology (NIST). (2020). *Privacy framework: a tool for improving privacy through enterprise risk management*. Versão atualizada. Gaithersburg: NIST, 2020. https://doi.org/10.6028/NIST.CSWP.01162020

Nissenbaum, H. (2009) *Privacy in context: technology, policy, and the integrity of social life.* Stanford: Stanford University Press.

Noble, S. U. (2018). *Algorithms of oppression: how search engines reinforce racism.* New York: New York University Press.

Organisation for Economic Co-operation and Development. (2026). *OECD Digital Education Outlook 2026: exploring Effective Uses of Generative AI in Education.* Paris: OECD, 2026.https://www.oecd.org/en/publications/oecd-digital-education-outlook-2026_062a7394-en.html

Reis, S. R. F. (2024). *Desafios da LGPD quanto à privacidade em ambientes educacionais: um mapeamento sistemático.* Revista de Gestão e Secretariado, v. 15, n. 3, e 3292. https://ojs.revistagesec.org.br/secretariado/article/view/3292

Saunders, M., Lewis, P., Thornhill, A. (2018). *Research methods for business students*. 7. ed. Harlow: Pearson, cap. 7, p. 200-240.

Selwyn, N. (2020). *Re-imagining 'learning analytics'…: a critical proposal for ensuring higher education students are not 'educated by data'.* British Journal of Educational Technology, v. 51, n. 3, p. 520-538, 2020. https://www.sciencedirect.com/science/article/abs/pii/S109675162030021X

Souza, L. L. de, Santos, G. J. F., Oliveira, J. G. de; Silva, M. V. A. da; Vasco, S. C. S., & Vieira, V. E. L. (2025). *Vazamento de dados em ambiente escolar.* Revista Brasileira de Estudos Jurídicos, v. 19, n.3. Edição Especial - Enade: itinerários formativos e avaliação no ensino superior, 2025.https://portalunifipmoc.emnuvens.com.br/rbej/article/view/274

Steve E. (2025). *Cyber threats facing the education sector in 2025*. https://www.bitsight.com/blog/top-10-cyber-threats-facing-education-sector

Tomaz, L. B. P., Nunes, R. R., Silva, I. R. B. da. (2025). *Rede federal em alerta: riscos de negócio para segurança cibernética na educação profissional, científica e tecnológica.* https://ppee.unb.br/wp-content/uploads/2025/09/Artigo-2-2.pdf

UNESCO. (2022). Minding the data: protecting learners' privacy and security. Unesco, 2022. https://doi.org/10.54675/NNAA4843

UNICEF. (2021) *The state of the World's Children 2021: on my mind – promoting, protecting and caring for children's mental health.* Nova Iorque: UNICEF. https://www.unicef.org/reports/state-worlds-children-2021

Zottmann, C. E. M., Georg, M. A. C., Alves, R. S., Silva, M. A., & Nunes, R. R. (2023). *Proposta de metodologia para avaliação de riscos de privacidade para órgãos do poder judiciário no Brasil.* ENAJUS. Encontro de Administração da Justiça, Brasília-DF, 2023. https://enajus.org.br/anais/assets/papers/2023/sessao-7/proposta-de-metodologia-para-avaliacao-de-riscos-de-privacidade-para-orgaos-do-poder-judiciario-no-brasil.pdf

Zuboff, S. (2019). *The age of surveillance capitalism: the fight for a human future at the new frontier of power.* New York: PublicAffairs.

APÊNDICE A

Matriz de controles integrados para governança da privacidade para a IFE

Nº	Controle	Percepções dos entrevistados	Grau de Prioridade
		Dimensão Técnico-Operacional	
		Controles Preventivos	
1	Princípios de privacidade desde a concepção (*Privacy by Design*) nos processos e sistemas.	- Controle necessário: implementar política de *Privacy by Default*: reconfigurar sistemas de informação e plataformas educacionais (ex: Moodle) para coletar apenas dados estritamente necessários, desativando rastreamento comportamental desproporcional por padrão. - Controle existente (parcial): uso de autenticação de usuários. - Controle PPSI recomendado: 16 - Segurança de Aplicações.	Alto
2	Gestão de Identidade e Acesso (IAM).	- Controle necessário: implementar o *principle of least privilege* com revisão periódica (semestral) de permissões. Criar perfis de acesso mínimos por função. - Controle existente: estrutura hierárquica básica no sistema acadêmico. - Controle PPSI recomendado: 6 - Gestão de Acesso	Alto
3	Auditorias periódicas de processos e formulários de coleta de dados.	- Controle necessário: criar checklist de verificação de processos e formulários. - Controle existente: - - Controle PPSI recomendado:-	Alto
4	Auditorias regulares de controles de segurança da informação com base nos riscos mapeados.	- Controle necessário: implantar sistemas de *logging* e SIEM (*Security Information and Event Management*) para detecção de acessos anômalos em tempo real. - Controle existente (parcial): logs de acesso básicos. - Controle PPSI recomendado: 8 - Gestão de registros de auditoria.	Alto
		Controles Mitigatórios	
5	Sistemas integrados e seguros.	- Controle necessário: implantar integração contínua. - Controle existente (parcial): autenticação de usuários. - Controle PPSI recomendado: 16 - Segurança de Aplicações.	Alto
6	Controles de segurança da informação (criptografia, MFA, RBAC, backups criptografados).	- Controle necessário: criptografia de ponta a ponta para dados sensíveis em trânsito e em repouso (especialmente em nuvem). - Controle existente (Baixa Maturidade): *backup* de dados. - Controle PPSI recomendado: 3 - Proteção de Dados.	Alto
		Dimensão Organizacional-Governamental	
		Controles preventivos	
7	Estrutura de governança integrada.	- Controle necessário: criar um Comitê Institucional de Privacidade com autoridade decisória, reunindo TI, jurídico, Encarregada de Tratamento de Dados Pessoais, acadêmico e administrativo. - Controle existente (fracasso): Decisões fragmentadas em 7 setores. - Controle PPSI recomendado: 0 - Estrutura básica de governança.	Alto
8	Políticas, normas, processos, termos e	- Controle necessário: desdobrar a Política de Privacidade em Manuais e POPs específicos (ex: "POP para Coleta em Avaliações Online").	Alto

	procedimentos operacionais	- Controles existentes: Política formal de segurança da informação, proteção de dados e privacidade. - Controle PPSI recomendado: 10 - Registro de Operações de Tratamento de Dados Pessoais. - Controle recomendados não existentes na IFE e no PPSI. - Política de minimização/pseudonimização de dados pessoais. - Política de gestão de dados com critérios de classificação e prazos de retenção e descarte de dados. - Política de monitoramento digital.	
9	Plano de resposta a incidentes de privacidade.	- Controle necessário: procedimento automatizado para isolamento de sistemas, revogação emergencial de acessos. - Controle existente (parcial): procedimento de resposta a incidentes - Controle PPSI recomendado: 17 - Gestão de Incidentes	Alto
10	Gestão de riscos e conformidade proativa.	- Controle necessário: implementar processo obrigatório de avaliação de impacto à proteção de dados (RIPD) para todas as novas operações de tratamento e sistemas. - Controle existente (crítico): ausência de RIPD em grande parte das operações de alto risco. - Controle PPSI recomendado: 0 - Estrutura básica de Governança (Processos de Gestão de Riscos de Segurança da Informação, e Gestão de Riscos relacionados a Operações de Tratamento de Dados Pessoais.	Alto
11	Programa de capacitação contínua e personalizada.	- Controle necessário: programa de treinamento regular e obrigatório e segmentado (conteúdo específico para professores, técnicos, gestores). - Controle existente (insuficiente): treinamento esporádico para poucos servidores - Controle PPSI recomendado: 14 - Conscientização e Treinamento de Competências.	Alto
		Controles mitigatórios	**Grau de Prioridade**
12	Minimização de coleta e retenção de dados.	- Controle necessário: definição de regras específicas para minimização da coleta e retenção de dados. - Controle existente (não existente): -. - Controle PPSI recomendado:-.	Alto
		Dimensão Contratual-Relacional	
		Controles preventivos	**Grau de Prioridade**
13	Cláusulas contratuais específicas sobre privacidade.	- Controle necessário: desenvolver e adotar cláusulas-padrão setoriais para licitações de tecnologia educacional, incluindo: finalidade limitada, proibição de uso secundário, direito de auditoria independente, obrigação de descarte seguro certificado. - Controle existente (frágil): cláusula genérica da LGPD. - Controle PPSI recomendado: 11 - Contratos, acordos e instrumentos congêneres.	Alto
14	Cláusulas contratuais de indenização e responsabilidade.	- Controle necessário: desenvolver e adotar cláusulas-padrão setoriais para licitações de tecnologia educacional, incluindo: finalidade limitada, proibição de uso secundário, direito de auditoria independente, obrigação de descarte seguro certificado. - Controle existente (frágil): cláusula genérica da LGPD. - Controle PPSI recomendado: 11 - Contratos, acordos e instrumentos congêneres.	Alto
15	*Due Diligence* e monitoramento de terceiros.	- Controle necessário: realizar auditorias periódicas ou exigir certificações (ex: ISO 27701) dos provedores de serviços. - Controle existente (insuficiente): análise jurídica superficial de contratos. - Controle PPSI recomendado: 16 - Gestão de provedor de serviços	Alto

16	Mapa de fluxos de dados.	- Controle necessário: manter inventário atualizado de todos os compartilhamentos de dados, incluindo finalidade, base legal e medidas de segurança do receptor. - Controle existente: -. - Controle PPSI recomendado: 19 - Registro de operações de tratamento de dados pessoais	Alto
		Controles mitigatórios	**Grau de Prioridade**
17	Cláusulas contratuais de indenização e responsabilidade.	- Controle necessário: garantir que contratos prevejam reparação por danos causados por violações do operador. - Controle existente: -. - Controle PPSI recomendado 11 - Contratos, acordos e instrumentos congêneres	Alto
18	Plano de transição de fornecedores.	- Controle necessário: garantir a portabilidade ou exclusão segura dos dados ao encerrar contratos. - Controle existente: -. - Controles PPSI recomendados: 11 - Contratos, acordos e instrumentos congêneres, 16 - Gestão de provedor de serviços.	Médio
		Dimensão Humana-Cultural	
		Controles Preventivos	**Grau de Prioridade**
19	Transparência ativa e comunicação clara.	- Controle necessário: criar um Portal da Transparência da Privacidade com linguagem acessível, explicando quais dados são coletados, por quê, e como exercer direitos. - Controle existente (ineficaz): comunicação insuficiente; Grande parte dos estudantes desconhecem os dados coletados. - Controle PPSI recomendado: 0 - Controle 21: Encarregado e Direitos de Titulares	Alto
20	Fortalecimento da cultura de privacidade.	- Controle necessário: campanhas internas contínuas, com ênfase na proteção de grupos vulneráveis (crianças/adolescentes). Incluir a privacidade como valor na missão institucional. - Controle existente (incipiente): conscientização inicial pontual. - Controle PPSI recomendado: 14 - Conscientização e Treinamento de Competências	Alto
21	Mecanismos de participação e ouvidoria.	- Controle necessário: estabelecer fóruns de consulta à comunidade acadêmica sobre novas tecnologias que envolvam tratamento de dados. - Controle existente: canais formais de ouvidoria (pouco utilizados para privacidade). - Controle PPSI recomendado: 21 - Encarregado e Direitos de Titulares	Alto
		Controles mitigatórios	**Grau de Prioridade**
22	Procedimentos para comunicação de incidentes envolvendo titulares de dados pessoais.	- Controle necessário: confidencial e seguro para reportar preocupações ou violações, com garantia de não-retaliação. - Controle existente: plataforma Fala.BR - Controle PPSI recomendado: 21 - Encarregado e Direitos de Titulares	Alto