RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 20/06/2026 | aceito: 23/06/2026 | publicação: 26/06/2026

Governança de Privacidade e Segurança da Informação no Ecossistema Escolar: Um Plano de Ação Estruturado sob a Ótica da LGPD e do Novo ECA Digital

Privacy Governance and Information Security in the School Ecosystem: A Structured Action Plan from the Perspective of the LGPD and the New Digital ECA

Gobernanza de la Privacidad y Seguridad de la Información en el Ecosistema Escolar: Un Plan de Acción Estructurado desde la Perspectiva de la LGPD y del Nuevo ECA Digital

David Fernando da Silva Marcelino – davifernando_10@hotmail.com
José Marcellus Nascimento de Assis – marcellus.assis@yahoo.com.br

Resumo:
A aceleração da transformação digital nas instituições de ensino expandiu a coleta de dados pessoais sensíveis de crianças e adolescentes, gerando um gap crítico entre a evolução da infraestrutura funcional de TIC e a maturidade organizacional em governança de privacidade. Este artigo propõe um plano de ação estruturado para mitigar vulnerabilidades cibernéticas e alinhar as unidades escolares às exigências da Lei Geral de Proteção de Dados (LGPD) e do recém-implementado Estatuto Digital da Criança e do Adolescente (Lei nº 15.211/2025). Por meio de uma abordagem qualitativa e exploratória baseada em Estudo de Caso, combinada com pesquisa bibliográfica e documental, identificaram-se os principais gargalos no ciclo de vida dos dados escolares, como o uso de canais informais de comunicação e a fragilidade de endpoints administrativos. Como contribuição prática, apresenta-se um framework de intervenção dividido em seis fases lógicas e consecutivas — abrangendo desde o diagnóstico situacional até o monitoramento contínuo —, além de evidenciar o papel estratégico do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) como salvaguarda jurídica e institucional perante os órgãos de fiscalização.

Palavras-chave:
Segurança da Informação. Lei Geral de Proteção de Dados (LGPD). Estatuto Digital (Lei nº 15.211/2025). Gestão de Endpoints. Unidades Escolares.

Abstract:
The acceleration of digital transformation in educational institutions has expanded the collection of sensitive personal data from children and adolescents, generating a critical gap between the evolution of functional ICT infrastructure and organizational maturity in privacy governance. This article proposes a structured action plan to mitigate cyber vulnerabilities and align school units with the requirements of the General Data Protection Law (LGPD) and the newly implemented Digital Child and Adolescent Statute (Law No. 15,211/2025). Through a qualitative and exploratory approach based on a Case Study, combined with bibliographical and documentary research, the main bottlenecks in the data life cycle within schools were identified, such as the use of informal communication channels and the fragility of administrative endpoints. As a practical contribution, an intervention framework divided into six logical and consecutive phases is presented — ranging from situational diagnosis to continuous monitoring —, while also highlighting the strategic role of the Personal Data Protection Impact Assessment (PDPIA) as a legal and institutional safeguard before supervisory bodies.

Keywords:
Information Security. General Data Protection Law (LGPD). Digital Statute (Law No. 15,211/2025). Endpoint Management. School Units.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 20/06/2026 | aceito: 23/06/2026 | publicação: 26/06/2026

Resumen:
La aceleración de la transformación digital en las instituciones educativas ha ampliado la recopilación de datos personales sensibles de niños y adolescentes, generando una brecha crítica entre la evolución de la infraestructura funcional de las TIC y la madurez organizacional en materia de gobernanza de la privacidad. Este artículo propone un plan de acción estructurado para mitigar las vulnerabilidades cibernéticas y alinear las unidades escolares con los requisitos de la Ley General de Protección de Datos (LGPD) y del recientemente implementado Estatuto Digital del Niño y del Adolescente (Ley n.º 15.211/2025). Mediante un enfoque cualitativo y exploratorio basado en un estudio de caso, combinado con investigación bibliográfica y documental, se identificaron los principales cuellos de botella en el ciclo de vida de los datos escolares, como el uso de canales informales de comunicación y la fragilidad de los endpoints administrativos. Como contribución práctica, se presenta un marco de intervención dividido en seis fases lógicas y consecutivas —desde el diagnóstico situacional hasta el monitoreo continuo—, además de destacar el papel estratégico del Informe de Impacto sobre la Protección de Datos Personales (RIPD) como salvaguarda jurídica e institucional ante los organismos de fiscalización.

Palabras clave:
Seguridad de la Información. Ley General de Protección de Datos (LGPD). Estatuto Digital (Ley n.º 15.211/2025). Gestión de Endpoints. Unidades Escolares.

Introdução

A aceleração do processo de transformação digital no cenário contemporâneo reconfigurou profundamente as dinâmicas operacionais, administrativas e pedagógicas das instituições de ensino. Unidades escolares, tanto no ecossistema público quanto no privado, migraram progressivamente suas rotinas para plataformas digitais de aprendizagem, sistemas de monitoramento em nuvem, diários de classe eletrônicos e portais de matrícula unificados. Se, por um lado, essa modernização tecnológica otimizou a gestão acadêmica e expandiu os horizontes pedagógicos, por outro, expandiu exponencialmente a superfície de ataque dessas instituições, resultando em uma coleta massiva e contínua de dados pessoais sensíveis pertencentes a um público hipervulnerável: crianças e adolescentes.

Dentro desse panorama, a entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD) — Lei nº 13.709/2018 — impôs um severo paradigma de conformidade ao mercado brasileiro, estabelecendo em seu Artigo 14 diretrizes rigorosas e específicas para o tratamento de dados de menores de idade, exigindo a observância do princípio do melhor interesse do menor e o consentimento explícito e destacado de seus responsáveis legais. Ocorre que, embora a infraestrutura de Tecnologia da Informação e Comunicação (TIC) nas escolas tenha avançado para viabilizar as atividades funcionais do ensino, a maturidade organizacional voltada à segurança da informação e à governança de privacidade não acompanhou a mesma velocidade

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 20/06/2026 | aceito: 23/06/2026 | publicação: 26/06/2026

de evolução. O cenário tornou-se ainda mais exigente com a recente promulgação da Lei nº 15.211/2025, o Estatuto Digital da Criança e do Adolescente, que tipificou e endureceu as regras para a exposição e o perfilamento informacional de menores em ambientes virtuais.

Dessa forma, observa-se na realidade prática das unidades escolares um cenário de vulnerabilidade estrutural de ativos e fluxos informacionais. É comum constatar a ausência de inventários de dados formais, armazenamento de cadastros estudantis e financeiros em computadores administrativos locais carentes de criptografia e o compartilhamento indiscriminado de informações de alta sensibilidade — como fichas médicas, registros de alergias e relatórios psicopedagógicos — por meio de canais de comunicação informais e aplicativos de mensagens instantâneas. Diante de fragilidades em perímetros de rede e de lacunas no treinamento de usuários contra vetores de engenharia social, o ecossistema educacional torna-se um alvo crítico para incidentes de segurança, vazamentos cibernéticos e sanções administrativas severas aplicadas pelos órgãos fiscalizadores competentes.

Diante desse contexto de risco, emerge o seguinte problema de pesquisa: Como mitigar as vulnerabilidades cibernéticas e de privacidade e estruturar de forma eficaz a governança de dados pessoais sensíveis em ambientes escolares de acordo com as exigências técnicas da LGPD e do Novo ECA Digital?

Justifica-se este estudo pela necessidade latente de preencher a lacuna metodológica existente entre as obrigações estritamente jurídicas da legislação de privacidade e a operação técnica real das equipes de suporte e infraestrutura de TI nas escolas. O objetivo geral deste artigo é propor e detalhar um plano de ação estruturado em fases lógicas e consecutivas para o gerenciamento do ciclo de vida dos dados escolares, promovendo a transição de um modelo puramente reativo de segurança para uma postura preventiva, resiliente e em estrita conformidade legal.

2 Marco Teórico / Resultados

2.1 A Proteção de Dados de Menores e o Impacto Regulatório da Lei nº 15.211/2025

A promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) inaugurou uma nova era de responsabilidade civil e governança da informação no território brasileiro. No âmbito das instituições de ensino, o impacto regulatório assume proporções ainda mais complexas devido à natureza do público atendido. O Artigo 14 da referida lei determina categoricamente que o tratamento de dados pessoais de crianças e adolescentes deve ser realizado em seu melhor

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 20/06/2026 | aceito: 23/06/2026 | publicação: 26/06/2026

interesse, conforme a legislação pertinente e os princípios gerais de proteção de dados (BRASIL, 2018).

O ordenamento jurídico brasileiro conferiu um status de "hipervulnerabilidade" aos menores de idade no ambiente digital. Isso se traduz na exigência de salvaguardas rigorosas: para além das bases legais convencionais, o tratamento de dados de crianças exige o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. No ambiente escolar, este preceito impacta diretamente os sistemas de matrícula, prontuários de acompanhamento pedagógico e até registros automatizados de frequência (MENDES; DONEDA, 2020, p. 52).

Essa tutela especial aos direitos da personalidade dos menores de idade encontrou um novo patamar de rigidez e especificidade com a entrada em vigor da Lei nº 15.211/2025, conhecida como o Estatuto Digital da Criança e do Adolescente (ECA Digital). Esta legislação estende formalmente o princípio constitucional da prioridade absoluta e da proteção integral para o ambiente virtual, impondo obrigações severas a produtos, aplicações e serviços de tecnologia que sejam direcionados ou que possuam probabilidade de acesso por esse público hipervulnerável (BRASIL, 2025).

Sob a égide da Lei nº 15.211/2025, o ecossistema digital das unidades escolares passa a ser fortemente impactado. O diploma legal veda taxativamente práticas de perfilamento de dados de menores para fins publicitários ou comerciais dentro de softwares educacionais. A nova lei estabelece que as plataformas e sistemas operacionais adotados configurem, por padrão (*privacy by default*), os modelos mais protetivos disponíveis em relação à privacidade, exigindo mecanismos auditáveis e confiáveis de controle e validação de acessos.

No cotidiano escolar, as categorias de dados manipuladas extrapolam o escopo meramente cadastral. Conforme o Guia Prático para o Setor de Educação da ANPD (2023), as instituições gerenciam rotineiramente relatórios psicopedagógicos, fichas médicas e laudos de restrições de saúde, configurados como dados pessoais sensíveis de acordo com o Artigo 5º, inciso II da LGPD. A falta de governança sobre essas informações, além de violar os princípios de necessidade e finalidade da lei geral, passa a sofrer o crivo punitivo do ECA Digital. As sanções previstas pela Lei nº 15.211/2025 incluem advertências institucionais e multas severas calculadas com base no faturamento ou por volume de usuários cadastrados expostos ao risco cibernético (BRASIL, 2025).

2.2 O Ciclo de Vida dos Dados e a Vulnerabilidade de Endpoints em TIC

Para além da conformidade jurídica, a segurança da informação exige o domínio técnico sobre o ciclo de vida dos dados, compreendendo as fases de coleta, processamento, compartilhamento, armazenamento e descarte seguro. Pinheiro (2021) adverte que a maior parte dos incidentes de vazamento de dados nas organizações não decorre de ataques externos altamente sofisticados, mas sim da ausência de processos claros de governança interna e mapeamento de fluxos informacionais.

Nas unidades escolares, o fluxo de dados frequentemente carece de rastreabilidade. Dados coletados no ato da matrícula são replicáveis em planilhas locais, compartilhados com o corpo docente e armazenados em computadores administrativos que funcionam como endpoints vulneráveis. De acordo com Nakamura e Geus (2017), um endpoint (estação de trabalho, notebook ou dispositivo conectado) sem a devida blindagem lógica atua como a principal porta de entrada para ameaças cibernéticas em ambientes corporativos. A falta de segmentação de redes nas escolas — permitindo que a rede Wi-Fi usada por alunos e visitantes acesse o mesmo servidor que armazena o banco de dados da secretaria — eleva drasticamente o risco de intrusões.

Soma-se a esse cenário técnico o "fator humano" como elemento de vulnerabilidade. Crespo (2022) destaca que a engenharia social, por meio de táticas de phishing ou indução ao erro, explora diretamente a falta de treinamento de usuários para obter credenciais de acesso de forma ilegítima. No cotidiano escolar, o hábito de compartilhar listas de turmas ou notas via aplicativos de mensagens instantâneas sem criptografia homologada (como grupos informais de WhatsApp corporativo ou pessoal) subverte qualquer controle perimetral de TI, pulverizando dados protegidos em infraestruturas de terceiros sem qualquer governança institucional.

2. Material e Método

Para a consecução dos objetivos delineados neste estudo, adotou-se uma abordagem metodológica de natureza qualitativa e caráter exploratório. Segundo Minayo (2014), a pesquisa qualitativa trabalha com o universo de significados, motivos, aspirações, crenças, valores e atitudes, o que corresponde a um espaço mais profundo das relações, dos processos e dos fenômenos que não podem ser reduzidos à operacionalização de variáveis quantitativas brutas. A escolha do caráter exploratório justifica-se pela necessidade de prover maior familiaridade

com o problema proposto, permitindo a convergência entre as exigências abstratas da legislação de privacidade e a realidade prática da infraestrutura de TI.

O procedimento técnico configurou-se como um Estudo de Caso, associado à pesquisa bibliográfica e documental. Conforme preconiza Yin (2015), o estudo de caso se apresenta como uma estratégia de investigação recomendada quando se busca compreender fenômenos contemporâneos inseridos em seu contexto real, especialmente quando as fronteiras entre o fenômeno e o contexto não estão claramente evidentes. O objeto de análise deste estudo consistiu nas rotinas operacionais, pedagógicas e administrativas de unidades escolares, mapeando seus fluxos informacionais latentes.

A coleta de dados documentais e bibliográficos sustentou-se no levantamento da legislação nacional vigente — com ênfase na Lei nº 13.709/2018 (LGPD) e na Lei nº 15.211/2025 (ECA Digital) —, em resoluções e guias práticos publicados pela Autoridade Nacional de Proteção de Dados (ANPD), bem como em frameworks e normas internacionais de segurança da informação, notadamente a ABNT NBR ISO/IEC 27001 e 27002. A análise dos dados foi realizada por meio da técnica de análise de conteúdo, permitindo identificar as principais vulnerabilidades estruturais dos ativos de TIC escolares e, a partir delas, conceber e estruturar um framework metodológico de intervenção preventiva e resiliente dividido em fases lógicas e replicáveis.

3. Resultados e Discussão

3.1 Diagnóstico Situacional e Problematização do Fluxo Informacional Escolar

A análise das rotinas operacionais e administrativas das unidades escolares evidenciou um ecossistema informacional caracterizado por alta fragmentação e vulnerabilidade difusa. O mapeamento do fluxo de dados revelou que o ciclo de vida das informações pessoais — desde a coleta inicial no ato da matrícula até o arquivamento definitivo ou expurgo — carece de rastreabilidade e de controles perimetrais de segurança da informação.

A primeira grande fragilidade identificada reside no armazenamento descentralizado e desprotegido de dados sensíveis em endpoints administrativos. Computadores alocados em secretarias e direções de unidades operam frequentemente sem segregação lógica de perfis, permitindo que usuários com diferentes atribuições funcionais acessem indiscriminadamente bancos de dados cadastrais, registros financeiros e históricos de saúde dos discentes. A ausência de criptografia em repouso nesses ativos e a falta de restrições a mídias removíveis (como

dispositivos USB) configuram vetores críticos para a exfiltração não autorizada de informações ou infecção por códigos maliciosos.

Paralelamente, a dimensão pedagógica revelou-se um gargalo operacional no que tange à privacidade. Diante da ausência de canais institucionais homologados e de políticas de uso claro, constatou-se a disseminação do uso de aplicativos de mensagens instantâneas e redes sociais privadas para o compartilhamento de relatórios psicopedagógicos, termos de ocorrência disciplinar e fichas de restrições médicas. Esse fluxo informal pulveriza dados sensíveis de menores de idade em servidores de terceiros, burlando os mecanismos de controle da área de TIC e contrariando frontalmente os princípios de segurança, finalidade e necessidade preconizados pela LGPD.

3.2 Framework de Intervenção: As Seis Fases da Governança de Privacidade na Escola

Como resposta técnica e estruturada aos gargalos dos diagnosticados, propõe-se um framework de governança e adequação dividido em seis fases lógicas, consecutivas e complementares, desenhado para elevar a maturidade organizacional da instituição e responder às exigências da LGPD e do ECA Digital (Lei nº 15.211/2025):

- **Fase 1 - Diagnóstico e Inventário de Dados:** Consiste no levantamento exaustivo e mapeamento de todos os ativos informacionais da escola, englobando arquivos físicos (pastas de arquivos mortos) e digitais (planilhas locais, sistemas legados). O objetivo é catalogar a natureza dos dados tratados, identificando os operadores e as bases legais que sustentam cada operação.
- **Fase 2 - Segregação de Acessos e Privilégio Mínimo:** Implementação de matrizes de controle de acesso baseadas em funções (*Role-Based Access Control - RBAC*). Sob essa ótica, o corpo docente e o corpo administrativo passam a ter visibilidade restrita apenas aos dados estritamente necessários ao cumprimento de suas funções pedagógicas ou operacionais. Essa matriz atende diretamente à exigência de configuração padrão protetiva (*privacy by default*) do ECA Digital, impedindo acessos universais ou indiscriminados a históricos sensíveis.
- **Fase 3 - Blindagem de Endpoints e Ativos de Rede:** Aplicação de controles rígidos de segurança lógica nas estações de trabalho. Esta fase compreende a instalação compulsória de soluções de antivírus e firewall corporativos, atualização automatizada

de patches de sistemas operacionais, criptografia de disco e o bloqueio físico ou lógico de portas USB para mitigar o risco de vazamentos e introdução de malwares.

- **Fase 4 - Homologação de Canais e Comunicação Segura:** Migração e centralização do fluxo de troca de informações para um ambiente de nuvem corporativa criptografada e oficialmente homologada pela instituição. Proíbe-se o uso de ferramentas de mensageria pessoal para fins profissionais, respondendo à determinação legal da Lei nº 15.211/2025, que obriga as instituições a monitorar e mitigar o tráfego de informações estudantis em ambientes desprovidos de mecanismos de supervisão e auditoria.
- **Fase 5 - Gestão de Descarte e Retenção:** Instituição de uma tabela de temporalidade documental e protocolos técnicos de descarte seguro. Dados de alunos que romperam o vínculo institucional devem ser eliminados ou anonimizados assim que expirado o prazo legal de retenção exigido pelo Ministério da Educação, evitando o acúmulo desnecessário de passivos de risco cibernético.
- **Fase 6 - Monitoramento, Cultura e Auditoria Contínua:** Estabelecimento de rotinas de auditoria por meio de checklists semanais de conformidade técnica e operacional. Adicionalmente, esta fase engloba a capacitação continuada do corpo docente e administrativo por meio de programas de conscientização contra vetores de engenharia social. O monitoramento contínuo garante que softwares contratados pela rede cumpram a proibição de perfilamento ou captação de dados abusiva dentro da sala de aula.

3.3 O Papel Estratégico do RIPD na Salvaguarda Institucional

A consolidação do framework de governança proposto culmina na elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), conforme recomendação da Autoridade Nacional de Proteção de Dados (ANPD). O RIPD funciona como uma peça de documentação técnica e jurídica viva, contendo a descrição detalhada dos processos de tratamento de dados que podem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares (os menores de idade e seus responsáveis).

Ao documentar os riscos inerentes à operação escolar e, sobretudo, ao apontar as medidas, salvaguardas e mecanismos de mitigação adotados ao longo das seis fases de intervenção, o RIPD confere à instituição de ensino uma sólida blindagem jurídica. Em cenários de fiscalização ativa ou incidentes fortuitos, a existência de um relatório de impacto estruturado e auditável atua como evidência cabal de governança, boa-fé e diligência técnica, minimizando

a aplicação das severas sanções administrativas da LGPD e do ECA Digital, demonstrando maturidade em segurança da informação perante a sociedade (ANPD, 2023).

Considerações Finais

A investigação conduzida ao longo deste estudo permitiu responder de forma estruturada ao problema de pesquisa proposto, demonstrando que a mitigação de vulnerabilidades cibernéticas e a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e com o Novo ECA Digital (Lei nº 15.211/2025) no ecossistema escolar dependem, fundamentalmente, da superação de um modelo de TI puramente reativo. A transição para uma postura preventiva e resiliente exige a implementação de uma governança de privacidade robusta, capaz de integrar a segurança da informação de infraestrutura lógica às rotinas operacionais, pedagógicas e administrativas diárias das unidades de ensino.

O objetivo geral deste artigo foi plenamente alcançado por meio da concepção e detalhamento do framework de intervenção dividido em seis fases consecutivas. Evidenciou-se que ações isoladas de tecnologia são insuficientes se não forem acompanhadas por um mapeamento sistemático do ciclo de vida dos dados, pela aplicação rigorosa do princípio do privilégio mínimo no controle de acessos corporativos e pela blindagem efetiva de endpoints administrativos nas secretarias escolares. Ademais, constatou-se que o fator humano desempenha um papel crítico na sustentação dessa engrenagem de segurança, tornando os programas contínuos de conscientização contra vetores de engenharia social um pilar indispensável para a construção de uma cultura organizacional de privacidade.

Sob a perspectiva jurídica e institucional, o estudo demonstrou a centralidade estratégica do Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Longe de configurar apenas uma obrigação burocrática, o RIPD consolida-se como um instrumento de governança viva e de salvaguarda institucional, servindo como evidência material de boa-fé, diligência e conformidade técnica perante os órgãos de fiscalização regulatória, como a Autoridade Nacional de Proteção de Dados (ANPD).

Como limitação deste trabalho, reconhece-se o seu caráter eminentemente conceitual e propositivo, estruturado a partir de um estudo de caso analítico baseado em revisão documental e bibliográfica. Para pesquisas e desdobramentos futuros, recomenda-se a aplicação empírica do framework das seis fases proposto em uma unidade ou rede municipal de ensino real. Tal implementação prática viabilizará a coleta de indicadores quantitativos de eficiência cibernética, a mensuração do nível de maturidade organizacional pós-intervenção e o

refinamento das metodologias de proteção de dados sensíveis voltadas à garantia do melhor interesse de crianças e adolescentes na era digital.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). ABNT NBR ISO/IEC 27002: Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Prático para Agentes de Tratamento de Dados no Setor de Educação. Brasília, DF: ANPD, 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

BRASIL. Lei nº 15.211, de 17 de setembro de 2025. Institui o Estatuto Digital da Criança e do Adolescente (ECA Digital) e dispõe sobre a proteção de crianças e adolescentes no ambiente digital. Brasília, DF: Presidência da República, 2025.

COSTA, Maria Adélia da. Políticas de Formação Docente para Educação Profissional: realidade ou utopia? Curitiba: Appris, 2016.

CRESPO, Marcelo Xavier. Cibersegurança e o fator humano: riscos e governança. Revista Brasileira de Direito Digital, v. 4, n. 2, p. 89-104, 2022.

DE CARVALHO, R. L.; CABRAL, R. G.; ROSARIO FERRER, Y. SISTEMAS TUTORES INTELIGENTES COMO RECURSO DIDÁTICO NO ENSINO DA MATEMÁTICA. HOLOS, [S. l.], v. 6, p. 1–11, 2019. DOI: 10.15628/holos.2019.7028. Disponível em: https://www2.ifrn.edu.br/ojs/index.php/HOLOS/article/view/7028. Acesso em: 04 jun. 2023.

MENDES, Laura Schertel; DONEDA, Danilo. A proteção de dados pessoais de crianças e adolescentes na LGPD. Revista de Direito do Consumidor, v. 128, p. 45-67, 2020.

MINAYO, Maria Cecília de Souza (org.). Pesquisa Social: teoria, método e criatividade. 34. ed. Petrópolis: Vozes, 2014.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. Segurança de Redes em Ambientes Corporativos. São Paulo: Novatec, 2017.

PINHEIRO, Patricia Peck. Direito Digital. 7. ed. São Paulo: Saraiva Educação, 2021.

ROSATELLI, M. C., & Self, J. A. Supporting distance learning from case studies. In S. P Lajoie, & M. Vivet (Eds.), Proceedings of 9th international conference on artificial intelligence in education, p. 457-564, abril. 2000.

YIN, Robert K. Estudo de Caso: planejamento e métodos. 5. ed. Porto Alegre: Bookman, 2015.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 20/06/2026 | aceito: 23/06/2026 | publicação: 26/06/2026

AGRADECIMENTOS

Agradeço primeiramente a Deus, pela força, sabedoria e discernimento concedidos ao longo de toda esta jornada acadêmica. À minha mãe, pelo apoio incondicional, amor exemplar e paciência nos momentos de ausência dedicados aos estudos. Aos professores e tutores do curso de MBA em Segurança da Informação, pela orientação precisa e compartilhamento de conhecimentos que tornaram possível o desenvolvimento técnico deste trabalho. Aos professores da área da educação que atuam na ponta do ecossistema escolar, pois, sem eles e sem a sua resiliência diária, não haveria a própria construção do conhecimento, a transformação digital nas salas de aula e, tampouco, a necessidade latente de protegermos a integridade e o futuro de nossos estudantes. Por fim, a todos os colegas e profissionais da área de Tecnologia da Informação que, de forma direta ou indireta, contribuíram para o amadurecimento dos conceitos e reflexões apresentados neste artigo.