RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 06/20/2026 | Accepted: 06/23/2026 | Publication: 06/26/2026

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

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

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

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.

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.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 06/20/2026 | Accepted: 06/23/2026 | Publication: 06/26/2026

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.

Introduction

The acceleration of the digital transformation process in the contemporary scenario has profoundly reconfigured the operational, administrative, and pedagogical dynamics of educational institutions. School units, both in the public and private ecosystems, have progressively migrated their routines to digital learning platforms, cloud-based monitoring systems, electronic class diaries, and unified enrollment portals. If, on the one hand, this technological modernization has optimized academic management and expanded pedagogical horizons, on the other hand, it has exponentially expanded the attack surface of these institutions, resulting in a massive and continuous collection of sensitive personal data belonging to a hyper-vulnerable public : children and adolescents.

Within this context, the entry into force of the General Data Protection Law (LGPD) — Law No. 13.709/2018 — imposed a severe compliance paradigm on the Brazilian market, establishing in its Article 14 rigorous and specific guidelines for the processing of data of minors, requiring observance of the principle of the best interests of the child and the explicit and prominent consent of their legal guardians. However, although the Information and Communication Technology (ICT) infrastructure in schools has advanced to enable the functional activities of teaching, organizational maturity regarding information security and privacy governance has not kept pace with the same rate of evolution. The scenario has become

even more demanding with the recent enactment of Law No. 15.211/2025, the Digital Statute of Children and Adolescents, which defined and tightened the rules for the exposure and informational profiling of minors in virtual environments.

Thus, in the practical reality of schools, a scenario of structural vulnerability of assets and information flows is observed. It is common to find the absence of formal data inventories, the storage of student and financial records on local administrative computers lacking encryption, and the indiscriminate sharing of highly sensitive information—such as medical records, allergy records, and psycho-pedagogical reports—through informal communication channels and instant messaging applications. Given weaknesses in network perimeters and gaps in user training against social engineering vectors, the educational ecosystem becomes a critical target for security incidents, cyber leaks, and severe administrative sanctions applied by the competent regulatory bodies.

Given this context of risk, the following research problem emerges: How to mitigate cybersecurity and privacy vulnerabilities and effectively structure the governance of sensitive personal data in school environments in accordance with the technical requirements of the LGPD (Brazilian General Data Protection Law) and the New Digital ECA (Brazilian Statute of Children and Adolescents)?

This study is justified by the latent need to fill the existing methodological gap between the strictly legal obligations of privacy legislation and the actual technical operation of IT support and infrastructure teams in schools. The overall objective of this article is to propose and detail a structured action plan in logical and consecutive phases for managing the lifecycle of school data, promoting the transition from a purely reactive security model to a preventive, resilient, and strictly legally compliant approach.

2. Theoretical Framework / Results

2.1 Data Protection of Minors and the Regulatory Impact of Law No. 15.211/2025

The enactment of the General Data Protection Law (LGPD) ushered in a new era of civil liability and information governance in Brazil. Within educational institutions, the regulatory impact takes on even more complex proportions due to the nature of the public served. Article 14 of the aforementioned law categorically states that the processing of personal data of children and adolescents must be carried out in their best interests, in accordance with relevant legislation and the general principles of data protection (BRAZIL, 2018).

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 06/20/2026 | Accepted: 06/23/2026 | Publication: 06/26/2026

Brazilian law has conferred a status of " hyper-vulnerability " on minors in the digital environment. This translates into the requirement for rigorous safeguards: beyond conventional legal bases, the processing of children's data requires specific and prominent consent given by at least one parent or legal guardian. In the school environment, this precept directly impacts enrollment systems, academic monitoring records, and even automated attendance records (MENDES; DONEDA, 2020, p. 52).

This special protection of the personality rights of minors reached a new level of rigor and specificity with the entry into force of Law No. 15.211/2025, known as the Digital Statute of Children and Adolescents (ECA Digital). This legislation formally extends the constitutional principle of absolute priority and full protection to the virtual environment, imposing severe obligations on technology products, applications, and services that are directed at or likely to be accessed by this highly vulnerable public (BRAZIL, 2025).

Under the aegis of Law No. 15.211/2025, the digital ecosystem of schools is now being heavily impacted. The legal instrument expressly prohibits practices of profiling minors' data for advertising or commercial purposes within educational software. The new law establishes that the platforms and operating systems adopted must configure, by default (*privacy). (by default*), the most protective models available in terms of privacy, requiring auditable and reliable mechanisms for access control and validation.

In the daily routine of schools, the categories of data handled go beyond the merely registration-based scope. According to the Practical Guide for the Education Sector of the ANPD (2023), institutions routinely manage psychopedagogical reports, medical records, and health restriction reports, which are classified as sensitive personal data according to Article 5, item II of the LGPD (Brazilian General Data Protection Law). The lack of governance over this information, in addition to violating the principles of necessity and purpose of the general law, becomes subject to the punitive scrutiny of the ECA Digital (Brazilian Statute of Children and Adolescents). The sanctions provided for by Law No. 15.211/2025 include institutional warnings and severe fines calculated based on revenue or the volume of registered users exposed to cyber risk (BRAZIL, 2025).

2.2 The Data Lifecycle and Endpoint Vulnerability in ICT

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Year VII, v.1 2026 | Submission: 06/20/2026 | Accepted: 06/23/2026 | Publication: 06/26/2026

Beyond legal compliance, information security requires technical expertise over the data lifecycle, encompassing the phases of collection, processing, sharing, storage, and secure disposal. Pinheiro (2021) warns that most data breach incidents in organizations do not stem from highly sophisticated external attacks, but rather from the absence of clear internal governance processes and mapping of information flows.

In schools, data flow often lacks traceability. Data collected during enrollment is replicated in local spreadsheets, shared with faculty, and stored on administrative computers that function as vulnerable endpoints . According to Nakamura and Geus (2017), an endpoint (workstation, notebook, or connected device) without proper logical protection acts as the main entry point for cyber threats in corporate environments. The lack of network segmentation in schools—allowing the Wi-Fi network used by students and visitors to access the same server that stores the administrative database—drastically increases the risk of intrusions.

Adding to this technical scenario is the "human factor" as an element of vulnerability. Crespo (2022) highlights that social engineering, through phishing tactics or inducement to error, directly exploits the lack of user training to obtain access credentials illegitimately. In everyday school life, the habit of sharing class lists or grades via instant messaging applications without certified encryption (such as informal corporate or personal WhatsApp groups) subverts any IT perimeter control, scattering protected data across third-party infrastructures without any institutional governance.

2. Material and Method

To achieve the objectives outlined in this study, a qualitative and exploratory methodological approach was adopted. According to Minayo (2014), qualitative research works with the universe of meanings, motives, aspirations, beliefs, values, and attitudes, which corresponds to a deeper space of relationships, processes, and phenomena that cannot be reduced to the operationalization of raw quantitative variables. The choice of an exploratory approach is justified by the need to provide greater familiarity with the proposed problem, allowing for convergence between the abstract requirements of privacy legislation and the practical reality of IT infrastructure.

The technical procedure was configured as a Case Study, associated with bibliographic and documentary research. As Yin (2015) advocates, the case study presents itself as a recommended research strategy when seeking to understand contemporary phenomena embedded in their real context, especially when the boundaries between the phenomenon and

the context are not clearly evident. The object of analysis of this study consisted of the operational, pedagogical, and administrative routines of school units, mapping their latent informational flows.

The collection of documentary and bibliographic data was based on a survey of current national legislation—with emphasis on Law No. 13.709/2018 (LGPD) and Law No. 15.211/2025 (ECA Digital)—, on resolutions and practical guides published by the National Data Protection Authority (ANPD), as well as on international information security frameworks and standards, notably ABNT NBR ISO/IEC 27001 and 27002. Data analysis was performed using content analysis techniques, allowing the identification of the main structural vulnerabilities of school ICT assets and, based on these, the conception and structuring of a methodological framework for preventive and resilient intervention divided into logical and replicable phases.

3. Results and Discussion

3.1 Situational Diagnosis and Problematization of the School Information Flow

The analysis of the operational and administrative routines of the school units revealed an informational ecosystem characterized by high fragmentation and diffuse vulnerability. The mapping of the data flow revealed that the life cycle of personal information — from the initial collection at the time of enrollment to the final archiving or purging — lacks traceability and perimeter controls for information security.

The first major vulnerability identified lies in the decentralized and unprotected storage of sensitive data on administrative endpoints . Computers located in departments and unit directorates often operate without logical segregation of profiles, allowing users with different functional responsibilities to indiscriminately access registration databases, financial records, and student health histories. The absence of encryption at rest on these assets and the lack of restrictions on removable media (such as USB devices) constitute critical vectors for the unauthorized exfiltration of information or infection by malicious code.

In parallel, the pedagogical dimension revealed itself to be an operational bottleneck regarding privacy. Given the absence of approved institutional channels and clear usage policies, the widespread use of instant messaging applications and private social networks for sharing psycho-pedagogical reports, disciplinary incident reports, and medical restriction forms was observed. This informal flow disperses sensitive data of minors across third-party servers,

circumventing ICT control mechanisms and directly contradicting the principles of security, purpose, and necessity advocated by the LGPD (Brazilian General Data Protection Law).

3.2 Intervention Framework: The Six Phases of Privacy Governance in Schools

As a technical and structured response to the bottlenecks identified, a governance and adaptation framework is proposed, divided into six logical, consecutive, and complementary phases, designed to raise the organizational maturity of the institution and meet the requirements of the LGPD (Brazilian General Data Protection Law) and the ECA Digital (Law No. 15.211/2025):

- **Phase 1 - Data Diagnosis and Inventory:** This phase consists of an exhaustive survey and mapping of all the school's informational assets, encompassing physical files (folders of archived files) and digital files (local spreadsheets, legacy systems). The objective is to catalog the nature of the data processed, identifying the operators and the legal bases that support each operation.
- **Phase 2 - Access Segregation and Minimum Privilege:** Implementation of *role- based access control matrices (RBAC*). From this perspective, faculty and administrative staff will have restricted visibility only to the data strictly necessary for the performance of their teaching or operational duties. This matrix directly addresses the requirement for a protective default configuration (*privacy) . by default*) of the ECA Digital, preventing universal or indiscriminate access to sensitive records.
- **Endpoint and Network Asset Shielding :** Application of strict logical security controls on workstations. This phase includes the mandatory installation of corporate antivirus and firewall solutions, automated operating system patch updates , disk encryption, and physical or logical blocking of USB ports to mitigate the risk of leaks and malware introduction.
- **Phase 4 - Channel Approval and Secure Communication:** Migration and centralization of the information exchange flow to an encrypted corporate cloud environment officially approved by the institution. The use of personal messaging tools for professional purposes is prohibited, complying with the legal requirement of Law No. 15.211/2025, which obliges institutions to monitor and mitigate the traffic of student information in environments lacking supervision and audit mechanisms.

- **Phase 5 - Disposal and Retention Management:** Establishment of a document retention schedule and technical protocols for secure disposal. Data from students who have broken their institutional ties must be deleted or anonymized as soon as the legal retention period required by the Ministry of Education expires, avoiding the unnecessary accumulation of cyber risk liabilities.
- **Phase 6 - Monitoring, Culture, and Continuous Auditing:** Establishment of auditing routines through weekly checklists of technical and operational compliance. Additionally, this phase encompasses the ongoing training of faculty and administrative staff through awareness programs against social engineering vectors. Continuous monitoring ensures that software contracted by the network complies with the prohibition of profiling or abusive data collection within the classroom.

3.3 The Strategic Role of RIPD in Institutional Safeguarding

The consolidation of the proposed governance framework culminates in the preparation of the Personal Data Protection Impact Assessment Report (PIIA), as recommended by the National Data Protection Authority (ANPD). The PIIA functions as a living piece of technical and legal documentation, containing a detailed description of data processing activities that may generate risks to the civil liberties and fundamental rights of data subjects (minors and their guardians).

By documenting the risks inherent in school operations and, above all, by outlining the measures, safeguards, and mitigation mechanisms adopted throughout the six phases of intervention, the RIPD (Report on Impact of Data Protection) provides the educational institution with solid legal protection. In scenarios of active oversight or unforeseen incidents, the existence of a structured and auditable impact report acts as conclusive evidence of governance, good faith, and technical diligence, minimizing the application of the severe administrative sanctions of the LGPD (Brazilian General Data Protection Law) and the ECA Digital (Brazilian Statute of Children and Adolescents), demonstrating maturity in information security to society (ANPD, 2023).

Final Considerations

The investigation conducted throughout this study allowed for a structured response to the proposed research problem, demonstrating that mitigating cybersecurity vulnerabilities and

ensuring compliance with the General Data Protection Law (LGPD) and the New Digital ECA (Law No. 15.211/2025) in the school ecosystem fundamentally depend on overcoming a purely reactive IT model. The transition to a proactive and resilient approach requires the implementation of robust privacy governance, capable of integrating logical infrastructure information security into the daily operational, pedagogical, and administrative routines of educational institutions.

The overall objective of this article was fully achieved through the design and detailing of the intervention framework divided into six consecutive phases. It became evident that isolated technological actions are insufficient if they are not accompanied by a systematic mapping of the data lifecycle, the rigorous application of the principle of least privilege in controlling corporate access, and the effective protection of administrative endpoints in school secretariats. Furthermore, it was found that the human factor plays a critical role in sustaining this security mechanism, making continuous awareness programs against social engineering vectors an indispensable pillar for building an organizational culture of privacy.

From a legal and institutional perspective, the study demonstrated the strategic centrality of the Data Protection Impact Assessment (DPIA). Far from being merely a bureaucratic obligation, the DPIA is consolidated as a living governance instrument and institutional safeguard, serving as material evidence of good faith, diligence, and technical compliance before regulatory oversight bodies, such as the National Data Protection Authority (ANPD).

As a limitation of this work, its eminently conceptual and propositional character is acknowledged, structured from an analytical case study based on documentary and bibliographic review. For future research and developments, the empirical application of the proposed six-phase framework in a real municipal education unit or network is recommended. Such practical implementation will enable the collection of quantitative indicators of cyber efficiency, the measurement of the level of organizational maturity post-intervention, and the refinement of sensitive data protection methodologies aimed at guaranteeing the best interests of children and adolescents in the digital age.

References

Brazilian Association of Technical Standards (ABNT). ABNT NBR ISO/IEC 27002: Information technology — Security techniques — Code of practice for information security controls. Rio de Janeiro: ABNT, 2022.

National Data Protection Authority (ANPD). Practical Guide for Data Processing Agents in the Education Sector. Brasília, DF: ANPD, 2023.

BRAZIL. Law No. 13.709, of August 14, 2018. General Law on the Protection of Personal Data (LGPD). Brasília, DF: Presidency of the Republic, 2018.

BRAZIL. Law No. 15.211, of September 17, 2025. Establishes the Digital Statute for Children and Adolescents (ECA Digital) and provides for the protection of children and adolescents in the digital environment. Brasília, DF: Presidency of the Republic, 2025.

COSTA, Maria Adélia da. Teacher Training Policies for Vocational Education: reality or utopia? Curitiba: Appris , 2016.

CRESPO, Marcelo Xavier. Cybersecurity and the human factor: risks and governance. Brazilian Journal of Digital Law, v. 4, n. 2, p. 89-104, 2022.

DE CARVALHO, RL; CABRAL, RG; ROSARIO FERRER, Y. INTELLIGENT TUTORING SYSTEMS AS A DIDACTIC RESOURCE IN MATHEMATICS TEACHING. HOLOS, [S. l.], v. 6, p. 1–11, 2019. DOI: 10.15628/holos.2019.7028. Available at: https://www2.ifrn.edu.br/ojs/index.php/HOLOS/article/view/7028. Accessed on: June 4, 2023.

MENDES, Laura Schertel ; DONEDA, Danilo. The protection of personal data of children and adolescents under the LGPD. Consumer Law Review, v. 128, p. 45-67, 2020.

MINAYO, Maria Cecília de Souza (ed.). Social Research: theory, method and creativity. 34th ed. Petrópolis: Vozes, 2014.

NAKAMURA, Emilio Tissato ; GEUS, Paulo Lício de. Network Security in Corporate Environments. São Paulo: Novatec , 2017.

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

ROSATELLI, MC, & Self, JA 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, April. 2000.

YIN, Robert K. Case Study: Planning and Methods. 5th ed. Porto Alegre: Bookman, 2015.

ACKNOWLEDGEMENTS

First and foremost, I thank God for the strength, wisdom, and discernment granted throughout this academic journey. To my mother, for her unconditional support, exemplary love, and patience during my absences dedicated to my studies. To the professors and tutors of the MBA in Information Security course, for the precise guidance and sharing of knowledge that made the technical development of this work possible. To the teachers in the field of education who work at the forefront of the school ecosystem, because without them and their daily resilience, there would be no construction of knowledge, no digital transformation in

classrooms, and no pressing need to protect the integrity and future of our students. Finally, to all colleagues and professionals in the field of Information Technology who, directly or indirectly, contributed to the maturation of the concepts and reflections presented in this article.