RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Año VII, vol. 1 2026 | Envío: 20/06/2026 | Aceptado: 23/06/2026 | Publicación: 26/06/2026

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

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

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

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.

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.

Introducción

La aceleración del proceso de transformación digital en el contexto actual ha reconfigurado profundamente la dinámica operativa, administrativa y pedagógica de las instituciones educativas. Los centros escolares, tanto públicos como privados, han migrado progresivamente sus rutinas a plataformas de aprendizaje digital, sistemas de monitorización en la nube, agendas electrónicas y portales de matriculación unificados. Si bien esta modernización tecnológica ha optimizado la gestión académica y ampliado los horizontes pedagógicos, también ha incrementado exponencialmente la superficie de ataque de estas instituciones, lo que ha derivado en una recopilación masiva y continua de datos personales sensibles pertenecientes a un público hipervulnerable : los niños y adolescentes.

En este contexto, la entrada en vigor de la Ley General de Protección de Datos (LGPD) —Ley n.º 13.709/2018— impuso un estricto paradigma de cumplimiento en el mercado brasileño, estableciendo en su artículo 14 directrices rigurosas y específicas para el tratamiento de datos de menores, exigiendo la observancia del principio del interés superior del niño y el consentimiento explícito y destacado de sus tutores legales. Sin embargo, si bien la infraestructura de Tecnologías de la Información y la Comunicación (TIC) en los centros

educativos ha avanzado para facilitar las actividades docentes, la madurez organizativa en materia de seguridad de la información y gobernanza de la privacidad no ha seguido el mismo ritmo de evolución. El panorama se ha vuelto aún más exigente con la reciente promulgación de la Ley n.º 15.211/2025, el Estatuto Digital del Niño y del Adolescente, que definió y reforzó las normas para la exposición y la elaboración de perfiles informativos de menores en entornos virtuales.

Así, en la práctica, se observa un escenario de vulnerabilidad estructural de los activos y los flujos de información en las escuelas. Es frecuente encontrar la ausencia de inventarios de datos formales, el almacenamiento de registros estudiantiles y financieros en computadoras administrativas locales sin cifrado, y el intercambio indiscriminado de información altamente sensible —como historiales médicos, registros de alergias e informes psicopedagógicos— a través de canales de comunicación informales y aplicaciones de mensajería instantánea. Dadas las debilidades en los perímetros de red y las deficiencias en la capacitación de los usuarios frente a las técnicas de ingeniería social, el ecosistema educativo se convierte en un objetivo crítico para incidentes de seguridad, filtraciones cibernéticas y severas sanciones administrativas impuestas por los organismos reguladores competentes.

Dado este contexto de riesgo, surge el siguiente problema de investigación: ¿Cómo mitigar las vulnerabilidades de ciberseguridad y privacidad y estructurar eficazmente la gobernanza de datos personales sensibles en entornos escolares de acuerdo con los requisitos técnicos de la LGPD (Ley General de Protección de Datos de Brasil) y la Nueva ECA Digital (Estatuto Brasileño de Niños y Adolescentes)?

Este estudio se justifica por la necesidad latente de subsanar la brecha metodológica existente entre las estrictas obligaciones legales de la legislación sobre privacidad y el funcionamiento técnico real de los equipos de soporte e infraestructura informática en los centros educativos. El objetivo general de este artículo es proponer y detallar un plan de acción estructurado en fases lógicas y consecutivas para gestionar el ciclo de vida de los datos escolares, promoviendo la transición de un modelo de seguridad puramente reactivo a un enfoque preventivo, resiliente y que cumpla estrictamente con la normativa legal.

2. Marco teórico / Resultados

2.1 **Protección de datos de menores y el impacto normativo de la Ley nº 15.211/2025**

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Año VII, vol. 1 2026 | Envío: 20/06/2026 | Aceptado: 23/06/2026 | Publicación: 26/06/2026

La entrada en vigor de la Ley General de Protección de Datos (LGPD) marcó el comienzo de una nueva era de responsabilidad civil y gobernanza de la información en Brasil. En las instituciones educativas, el impacto regulatorio adquiere una dimensión aún más compleja debido a la naturaleza del público al que sirve. El artículo 14 de dicha ley establece categóricamente que el tratamiento de datos personales de niños y adolescentes debe realizarse en su mejor interés, de conformidad con la legislación pertinente y los principios generales de protección de datos (BRASIL, 2018).

La legislación brasileña ha otorgado a los menores de edad un estatus de " hipervulnerabilidad " en el entorno digital. Esto se traduce en la exigencia de medidas de seguridad rigurosas: más allá de las bases legales convencionales, el tratamiento de datos de menores requiere el consentimiento específico y explícito de al menos uno de sus padres o tutores legales. En el ámbito escolar, este precepto impacta directamente en los sistemas de matriculación, los registros de seguimiento académico e incluso los registros automatizados de asistencia (MENDES; DONEDA, 2020, p. 52).

Esta protección especial de los derechos de la personalidad de los menores alcanzó un nuevo nivel de rigor y especificidad con la entrada en vigor de la Ley N° 15.211/2025, conocida como Estatuto Digital de Niños y Adolescentes (ECA Digital). Esta legislación extiende formalmente el principio constitucional de prioridad absoluta y protección plena al entorno virtual, imponiendo severas obligaciones a los productos, aplicaciones y servicios tecnológicos dirigidos a este público altamente vulnerable o que puedan ser utilizados por él (BRASIL, 2025).

Bajo la Ley N° 15.211/2025, el ecosistema digital de las escuelas se ve ahora fuertemente impactado. El instrumento legal prohíbe expresamente las prácticas de elaboración de perfiles de datos de menores con fines publicitarios o comerciales dentro del software educativo. La nueva ley establece que las plataformas y los sistemas operativos adoptados deben configurar, por defecto, la *privacidad. (por defecto*), los modelos más protectores disponibles en términos de privacidad, que requieren mecanismos auditables y confiables para el control de acceso y la validación.

En la rutina diaria de las escuelas, las categorías de datos que se manejan van más allá del ámbito meramente basado en el registro. Según la Guía Práctica para el Sector Educativo de la ANPD (2023), las instituciones manejan habitualmente informes psicopedagógicos, expedientes médicos e informes de restricciones de salud, que se clasifican como datos personales sensibles según el artículo 5, inciso II de la LGPD (Ley General de Protección de Datos de Brasil). La falta de gobernanza sobre esta información, además de violar los principios

de necesidad y finalidad de la ley general, la hace susceptible de la supervisión punitiva de la ECA Digital (Ley de Niños y Adolescentes de Brasil). Las sanciones previstas en la Ley N° 15.211/2025 incluyen advertencias institucionales y multas severas calculadas en función de los ingresos o el volumen de usuarios registrados expuestos al riesgo cibernético (BRASIL, 2025).

2.2 El ciclo de vida de los datos y la vulnerabilidad de los puntos finales en las TIC

Más allá del cumplimiento legal, la seguridad de la información requiere experiencia técnica en todo el ciclo de vida de los datos, abarcando las fases de recopilación, procesamiento, intercambio, almacenamiento y eliminación segura. Pinheiro (2021) advierte que la mayoría de los incidentes de filtración de datos en las organizaciones no se deben a ataques externos altamente sofisticados, sino a la ausencia de procesos de gobernanza interna claros y de un mapeo adecuado de los flujos de información.

En los centros educativos, el flujo de datos suele carecer de trazabilidad. Los datos recopilados durante la matrícula se replican en hojas de cálculo locales, se comparten con el profesorado y se almacenan en ordenadores administrativos que funcionan como puntos de acceso vulnerables . Según Nakamura y Geus (2017), un punto de acceso (estación de trabajo, portátil o dispositivo conectado) sin la protección lógica adecuada actúa como principal puerta de entrada para las ciberamenazas en entornos corporativos. La falta de segmentación de la red en los centros educativos —que permite que la red Wi-Fi utilizada por estudiantes y visitantes acceda al mismo servidor que almacena la base de datos administrativa— aumenta drásticamente el riesgo de intrusiones.

A este escenario técnico se suma el factor humano como elemento de vulnerabilidad. Crespo (2022) destaca que la ingeniería social, mediante tácticas de phishing o la inducción al error, explota directamente la falta de capacitación del usuario para obtener credenciales de acceso ilegítimamente. En la vida escolar cotidiana, el hábito de compartir listas de clase o calificaciones a través de aplicaciones de mensajería instantánea sin cifrado certificado (como grupos informales de WhatsApp corporativos o personales) socava cualquier control perimetral de TI, dispersando datos protegidos en infraestructuras de terceros sin ninguna gobernanza institucional.

2. Material y método

Para alcanzar los objetivos planteados en este estudio, se adoptó un enfoque metodológico cualitativo y exploratorio. Según Minayo (2014), la investigación cualitativa trabaja con el universo de significados, motivos, aspiraciones, creencias, valores y actitudes, lo que corresponde a un espacio más profundo de relaciones, procesos y fenómenos que no pueden reducirse a la operacionalización de variables cuantitativas básicas. La elección de un enfoque exploratorio se justifica por la necesidad de comprender mejor el problema propuesto, permitiendo la convergencia entre los requisitos abstractos de la legislación sobre privacidad y la realidad práctica de la infraestructura de TI.

El procedimiento técnico se configuró como un estudio de caso, asociado a una investigación bibliográfica y documental. Como propone Yin (2015), el estudio de caso se presenta como una estrategia de investigación recomendable para comprender fenómenos contemporáneos insertos en su contexto real, especialmente cuando los límites entre el fenómeno y el contexto no son claramente evidentes. El objeto de análisis de este estudio consistió en las rutinas operativas, pedagógicas y administrativas de las unidades escolares, mapeando sus flujos de información latentes.

La recopilación de datos documentales y bibliográficos se basó en un estudio de la legislación nacional vigente —con especial énfasis en la Ley n.º 13.709/2018 (LGPD) y la Ley n.º 15.211/2025 (ECA Digital)—, en resoluciones y guías prácticas publicadas por la Autoridad Nacional de Protección de Datos (ANPD), así como en marcos y estándares internacionales de seguridad de la información, en particular ABNT NBR ISO/IEC 27001 y 27002. El análisis de datos se realizó mediante técnicas de análisis de contenido, lo que permitió identificar las principales vulnerabilidades estructurales de los activos TIC escolares y, a partir de estas, concebir y estructurar un marco metodológico para la intervención preventiva y resiliente, dividido en fases lógicas y replicables.

3. Resultados y discusión

3.1 Diagnóstico situacional y problematización del flujo de información escolar

El análisis de las rutinas operativas y administrativas de las unidades escolares reveló un ecosistema informativo caracterizado por una alta fragmentación y una vulnerabilidad difusa. El mapeo del flujo de datos reveló que el ciclo de vida de la información personal —

desde la recopilación inicial al momento de la inscripción hasta el archivo o la eliminación final— carece de trazabilidad y controles perimetrales para la seguridad de la información.

La primera vulnerabilidad importante identificada reside en el almacenamiento descentralizado y sin protección de datos confidenciales en los equipos administrativos . Los ordenadores ubicados en departamentos y direcciones suelen funcionar sin una segregación lógica de perfiles, lo que permite a usuarios con diferentes responsabilidades funcionales acceder indiscriminadamente a bases de datos de registro, historiales financieros e historiales médicos de los estudiantes. La ausencia de cifrado en reposo en estos activos y la falta de restricciones en los soportes extraíbles (como los dispositivos USB) constituyen vectores críticos para la filtración no autorizada de información o la infección por código malicioso.

Paralelamente, la dimensión pedagógica se reveló como un cuello de botella operativo en lo que respecta a la privacidad. Ante la ausencia de canales institucionales aprobados y políticas de uso claras, se observó el uso generalizado de aplicaciones de mensajería instantánea y redes sociales privadas para compartir informes psicopedagógicos, informes de incidentes disciplinarios y formularios de restricciones médicas. Este flujo informal dispersa datos sensibles de menores a través de servidores de terceros, eludiendo los mecanismos de control de las TIC y contradiciendo directamente los principios de seguridad, finalidad y necesidad que promueve la LGPD (Ley General de Protección de Datos de Brasil).

3.2 Marco de intervención: Las seis fases de la gobernanza de la privacidad en las escuelas

Como respuesta técnica y estructurada a los cuellos de botella identificados, se propone un marco de gobernanza y adaptación, dividido en seis fases lógicas, consecutivas y complementarias, diseñado para elevar la madurez organizativa de la institución y cumplir con los requisitos de la LGPD (Ley General de Protección de Datos de Brasil) y la ECA Digital (Ley nº 15.211/2025):

- **Fase 1 - Diagnóstico e inventario de datos:** Esta fase consiste en un análisis exhaustivo y la cartografía de todos los activos informáticos del centro educativo, incluyendo archivos físicos (carpetas de archivos archivados) y digitales (hojas de cálculo locales, sistemas heredados). El objetivo es catalogar la naturaleza de los datos procesados, identificando a los operadores y las bases legales que sustentan cada operación.
- **Fase 2 - Segregación de acceso y privilegios mínimos:** Implementación de matrices *de control de acceso basado en roles (RBAC*). Desde esta perspectiva, el profesorado

y el personal administrativo tendrán visibilidad restringida únicamente a los datos estrictamente necesarios para el desempeño de sus funciones docentes u operativas. Esta matriz aborda directamente el requisito de una configuración predeterminada de protección (*privacidad) . por defecto*) de la ECA Digital, impidiendo el acceso universal o indiscriminado a los registros sensibles.

- **Protección de puntos finales y activos de red :** Aplicación de estrictos controles de seguridad lógica en las estaciones de trabajo. Esta fase incluye la instalación obligatoria de soluciones antivirus y de firewall corporativas, actualizaciones automáticas de parches del sistema operativo , cifrado de disco y bloqueo físico o lógico de los puertos USB para mitigar el riesgo de fugas e introducción de malware.
- **Fase 4 - Aprobación del canal y comunicación segura:** Migración y centralización del flujo de intercambio de información a un entorno de nube corporativa cifrada, oficialmente aprobado por la institución. Se prohíbe el uso de herramientas de mensajería personal con fines profesionales, en cumplimiento de la Ley N° 15.211/2025, que obliga a las instituciones a supervisar y mitigar el tráfico de información estudiantil en entornos que carecen de mecanismos de supervisión y auditoría.
- **Fase 5 - Gestión de Eliminación y Retención:** Establecimiento de un calendario de retención de documentos y protocolos técnicos para su eliminación segura. Los datos de los estudiantes que hayan roto sus vínculos institucionales deben eliminarse o anonimizarse tan pronto como expire el período de retención legal exigido por el Ministerio de Educación, evitando así la acumulación innecesaria de responsabilidades por riesgos cibernéticos.
- **Fase 6 - Monitoreo, Cultura y Auditoría Continua:** Establecimiento de rutinas de auditoría mediante listas de verificación semanales de cumplimiento técnico y operativo. Además, esta fase abarca la capacitación continua del profesorado y el personal administrativo a través de programas de concientización sobre las técnicas de ingeniería social. El monitoreo continuo garantiza que el software contratado por la red cumpla con la prohibición de la elaboración de perfiles o la recopilación abusiva de datos en el aula.

3.3 El papel estratégico de la RIPD en la protección institucional

La consolidación del marco de gobernanza propuesto culmina con la elaboración del Informe de Evaluación de Impacto en la Protección de Datos Personales (IEIP), según lo recomendado por la Autoridad Nacional de Protección de Datos (ANPD). El IEIP funciona como un documento técnico y jurídico dinámico que contiene una descripción detallada de las actividades de tratamiento de datos que pueden generar riesgos para las libertades civiles y los derechos fundamentales de los titulares de los datos (menores y sus tutores).

Al documentar los riesgos inherentes a las operaciones escolares y, sobre todo, al detallar las medidas, salvaguardias y mecanismos de mitigación adoptados a lo largo de las seis fases de intervención, el RIPD (Informe sobre el Impacto de la Protección de Datos) proporciona a la institución educativa una sólida protección jurídica. En escenarios de supervisión activa o incidentes imprevistos, la existencia de un informe de impacto estructurado y auditable constituye una prueba concluyente de gobernanza, buena fe y diligencia técnica, minimizando la aplicación de las severas sanciones administrativas de la LGPD (Ley General de Protección de Datos de Brasil) y la ECA Digital (Ley de la Infancia y la Adolescente de Brasil), demostrando madurez en materia de seguridad de la información ante la sociedad (ANPD, 2023).

Consideraciones finales

La investigación realizada a lo largo de este estudio permitió una respuesta estructurada al problema de investigación planteado, demostrando que la mitigación de las vulnerabilidades de ciberseguridad y el cumplimiento del Reglamento General de Protección de Datos (RGPD) y la Nueva Ley de Educación y Cultura Digital (Ley n.º 15.211/2025) en el ecosistema escolar dependen fundamentalmente de superar un modelo de TI puramente reactivo. La transición hacia un enfoque proactivo y resiliente requiere la implementación de una sólida gobernanza de la privacidad, capaz de integrar la seguridad de la información de la infraestructura lógica en las rutinas operativas, pedagógicas y administrativas diarias de las instituciones educativas.

El objetivo general de este artículo se logró plenamente mediante el diseño y la elaboración del marco de intervención, dividido en seis fases consecutivas. Se hizo evidente que las acciones tecnológicas aisladas resultan insuficientes si no se complementan con un mapeo sistemático del ciclo de vida de los datos, la aplicación rigurosa del principio de mínimo privilegio en el control del acceso corporativo y la protección efectiva de los puntos finales administrativos en las secretarías escolares. Asimismo, se constató que el factor humano desempeña un papel fundamental en el mantenimiento de este mecanismo de seguridad, lo que

convierte a los programas de sensibilización continua contra los vectores de ingeniería social en un pilar indispensable para la construcción de una cultura organizacional de privacidad.

Desde una perspectiva jurídica e institucional, el estudio demostró la importancia estratégica de la Evaluación de Impacto en la Protección de Datos (EIPD). Lejos de ser una mera obligación burocrática, la EIPD se consolida como un instrumento de gobernanza dinámico y una salvaguarda institucional, que sirve como prueba fehaciente de buena fe, diligencia y cumplimiento técnico ante organismos de supervisión regulatoria, como la Autoridad Nacional de Protección de Datos (ANPD).

Como limitación de este trabajo, se reconoce su carácter eminentemente conceptual y proposicional, estructurado a partir de un estudio de caso analítico basado en una revisión documental y bibliográfica. Para futuras investigaciones y desarrollos, se recomienda la aplicación empírica del marco de seis fases propuesto en una unidad o red educativa municipal real. Dicha implementación práctica permitirá recopilar indicadores cuantitativos de cibereficiencia, medir el nivel de madurez organizacional tras la intervención y perfeccionar metodologías de protección de datos sensibles, con el fin de garantizar el interés superior de los niños y adolescentes en la era digital.

Referencias

Asociación Brasileña de Normas Técnicas (ABNT). ABNT NBR ISO/IEC 27002: Tecnología de la información — Técnicas de seguridad — Código de buenas prácticas para los controles de seguridad de la información. Río de Janeiro: ABNT, 2022.

Autoridad Nacional de Protección de Datos (ANPD). Guía práctica para los responsables del tratamiento de datos en el sector educativo. Brasilia, DF: ANPD, 2023.

BRASIL. Ley N° 13.709, de 14 de agosto de 2018. Ley General de Protección de Datos Personales (LGPD). Brasilia, DF: Presidencia de la República, 2018.

BRASIL. Ley N° 15.211, del 17 de septiembre de 2025. Por la cual se establece el Estatuto Digital para Niños y Adolescentes (ECA Digital) y se prevé la protección de los niños y adolescentes en el entorno digital. Brasilia, DF: Presidencia de la República, 2025.

COSTA, María Adélia da. Políticas de formación docente para la Educación Profesional: ¿realidad o utopía? Curitiba: Appris , 2016.

CRESPO, Marcelo Xavier. Ciberseguridad y factor humano: riesgos y gobernanza. Revista Brasileña de Derecho Digital, vol. 4, n.º 2, págs. 89-104, 2022.

DE CARVALHO, RL; CABRAL, RG; ROSARIO FERRER, Y. SISTEMAS DE TUTORÍA INTELIGENTE COMO RECURSO DIDÁCTICO EN LA ENSEÑANZA DE LAS MATEMÁTICAS. HOLOS, [S. l.], vol. 6, págs. 1–11, 2019. DOI: 10.15628/holos.2019.7028.

Disponible en: https://www2.ifrn.edu.br/ojs/index.php/HOLOS/article/view/7028. Consultado el 4 de junio de 2023.

MENDES, Laura Schertel ; DONEDA, Danilo. La protección de datos personales de niños y adolescentes según la LGPD. Consumer Law Review, vol. 128, págs. 45-67, 2020.

MINAYO, María Cecília de Souza (ed.). Investigación Social: teoría, método y creatividad. 34ª edición. Petrópolis: Vozes, 2014.

NAKAMURA, Emilio Tissato ; GEUS, Paulo Lício de. Seguridad de redes en entornos corporativos. São Paulo: Novatec , 2017.

PINHEIRO, Patricia Peck. Derecho Digital. 7ª edición. São Paulo: Saraiva Educação, 2021.

ROSATELLI, MC y Self, JA Apoyo aprendizaje a distancia a partir de estudios de caso . En S. P Lajoie y M. Vivet (Eds.), Actas del 9º internacional conferencia Sobre inteligencia artificial en la educación , págs. 457-564, abril de 2000.

YIN, Robert K. Estudio de caso: Planificación y métodos. 5.ª ed. Porto Alegre: Bookman, 2015.

EXPRESIONES DE GRATITUD

En primer lugar, agradezco a Dios la fortaleza, la sabiduría y el discernimiento que me han brindado a lo largo de este camino académico. A mi madre, por su apoyo incondicional, su amor ejemplar y su paciencia durante mis ausencias dedicadas a mis estudios. A los profesores y tutores del MBA en Seguridad de la Información, por la precisa orientación y el intercambio de conocimientos que hicieron posible el desarrollo técnico de este trabajo. A los docentes del ámbito educativo que trabajan en la vanguardia del ecosistema escolar, porque sin ellos y su resiliencia diaria, no habría construcción de conocimiento, ni transformación digital en las aulas, ni la imperiosa necesidad de proteger la integridad y el futuro de nuestros estudiantes. Finalmente, a todos los colegas y profesionales del campo de las Tecnologías de la Información que, directa o indirectamente, contribuyeron a la maduración de los conceptos y reflexiones presentados en este artículo.