Revista: Pulso Científico
ISSN: 3091-1958
DOI: https://doi.org/10.70577/rps.v4i1.144

Periodicidad: Trimestral Enero-Marzo, Volumen: 4, Número: 1, Año: 2026 páginas 50-65

Protección de datos personales: estudiantes universitarios en entornos virtuales, desafíos y propuestas en el contexto ecuatoriano

Personal data protection: university students in virtual environments, challenges and proposals in the ecuadorian context

Henry Antonio Guerrero Alcívar[1]
henry.guerrero@unesum.edu.ec
https://orcid.org/0000-0003-2566-7189
Universidad Estatal del Sur de Manabí, Jipijapa

Valeria Patricia Plaza Macías[2]
plaza-valeria5941@unesum.edu.ec
https://orcid.org/0009-0000-3102-1662
Universidad Estatal del Sur de Manabí, Jipijapa

Ivonne Margarita Alcívar Arteaga[3]
ing.ivonnealcivar@hotmail.com
https://orcid.org/0009-0006-9351-1011
Unidad Educativa Cristo Rey, Portoviejo

Amarilis Rocio Murillo Quimiz[4]
amarilis.murillo@unesum.edu.ec
https://orcid.org/0009-0003-1709-3258
Universidad Estatal del Sur de Manabí, Jipijapa

Como citar:

Guerrero Alcívar, H. A., Plaza Macías, V. P., Alcívar Arteaga, I. M., & Murillo Quimiz, A. R. (2026). Protección de datos personales: estudiantes universitarios en entornos virtuales, desafíos y propuestas en el contexto ecuatoriano. *Revista Pulso Científico*, *4*(1), 50–65. https://doi.org/10.70577/rps.v4i1.144

Fecha de recepción: 2026-01-03

Fecha de aceptación: 2026-01-27

Fecha de publicación: 2026-02-02

Revista: Pulso Científico
ISSN: 3091-1958
DOI: https://doi.org/10.70577/rps.v4i1.144

RESUMEN

La incorporación masiva de entornos virtuales en la educación superior ha intensificado el tratamiento de datos personales de los estudiantes, generando riesgos significativos para la privacidad. En este escenario, el estudio tuvo como objetivo identificar los desafíos predominantes y analizar estrategias efectivas para la protección de los datos personales de los estudiantes universitarios en entornos virtuales, en estricta coherencia con el marco legal ecuatoriano. La investigación se desarrolló bajo un enfoque cualitativo, mediante un estudio bibliográfico-documental sustentado en la metodología PRISMA, que permitió la revisión sistemática de literatura científica publicada entre 2022 y 2026 en bases de datos indexadas, seleccionándose un total de 28 artículos para el análisis. Los resultados muestran que los desafíos más recurrentes se concentran en la gobernanza institucional fragmentada de los datos, la dependencia de proveedores tecnológicos externos, el uso de tecnologías de evaluación remota con alto nivel de intrusión y la limitada cultura digital en materia de protección de datos. El análisis evidencia que las estrategias consideradas más efectivas en la literatura se relacionan con la responsabilidad proactiva, la seguridad de la información por diseño y por defecto, la regulación contractual de los encargados del tratamiento y la formación continua de la comunidad universitaria, las cuales presentan una alta coherencia con la Ley Orgánica de Protección de Datos Personales del Ecuador. Se concluye que la protección de los datos personales en la educación superior virtual no depende de la creación de nuevas normas, sino de la aplicación integral, preventiva y sostenida del marco legal existente, articulada con capacidades institucionales y una cultura organizacional orientada a la garantía de los derechos fundamentales de los estudiantes.

Palabras clave: Protección de datos, educación superior, entornos virtuales, privacidad.

ABSTRACT

The widespread adoption of virtual environments in higher education has intensified the processing of students' personal data, generating significant privacy risks. In this context, this study aimed to identify the prevailing challenges and analyze effective strategies for protecting the personal data of university students in virtual environments, in strict accordance with the Ecuadorian legal framework. The research was conducted using a qualitative approach, through a bibliographic-documentary study based on the PRISMA methodology. This allowed for a systematic review of scientific literature published between 2022 and 2026 in indexed databases, resulting in the selection of 28 articles for analysis. The results show that the most recurring challenges are concentrated in fragmented institutional data governance, dependence on external technology providers, the use of highly intrusive remote assessment technologies, and a limited digital culture regarding data protection. The analysis reveals that the most effective strategies identified in the literature relate to proactive responsibility, information security by design and by default, contractual regulation of data

Revista: Pulso Científico
ISSN: 3091-1958
DOI: https://doi.org/10.70577/rps.v4i1.144

processors, and ongoing training for the university community. These strategies are highly consistent with Ecuador's Organic Law on the Protection of Personal Data. The analysis concludes that the protection of personal data in online higher education does not depend on the creation of new regulations, but rather on the comprehensive, preventive, and sustained application of the existing legal framework, combined with institutional capacities and an organizational culture focused on guaranteeing students' fundamental rights.

Keywords: Data protection, higher education, virtual environments, privacy.

INTRODUCCIÓN

La expansión sostenida de los entornos virtuales en la educación superior ha incrementado de forma significativa la recolección, almacenamiento y análisis de datos personales de estudiantes. En este sentido, a escala global, este escenario ha intensificado el debate sobre privacidad y gobernanza de datos en educación, un informe de la Organización de las Naciones Unidas para la Educación (2023) advierte que los marcos legales educativos aún son insuficientes para garantizar privacidad de datos y que múltiples productos de tecnología educativa han incorporado prácticas de seguimiento y recolección de información con riesgos para los derechos de los usuarios. En paralelo, Liu y Khalil (2023) muestran que la protección de datos en contextos de analítica educativa no puede tratarse como un asunto “periférico”, pues los riesgos atraviesan todo el ciclo de uso de datos; por ello, se insiste en soluciones basadas en evidencia, transparencia e involucramiento de actores institucionales y estudiantiles.

En este marco, comprender la percepción y las preocupaciones de los estudiantes resulta clave para diseñar medidas efectivas. Mutimukwe et al., (2022) validan un modelo de preocupaciones de privacidad en *learning analytics* y evidencian cómo el equilibrio entre riesgo percibido, control percibido y confianza se relaciona con conductas de no divulgación y reservas frente al uso institucional de datos. De manera complementaria, Svetec y Divjak (2021) identifica que los problemas de privacidad y protección de datos son múltiples e interdependientes, y que su abordaje requiere políticas y prácticas sostenidas, no solo declaraciones formales.

En el contexto ecuatoriano, estas discusiones adquieren especial relevancia por la consolidación de plataformas digitales en universidades e institutos y por la exigencia normativa de proteger la información personal. La Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (2022) reporta que, con base en registros del sistema de información de educación superior, el registro de matrícula en universidades y escuelas politécnicas mostró un crecimiento promedio anual (2015–2022) del 4,82%, y en institutos técnicos y tecnológicos un crecimiento promedio semestral tomando como base el segundo semestre de 2017 frente al segundo semestre de 2022 del 25,03%, lo cual refuerza la presión sobre los ecosistemas digitales que gestionan datos estudiantiles.

Revista: Pulso Científico
ISSN: 3091-1958
DOI: https://doi.org/10.70577/rps.v4i1.144

A nivel aplicado, Álvarez y Hernández (2024) analizan la protección de datos en plataformas educativas del sistema de educación superior y señala desafíos de implementación, como; la infraestructura, capacitación y cultura de seguridad, proponiendo medidas como auditorías, políticas de seguridad y enfoques de privacidad por diseño. En este contexto, la investigación no solo busca responder a las posibles falencias en las medidas de protección de datos personales, sino que además se alinea y contribuye de manera significativa al proyecto de vinculación "Alfabetización e integración de las TIC en prácticas pedagógicas de unidades educativas y comunidades del sur de Manabí", al abordar de forma integral la relación entre educación digital, uso responsable de las tecnologías y protección de la información personal. En consecuencia, el estudio se orienta a identificar los desafíos predominantes y analizar estrategias efectivas para la protección de los datos personales de los estudiantes universitarios en entornos virtuales, en estricta coherencia con el marco legal ecuatoriano.

Protección de datos personales en la educación superior digital

La virtualización acelerada de la educación superior ha incrementado la captura, almacenamiento, análisis y circulación de datos personales a través de aulas virtuales, videoconferencias, repositorios institucionales, herramientas de evaluación y sistemas de analítica del aprendizaje. En este ecosistema, la identidad digital estudiantil se vuelve un activo crítico: credenciales, trazas de acceso, interacciones, rendimiento académico y contenidos generados por el usuario pueden ser tratados por múltiples actores, lo que amplía la superficie de riesgo y exige gobernanza institucional. Esta visión es coherente con Marín y Tur (2023) que advierten que la mediación tecnológica en entornos educativos demanda responsabilidad, transparencia y seguridad como condiciones para sostener confianza y legitimidad institucional.

Desde un enfoque normativo-garantista, la protección de datos debe entenderse como un derecho fundamental que exige límites al poder informacional de las organizaciones y mecanismos efectivos para que las personas controlen su información. En Ecuador, este marco se concreta principalmente en la Ley Orgánica de Protección de Datos Personales (2021) y su aplicación práctica en sectores intensivos en datos, como el educativo, donde históricamente se han recolectado datos "por defecto" sin estándares equivalentes de minimización, información y seguridad. Por su parte, Morales et al., (2024) subrayan que la implementación real de políticas de datos depende de capacidades institucionales, claridad regulatoria y cultura organizacional orientada a derechos.

Un punto especialmente sensible en la universidad digital es la evaluación remota, Flores (2024) muestra que el *e-proctoring* se ha expandido en educación superior latinoamericana y que la discusión científica se organiza, al menos, en cuatro ejes: efectividad, reconfiguración de relaciones entre actores, percepciones de estudiantes/docentes y factores de aceptación/implementación. Estos ejes son relevantes porque el proctoring

Revista: Pulso Científico
ISSN: 3091-1958
DOI: https://doi.org/10.70577/rps.v4i1.144

tiende a implicar tratamiento de datos de alto impacto, elevando exigencias de proporcionalidad y protección reforzada. Con el propósito de sistematizar la información analizada, en la Tabla 1 se presentan los principales tipos de datos personales tratados en los entornos virtuales universitarios, junto con los riesgos asociados y los enfoques de control recomendados conforme al marco normativo ecuatoriano.

Tabla 1

Tipos de datos tratados en entornos virtuales universitarios y riesgos típicos

Tipo de dato	Dónde se recolecta	Riesgos predominantes	Enfoque de control recomendado
Identificación y autenticación (usuario, correo, IP, MFA)	LMS, SSO, correo institucional	suplantación, accesos indebidos	Autenticación fuerte, gestión de identidades y accesos, trazabilidad y alertas (Pillajo & Avila, 2023).
Académicos (notas, expedientes, asistencia, historial)	SIS académico, LMS	exposición por errores de permisos, perfiles indebidos	Control de roles, minimización, retención justificada, auditorías (Vinueza et al., 2024).
Interacción y analítica (clics, tiempo, participación, foros)	LMS, analítica	vigilancia, perfilamiento excesivo	Limitación de finalidad, transparencia, evaluaciones de impacto (Morales et al., 2024)
Evaluación remota (video, audio, pantalla, metadatos)	proctoring, videoplataformas	intrusión, sesgos, “daño” reputacional	Proporcionalidad, alternativas menos invasivas, garantías y consentimiento válido (Flores, 2024).
Biometría (rostro, huella, patrones)	controles de acceso/proctoring	discriminación, irreversibilidad del daño	Protección reforzada, estricta necesidad, medidas técnicas y jurídicas (Pillajo & Avila, 2023).
Transferencias/terceros (cloud, proveedores)	servicios externos	fugas, transferencias internacionales no controladas	Contratos, evaluación de proveedores, reglas de transferencia y seguridad (Morales et al., 2024).

Nota. Elaboración bajo la información de (Flores, 2024; Morales et al., 2024; Pillajo & Avila, 2023; Vinueza et al., 2024).

Revista: Pulso Científico
ISSN: 3091-1958
DOI: https://doi.org/10.70577/rps.v4i1.144

Desafíos predominantes y estrategias efectivas de protección alineadas al marco ecuatoriano

La consolidación de los entornos virtuales en la educación superior ecuatoriana ha generado un escenario de alta dependencia tecnológica que incrementa de manera sustantiva el tratamiento de datos personales de los estudiantes. En este contexto, la Ley Orgánica de Protección de Datos Personales (2021) se configura como el eje normativo que orienta la gestión legítima, segura y responsable de la información personal, especialmente en instituciones universitarias que operan plataformas digitales para docencia, evaluación y administración académica. Sin embargo, la aplicación práctica de este marco legal enfrenta desafíos complejos que no se limitan al cumplimiento formal de la norma, sino que se vinculan con aspectos estructurales, culturales y tecnológicos.

Uno de los desafíos predominantes se relaciona con la gobernanza institucional de los datos personales. Ordóñez et al., (2022) señalan que, en las universidades, la gestión de la información suele encontrarse fragmentada entre unidades académicas, administrativas y tecnológicas, lo que dificulta la definición clara de responsabilidades y la aplicación homogénea de los principios de la LOPDP, como la legalidad, la finalidad y la minimización de datos. Esta dispersión organizativa debilita la capacidad institucional para demostrar cumplimiento normativo continuo, exigencia central del principio de responsabilidad proactiva establecido en la legislación ecuatoriana.

A ello se suma el desafío derivado de la tercerización de servicios tecnológicos, ya que gran parte de los entornos virtuales universitarios dependen de proveedores externos para el alojamiento de datos, la videoconferencia, la analítica del aprendizaje o la evaluación remota. Según Vásquez et al., (2026) advierten que esta dependencia incrementa los riesgos de accesos no autorizados, transferencias internacionales de datos sin garantías suficientes y usos incompatibles con las finalidades educativas originales, especialmente cuando los contratos con los encargados del tratamiento no desarrollan de forma explícita las obligaciones de confidencialidad, seguridad y supresión de datos.

Otro desafío relevante se manifiesta en la seguridad de la información en plataformas de aprendizaje virtual. Rosas y Pila (2023) evidencian que muchas vulneraciones de datos en el ámbito educativo no responden únicamente a fallos tecnológicos, sino a configuraciones inadecuadas, controles de acceso deficientes y falta de capacitación del personal y de los propios estudiantes. En el caso ecuatoriano, estos riesgos se intensifican cuando las instituciones no integran la seguridad de la información como un proceso transversal, sino como una respuesta reactiva ante incidentes, lo cual resulta contrario al enfoque preventivo promovido por la LOPDP.

De forma particular, la evaluación remota y el uso de tecnologías de supervisión digital, como el *e-proctoring*, constituyen uno de los puntos de mayor tensión entre innovación educativa y protección de derechos

Revista: Pulso Científico
ISSN: 3091-1958
DOI: https://doi.org/10.70577/rps.v4i1.144

fundamentales. De acuerdo a Angela et al., (2025) en educación superior latinoamericana sostienen que estas herramientas implican un tratamiento intensivo de datos personales, incluyendo imágenes, audio y metadatos del entorno del estudiante, lo que exige un análisis riguroso de proporcionalidad y necesidad para evitar prácticas de vigilancia excesiva o potencialmente discriminatorias. Desde la perspectiva de la LOPDP, este desafío interpela directamente al principio de minimización y al deber de garantizar que el tratamiento de datos no genere afectaciones indebidas a la dignidad y privacidad del estudiante.

Frente a estos desafíos, Hernández (2022) coincide en que las estrategias efectivas de protección de datos en entornos virtuales universitarios deben entenderse como un proceso integral y continuo, alineado de manera estricta al marco legal ecuatoriano. La evidencia académica resalta que la implementación de políticas institucionales claras, acompañadas de mecanismos de control y verificación permanente, fortalece la capacidad de las universidades para cumplir con el principio de responsabilidad demostrada y para generar confianza en la comunidad estudiantil. Estas estrategias no se limitan al plano normativo, sino que incorporan medidas técnicas y organizativas que permiten anticipar riesgos y reducir la probabilidad de incidentes de seguridad.

De esta manera, Lamounier (2023) subraya que la seguridad de la información por diseño y por defecto constituye una estrategia clave en la protección de datos personales en educación superior. Este enfoque implica que las plataformas y procesos académicos integren desde su concepción mecanismos de protección, tales como control de accesos, cifrado y gestión adecuada de permisos, en coherencia con los principios de la LOPDP y con las mejores prácticas internacionales en ciberseguridad educativa. De esta manera, la protección de datos deja de ser un requisito accesorio y se convierte en un componente estructural de la calidad institucional.

La formación y concienciación de la comunidad universitaria emerge como una estrategia transversal para enfrentar los desafíos identificados. Razza (2020) destaca que la educación digital en materia de privacidad y protección de datos contribuye significativamente a reducir riesgos asociados al error humano y a fortalecer la autodeterminación informativa de los estudiantes. Este enfoque resulta coherente con la LOPDP, que reconoce la educación digital como un elemento esencial para garantizar el ejercicio efectivo de los derechos de los titulares de datos en entornos tecnológicos. A fin de facilitar la comprensión del enfoque teórico adoptado, la Figura 1 resume la articulación entre la LOPDP, los principales desafíos en los entornos virtuales universitarios y las estrategias de protección de datos.

Revista: Pulso Científico
ISSN: 3091-1958
DOI: https://doi.org/10.70577/rps.v4i1.144

Figura 1

Articulación entre la LOPDP, los desafíos y las estrategias de protección en entornos virtuales universitarios

Nota. La figura integra el enfoque de responsabilidad proactiva y seguridad por diseño exigidos por la LOPDP en el contexto de la educación superior virtual.

Los desafíos predominantes en la protección de datos personales en entornos virtuales universitarios ecuatorianos evidencian la necesidad de una aplicación sustantiva y no meramente formal de la LOPDP. La articulación entre marco normativo, estrategias institucionales y cultura de protección de datos se presenta como un elemento clave para garantizar que la digitalización de la educación superior se desarrolle en armonía con los derechos fundamentales de los estudiantes.

Revista: Pulso Científico
ISSN: 3091-1958
DOI: https://doi.org/10.70577/rps.v4i1.144

MATERIALES Y MÉTODOS

La investigación se desarrolló bajo un enfoque cualitativo, con un diseño bibliográfico-documental, orientado al análisis sistemático de la producción científica relacionada con la protección de datos personales de estudiantes universitarios en entornos virtuales y su articulación con el marco legal ecuatoriano. Para garantizar la rigurosidad metodológica y la transparencia del proceso de revisión, se adoptó la metodología PRISMA, la cual permitió estructurar de manera ordenada las fases de identificación, selección, elegibilidad e inclusión de los estudios analizados.

Seguidamente, la búsqueda de información se realizó en bases de datos científicas de reconocido prestigio académico, entre las que se incluyeron Scopus, Web of Science, SciELO, Redalyc y Google Scholar, considerando publicaciones comprendidas entre los años 2022 y 2026. Para ello, se emplearon descriptores en español e inglés relacionados con la protección de datos personales, privacidad, educación superior y entornos virtuales, combinados mediante operadores booleanos, lo que permitió recuperar un total de 438 registros iniciales.

Posteriormente, una vez consolidada la base documental, se procedió a la eliminación de registros duplicados, lo que redujo el número de estudios a 346 documentos. A continuación, se efectuó el cribado de títulos y resúmenes, fase en la cual se excluyeron 214 registros por no presentar relación directa con el objeto de estudio, quedando 132 artículos para la revisión a texto completo.

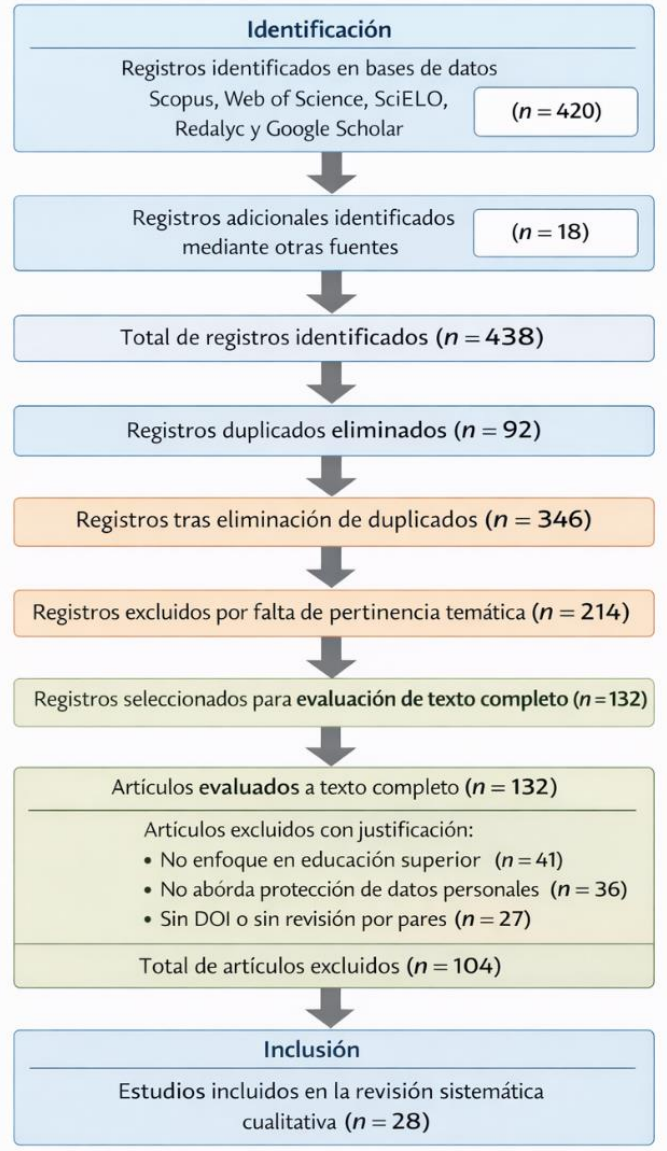
Luego, durante la fase de elegibilidad, se evaluaron exhaustivamente los textos completos de los estudios seleccionados, considerando criterios de pertinencia temática, enfoque en educación superior, disponibilidad de texto completo, revisión por pares y presencia de DOI verificable. Como resultado de esta evaluación, se excluyeron 104 artículos por no cumplir con los criterios establecidos, principalmente por no abordar de manera específica la protección de datos personales en entornos universitarios virtuales o por carecer de respaldo científico suficiente.

El proceso de selección culminó con la inclusión de 28 estudios científicos, los cuales conformaron el corpus definitivo de análisis. Este proceso se sintetiza gráficamente en la Figura 2, correspondiente al diagrama de flujo PRISMA, el cual evidencia de manera clara y secuencial las etapas seguidas desde la identificación inicial de los registros hasta la inclusión final de los estudios analizados, garantizando así la trazabilidad, coherencia y transparencia metodológica del estudio.

Revista: Pulso Científico
ISSN: 3091-1958
DOI: https://doi.org/10.70577/rps.v4i1.144

Figura 2

Diagrama de flujo PRISMA del proceso de selección de estudios



Nota. El diagrama muestra el proceso de identificación, selección y exclusión de los estudios analizados.

RESULTADOS Y DISCUSIÓN

El análisis de los 28 estudios científicos incluidos en la revisión sistemática, seleccionados mediante la metodología PRISMA, permitió identificar patrones consistentes en torno a los desafíos predominantes y a las estrategias efectivas para la protección de los datos personales de estudiantes universitarios en entornos

Revista: Pulso Científico
ISSN: 3091-1958
DOI: https://doi.org/10.70577/rps.v4i1.144

virtuales. Los resultados evidencian que la problemática no se circunscribe exclusivamente al ámbito tecnológico, sino que responde a una interacción compleja entre factores normativos, institucionales y culturales, lo cual coincide con lo señalado por Gutema (2023), quienes sostienen que la gobernanza de datos en educación superior requiere un enfoque sistémico y transversal.

En términos cuantitativos, el análisis estadístico descriptivo de la literatura revisada muestra que el desafío más recurrente es la debilidad en la gobernanza institucional de los datos, identificado en 21 de los 28 estudios analizados. Esta situación se asocia a la ausencia de políticas internas claras, a la dispersión de responsabilidades entre áreas académicas y administrativas, y a la limitada articulación entre unidades de tecnología y autoridades universitarias. Tales resultados coinciden con lo expuesto por Jiménez (2024), quien afirma que la falta de estructuras formales de gobernanza digital incrementa el riesgo de incumplimiento normativo en instituciones públicas y educativas.

Tabla 2

Frecuencia de desafíos identificados en la literatura científica (n = 28)

Desafío predominante	Frecuencia absoluta	(%)
Gobernanza institucional fragmentada	21	75,0
Dependencia de proveedores tecnológicos	19	67,9
Brechas de seguridad de la información	17	60,7
Evaluación remota con alta intrusión	15	53,6
Cultura digital limitada en privacidad	14	50,0

Nota. Los estadísticos se calcularon a partir de la frecuencia de aparición de cada desafío en los estudios incluidos (n = 28), con el fin de describir su tendencia central y variabilidad dentro de la literatura analizada.

Los resultados también evidencian que la dependencia de proveedores tecnológicos externos constituye un desafío crítico, especialmente en contextos donde las universidades utilizan plataformas de terceros para videoconferencias, almacenamiento en la nube y evaluación en línea. Estudios recientes de Molina y Pachano (2025) advierten que la externalización de servicios digitales sin controles contractuales robustos puede derivar en transferencias de datos no transparentes y en usos incompatibles con las finalidades educativas, situación que entra en tensión directa con los principios de finalidad y confidencialidad establecidos en la normativa ecuatoriana.

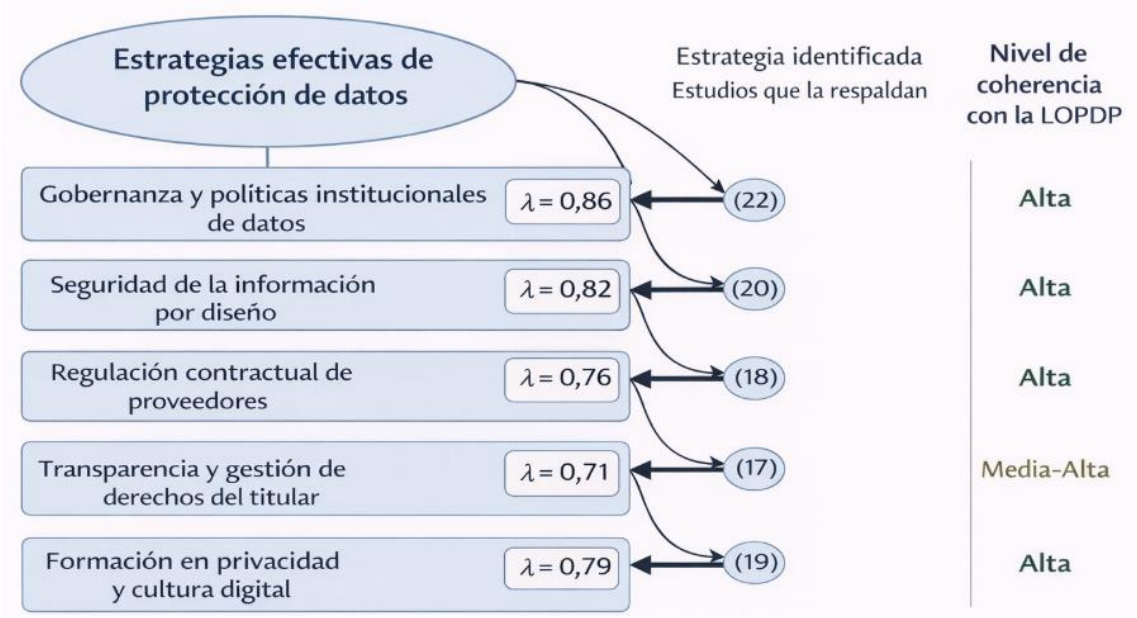
Revista: Pulso Científico
ISSN: 3091-1958
DOI: https://doi.org/10.70577/rps.v4i1.144

Otro hallazgo relevante se relaciona con la seguridad de la información, identificada como problemática en más del sesenta por ciento de los estudios analizados. La literatura señala que las vulnerabilidades técnicas se ven agravadas por prácticas inadecuadas de los usuarios, como el uso de contraseñas débiles o la compartición indiscriminada de credenciales, lo que coincide con los planteamientos de Villa et al., (2023), quienes destacan que el factor humano sigue siendo determinante en los incidentes de seguridad digital en entornos educativos.

Por su parte, el uso de tecnologías de evaluación remota, particularmente aquellas basadas en monitoreo audiovisual, aparece como uno de los temas más controvertidos en la revisión. Los estudios revisados advierten que estas prácticas pueden generar afectaciones a la privacidad y al bienestar psicológico del estudiante, especialmente cuando no se aplican criterios claros de necesidad y proporcionalidad. En este sentido, Jara et al., (2024) sostienen que las instituciones de educación superior deben equilibrar la integridad académica con el respeto a los derechos fundamentales, adoptando enfoques éticos y jurídicamente compatibles con los marcos de protección de datos.

Figura 3

Estrategias efectivas analizadas en los estudios revisados



Nota. El diagrama muestra los pesos factoriales estandarizados (λ) de las estrategias efectivas identificadas, reflejando su contribución relativa al modelo y su coherencia con la Ley Orgánica de Protección de Datos Personales del Ecuador.

Revista: Pulso Científico
ISSN: 3091-1958
DOI: https://doi.org/10.70577/rps.v4i1.144

En cuanto a las estrategias efectivas, los resultados muestran una alta coincidencia en la literatura respecto a la necesidad de implementar mecanismos de responsabilidad proactiva, entendida como la capacidad institucional de anticipar riesgos y demostrar cumplimiento normativo. Autores como Quijije y Moreira (2025) destacan que este enfoque fortalece la legitimidad institucional y reduce la probabilidad de sanciones legales, especialmente en sectores intensivos en datos como la educación superior.

De esta manera, la seguridad de la información por diseño y por defecto se posiciona como una estrategia central, al permitir que los sistemas virtuales integren controles de privacidad desde su concepción. Esta aproximación resulta coherente con los principios de la LOPDP y con los planteamientos de Barzola y Núñez (2025), quienes sostienen que la protección de datos debe incorporarse como un criterio estructural de calidad en los sistemas digitales.

De igual forma, la literatura revisada subraya la importancia de la educación digital en privacidad, tanto para estudiantes como para docentes, como una estrategia transversal que contribuye a la reducción de riesgos derivados del desconocimiento normativo y técnico. Según Villa et al., (2023), la alfabetización en protección de datos fortalece la autodeterminación informativa y mejora la capacidad de los usuarios para ejercer sus derechos en entornos digitales complejos.

CONCLUSIONES

Los resultados del estudio evidencian que los desafíos predominantes en la protección de los datos personales de los estudiantes universitarios en entornos virtuales no derivan de la ausencia de un marco normativo, sino de limitaciones en su aplicación práctica, especialmente en lo relacionado con la gobernanza institucional de la información, la gestión de proveedores tecnológicos y la seguridad de los entornos digitales, lo que incrementa el riesgo de vulneración de derechos fundamentales.

El análisis de la literatura científica demuestra que las estrategias efectivas de protección de datos, tales como la responsabilidad proactiva, la seguridad de la información por diseño, la regulación contractual de los encargados del tratamiento y la educación digital en privacidad, presentan una alta coherencia con la Ley Orgánica de Protección de Datos Personales del Ecuador, consolidándose como elementos clave para garantizar el tratamiento legítimo y seguro de la información estudiantil en la educación superior virtual.

Además, la protección de los datos personales en entornos virtuales universitarios requiere un enfoque integral y sostenido que articule el cumplimiento legal con capacidades institucionales y cultura organizacional, de modo que la aplicación efectiva del marco ecuatoriano contribuya no solo a la mitigación de riesgos, sino también al fortalecimiento de la confianza, la transparencia y la calidad del proceso educativo en la educación superior digital.

REFERENCIAS BIBLIOGRÁFICAS

Álvarez, C. J. A., & Hernández, S. G. P. (2024). Protección de Datos Personales en Plataformas Educativas Digitales en el Sistema de Educación Superior de Ecuador. *MQRInvestigar, 8*(3), 5324–5339. https://doi.org/10.56048/MQR20225.8.3.2024.5324-5339

Angela, J. B. Q., Anyie, M. F. C., Marco, A. J. V., & Zamora, M. D. J. (2025). La Protección de Datos Personales en el Gobierno Electrónico y Desafíos para la Gestión Pública. *Revista Veritas de Difusão Científica*, *6*(1), 1029–1046. https://doi.org/10.61616/RVDC.V6I1.447

Barzola, P. Y. G., & Núñez, R. R. A. (2025). Desafíos legales en la protección de datos personales en la era digital. *Multidisciplinary Collaborative Journal*, *3*(1), 31–43. https://doi.org/10.70881/MCJ/V3/N1/44

Flores, Z. C. E. (2024). Revisión sistemática de la literatura sobre las tecnologías de e-proctoring para la supervisión de exámenes en educación superior: Entre la innovación y el daño. *Perfiles Educativos*, *46*(185), 90–110. https://doi.org/10.22201/IISUE.24486167E.2024.185.61323

Gutema, D. (2023). *Prácticas de gobernanza de datos en instituciones de educación superior: oportunidades y desafíos*. https://www.doria.fi/handle/10024/187361

Hernández, P. J. C. (2022). Campañas electorales, big data y perfilado ideológico. Aproximación a su problemática desde el derecho fundamental a la protección de datos. *Revista Española de Derecho Constitucional*, *0*(124), 41–73. https://doi.org/10.18042/cepc/redc.124.02

Jara, V. F. L., Villa, E. I. C., Solorzano, C. A. J., & Rodríguez, H. S. P. (2024). Desafíos actuales ante la integración de las TIC y estrategias empresariales en la educación superior. *Simbiosis*, *4*(7), 59–72. https://doi.org/10.59993/SIMBIOSIS.V4I7.38

Jiménez, J. M. (2024). Seguridad y Privacidad en el Tiempo Digital, la Era de la Información Liquida. *Ciencia Latina Revista Científica Multidisciplinar*, *8*(2), 7399–7420. https://doi.org/10.37811/CL_RCM.V8I2.11136

Lamounier, H. H. (2023). La autoridad nacional de protección de datos bajo la perspectiva del análisis costo-beneficio. *Revista de Derecho Público*, (98). https://doi.org/10.5354/0719-5249.2023.71322

Ley Orgánica de Protección de Datos Personales (2021). www.lexis.com.ec

Liu, Q., & Khalil, M. (2023). Comprender las cuestiones de privacidad y protección de datos en el análisis del aprendizaje mediante una revisión sistemática. *British Journal of Educational Technology*, *54*(6), 1715–1747. https://doi.org/10.1111/BJET.13388

Marín, V. I., & Tur, G. (2023). La privacidad de los datos en Tecnología Educativa: resultados de una revisión de alcance. *Edutec, Revista Electrónica de Tecnología Educativa*, *83*(83), 7–23. https://doi.org/10.21556/edutec.2023.83.2701

Molina, N. K. E., & Pachano, Z. A. C. (2025). La protección de datos personales en el entorno digital ecuatoriano: análisis crítico del marco normativo y su aplicación práctica. *Sociedad & Tecnología*, *8*(S3), 1053–1066. https://doi.org/10.51247/ST.V8IS3.350

Morales, E. D. A., Morales, A. F. P., Cajamarca, A. E. E., & Intriago, U. F. J. (2024). La protección de datos personales en Ecuador: evolución legislativa y comparación con modelos regionales en Sudamérica. *Perspectivas Sociales y Administrativas*, *2*(2), 35–44. https://doi.org/10.61347/PSA.V2I2.70

Mutimukwe, C., Viberg, O., Oberg, L. M., & Cerratto-Pargman, T. (2022). Preocupaciones de los estudiantes sobre la privacidad en el análisis del aprendizaje: desarrollo de modelos. *British Journal of Educational Technology*, *53*(4), 932–951. https://doi.org/10.1111/BJET.13234

Ordóñez, P. L., Correa, Q. L., & Correa, C. A. (2022). Políticas públicas y protección de datos personales en Ecuador: reflexiones desde la emergencia sanitaria. *Estado & Comunes*, *2*(15), 77–97. https://doi.org/10.37228/estado_comunes.v2.n15.2022.270

Organización de las Naciones Unidas para la Educación, la C. y la C. (2023). Informe de seguimiento de la educación en el mundo, 2023: la tecnología en la educación: ¿una herramienta en los términos de quién? In *Global Education Monitoring Report 2023: Technology in education: A tool on whose terms?* GEM Report UNESCO. https://doi.org/10.54676/UZQV8501

Pillajo, G. P. A., & Avila, P. D. (2023). Análisis de ciberseguridad en plataformas e-learning: revisión sistemática de la literatura. *Revista Perspectivas*, *5*(1), 19–29. https://doi.org/10.47187/PERSPECTIVAS.5.1.179

Quijije, M. C., & Moreira, S. W. (2025). Seguridad y privacidad de los datos en la era de la información en el Ecuador. *INNOVATION & DEVELOPMENT IN ENGINEERING AND APPLIED SCIENCES*, *7*(2), 13–13. https://doi.org/10.53358/IDEAS.V7I2.1287

Razza, C. (2020). Transferencia internacional de datos personales en Latinoamérica. *Revista Cálamo*, (13), 34–52. https://doi.org/10.61243/CALAMO.13.158

Rosas, L. G., & Pila, C. G. (2023). La protección de datos personales en Ecuador: Una revisión histórica-normativa de este derecho fundamental en el país suramericano. *VISUAL REVIEW. International Visual Culture Review / Revista Internacional de Cultura Visual*, *13*(2), 1–16. https://doi.org/10.37467/revvisual.v10.4568

Secretaría de Educación Superior, C. T. e I. (2022). *Registro de Matrícula*. https://siau.senescyt.gob.ec/universidades-y-escuelas-politecnicas-matriculas/

Svetec, B., & Divjak, B. (2021). Análisis de aprendizaje confiable para ecosistemas de aprendizaje inteligentes. *Journal of Learning Analytics*, *8*(3), 81–100. https://doi.org/10.18608/JLA.2021.7379

Vásquez, C. L. H., Aguas, V. J. F., Villota, O. W. R., Tacle, H. P. M., & Tapia, R. C. S. (2026). Artificial Intelligence in Higher Education 5.0: Ethical Implications, Pedagogical Innovation and Personalized Learning. *Data and Metadata*, *5*, 1295–1295. https://doi.org/10.56294/DM20261295

Villa, Q. M., Cadena, M. J., Gavilanez, G. A., & Centeno, A. C. (2023). Protección de Datos Personales en Ecuador y Colombia: Principios, Ética y Desafíos Actuales. *Revista Científica de Informática ENCRIPTAR - ISSN: 2737-6389.*, *6*(11), 19–34. https://doi.org/10.56124/ENCRIPTAR.V6I11.0002

Vinueza, O. N. V., Macías, Á. M. Á., & Maldonado, M. R. L. (2024). Implementación de medidas de seguridad y principio de conservación de datos según la ley orgánica de protección de datos personales en instituciones públicas de Babahoyo, Ecuador. *Dilemas Contemporáneos: Educación, Política y Valores*. https://doi.org/10.46377/DILEMAS.V11I2.4080

Conflicto de intereses:

Los autores declaran que no existe conflicto de interés posible.

Financiamiento:

No existió asistencia financiera de partes externas al presente artículo.

Nota:

El artículo no es producto de una publicación anterior.