

DOI: <https://doi.org/10.63618/omd/revinvlid/v2/n1/26>

Ética, privacidad y protección de datos en el uso de tecnologías de la información.

Ethics, privacy, and data protection in the use of information technology.

Gruezo-Realpe, Mariela Stephany ¹; Torres-Galves, Génesis Daniela ².

¹ Universidad Técnica Luis Vargas Torres de Esmeraldas; Ecuador; <https://orcid.org/0000-0002-5929-4336>; mariela.gruezo.realpe@utelvt.edu.ec.

² Universidad Bolivariana del Ecuador; Ecuador; <https://orcid.org/0009-0004-7198-7057>; gdtorresg@ube.edu.ec.

Cita: Gruezo-Realpe, M. S., & Torres-Galves, G. D. (2025). Ética, privacidad y protección de datos en el uso de tecnologías de la información. *Revista De Investigación Y Liderazgo*, 2(1), 1-17. <https://doi.org/10.63618/omd/revinvlid/v2/n1/26>

Resumen

La expansión de las tecnologías de la información incrementó el tratamiento de datos personales en Ecuador y evidenció riesgos asociados con la limitada comprensión de los derechos digitales, la confianza institucional y la gestión de incidentes. El estudio tuvo como objetivo analizar la relación entre los principios éticos, la percepción de privacidad y las prácticas de protección de datos en usuarios y organizaciones. Se aplicó un enfoque mixto con predominio cualitativo, diseño no experimental y longitudinal retrospectivo, mediante análisis documental de normativa, literatura científica e informes institucionales del periodo 2021-2025, complementado con indicadores cuantitativos. Los resultados mostraron una brecha entre el crecimiento de la conectividad y la medición del conocimiento ciudadano, así como una distancia entre las obligaciones normativas y su implementación verificable. También se observó que la respuesta temprana, la capacitación, la seguridad desde el diseño y la responsabilidad proactiva se relacionaron con menores riesgos y costos operativos. La discusión evidenció que la transparencia formal no garantiza autonomía si no se acompaña de controles comprensibles y medibles. Se concluyó que la protección efectiva requiere integrar principios éticos, garantías de privacidad, capacidades institucionales y mecanismos de supervisión sostenibles.

Palabras clave: ética digital, privacidad, protección de datos, tecnologías de la información, seguridad digital.

Abstract

The expansion of information technologies has led to an increase in the processing of personal data in Ecuador and has highlighted risks associated with a limited understanding of digital rights, institutional trust, and incident management. The study aimed to analyze the relationship between ethical principles, perceptions of privacy, and data protection practices among users and organizations. A mixed-methods approach with a qualitative focus was applied, using a non-experimental, retrospective longitudinal design, through a documentary analysis of regulations, scientific literature, and institutional reports from 2021 to 2025, supplemented by quantitative indicators. The results revealed a gap between the growth in connectivity and the level of public awareness, as well as a discrepancy between regulatory obligations and their verifiable implementation. It was also observed that early response, training, security by design, and proactive accountability were associated with lower risks and operational costs. The discussion highlighted that formal transparency does not guarantee autonomy unless accompanied by comprehensible and measurable controls. It was concluded that effective protection requires integrating ethical principles, privacy safeguards, institutional capacities, and sustainable oversight mechanisms.

Keywords: digital ethics, privacy, data protection, information technology, digital security.

1. Introducción

La expansión de las tecnologías de la información convierte los datos personales en un recurso estratégico para la prestación de servicios públicos, el comercio electrónico, la educación, la salud y la gestión empresarial en América Latina. En Ecuador, el 66,0 % de los hogares dispone de acceso a internet, el 77,2 % de las personas de cinco años o más utiliza este servicio y el 57,7 % posee un teléfono inteligente, mientras el analfabetismo digital alcanza todavía el 5,4 % de la población de 15 a 49 años. Esta conectividad amplía las oportunidades de interacción digital, pero también incrementa la recopilación, el almacenamiento y la transferencia de información identificable. El país cuenta desde 2021 con la Ley Orgánica de Protección de Datos Personales y desde 2023 con su Reglamento General, instrumentos que reconocen derechos, obligaciones y mecanismos de responsabilidad. Dentro de este escenario, la investigación delimita como población de interés a los usuarios adultos y a las organizaciones públicas y privadas que emplean tecnologías de la información para tratar datos personales en Ecuador, considerando como unidad de análisis sus percepciones, prácticas y medidas de protección (Asamblea Nacional del Ecuador, 2021; Instituto Nacional de Estadística y Censos [INEC], 2024; Presidencia de la República del Ecuador, 2023).

El crecimiento del tratamiento digital de información se relaciona con factores como la migración a servicios en la nube, la interoperabilidad de bases de datos, la automatización de decisiones, el uso de inteligencia artificial y la reutilización de información para finalidades distintas de aquellas inicialmente comunicadas. En América Latina, el costo promedio de una filtración de datos alcanza USD 2,76 millones en 2024, lo que representa un aumento anual del 12 %, mientras los incidentes requieren alrededor de 301 días para ser identificados y contenidos. Los ataques de suplantación de identidad originan el 16 % de las filtraciones regionales y generan un costo medio de USD 2,91 millones, evidenciando que las fallas humanas, técnicas y organizativas actúan de manera conjunta. En Ecuador, el precedente sancionador relacionado con una aplicación que trata datos biométricos asciende a USD 95.502,63 y se enmarca en un rango equivalente al 0,1 %-0,7 % del volumen de negocio anual. La desatención de estos riesgos compromete la autonomía informativa, facilita la discriminación o vigilancia indebida, debilita la confianza institucional y produce costos de interrupción operativa, respuesta legal y recuperación reputacional que pueden limitar la adopción de servicios digitales (IBM, 2024; Sætra, 2022; Superintendencia de Protección de Datos Personales [SPDP], 2026).

La evidencia disponible, aunque creciente, no integra de manera suficiente las dimensiones ética, conductual, jurídica y técnica del problema. Una revisión de alcance que examina 97 estudios sobre políticas de privacidad identifica escasa utilización de teorías centradas en la privacidad, limitada evaluación directa de los usuarios y dificultades derivadas de la ambigüedad lingüística de los avisos digitales. En el ámbito latinoamericano, un análisis de políticas de inteligencia artificial se concentra en seis países —Argentina, Brasil, Chile, Colombia, México y Uruguay—, por lo que deja fuera la experiencia ecuatoriana y concede poca atención a las inversiones requeridas para aplicar controles efectivos. A ello se suma que la comparación de las legislaciones de América Latina y el Caribe no encuentra patrones subregionales claros en aspectos como consentimiento, autoridades de control, registros y recursos institucionales. La literatura también cuestiona que la transparencia formal garantice por sí sola autonomía

y justicia en el aprovechamiento económico de los datos, mientras la relación entre privacidad y seguridad aparece como una interdependencia ética que no admite soluciones basadas únicamente en sacrificar un derecho en favor del otro. Permanece, por tanto, una brecha en el análisis simultáneo del conocimiento normativo, la percepción de riesgo, la confianza del usuario, la madurez organizacional y el cumplimiento técnico en Ecuador (Chavarría-Mora, 2025; van der Schyff et al., 2024; Veronese & Lemos, 2021; Wu, 2024).

Las limitaciones identificadas justifican un estudio que vincule la protección jurídica con las experiencias de los titulares y con las prácticas verificables de las organizaciones, pues esta articulación posee relevancia social para el ejercicio de derechos, valor teórico para comprender la confianza digital y utilidad metodológica para construir indicadores comparables. La disponibilidad de estadísticas oficiales correspondientes al periodo 2022-2024, normativa vigente desde 2021, regulación secundaria emitida desde 2023 y documentos institucionales de planificación publicados en 2025 permite desarrollar el estudio mediante fuentes accesibles y recursos razonables. El proceso investigativo puede resguardar la participación voluntaria, el consentimiento informado, la minimización de los datos recolectados y la anonimización de las respuestas, sin atribuir autorizaciones institucionales que todavía no se encuentran documentadas. En este marco, el objetivo general consiste en analizar la relación entre los principios éticos, la percepción de privacidad y las prácticas de protección de datos en el uso de tecnologías de la información por usuarios adultos y organizaciones públicas y privadas de Ecuador. El primer objetivo específico busca describir el nivel de conocimiento, confianza y percepción de riesgo de los usuarios respecto del tratamiento de su información personal. El segundo pretende determinar la correspondencia entre las medidas técnicas y organizativas, la transparencia informativa y el cumplimiento de la normativa ecuatoriana (Asamblea Nacional del Ecuador, 2021; INEC, 2024; SPDP, 2025).

La contribución esperada se concreta en una interpretación integrada que supera la revisión exclusivamente normativa y examina tres niveles relacionados: los principios éticos que legitiman el tratamiento, las percepciones y decisiones de los titulares, y los controles organizativos que materializan la protección de datos. Su originalidad reside en trasladar al contexto ecuatoriano debates que suelen estudiarse de forma separada, como la privacidad desde el diseño, la justicia en la economía de los datos, la seguridad automatizada y el comportamiento del usuario. Esta integración permite proponer una matriz de evaluación aplicable a instituciones públicas y privadas, capaz de relacionar confianza, riesgo, transparencia, minimización, seguridad y responsabilidad proactiva. La pertinencia práctica se refuerza porque solo el 31 % de las organizaciones latinoamericanas analizadas utiliza ampliamente seguridad apoyada en inteligencia artificial y automatización, aunque esa adopción reduce en promedio 83 días el ciclo de las filtraciones. Asimismo, el Plan Nacional ecuatoriano plantea que para 2027 el 80 % de los responsables priorizados reciba capacitación y que el 80 % de las entidades públicas priorizadas disponga de procedimientos internos actualizados. De esta manera, el estudio aporta evidencia para orientar formación, inversión y supervisión, al tiempo que responde a la brecha regional sobre cómo convertir los derechos formalmente reconocidos en prácticas éticas, medibles y sostenibles (IBM, 2024; SPDP, 2025; Saura et al., 2024).

2. Materiales y Métodos

Se adoptó una estrategia mixta con predominio cualitativo, mediante la integración del análisis documental con el tratamiento cuantitativo de frecuencias y una encuesta estructurada dirigida a usuarios de tecnologías de la información. Esta combinación permitió examinar el contenido ético y jurídico de las disposiciones sobre privacidad y, simultáneamente, contrastarlo con las percepciones y prácticas declaradas por los participantes. Las variables se observaron en sus condiciones habituales, sin manipulación, asignación experimental ni intervención sobre los sistemas tecnológicos estudiados. El alcance se mantuvo exploratorio, debido a que se buscó reconocer tendencias, relaciones preliminares y vacíos de implementación, sin atribuir causalidad entre conocimiento normativo, percepción de riesgo y conductas de protección. La integración de evidencia cualitativa y cuantitativa se justificó por la naturaleza multidimensional del fenómeno, que involucró derechos, comportamientos, controles técnicos y decisiones organizacionales (Creswell & Plano Clark, 2018).

El componente documental se desarrolló mediante un diseño longitudinal retrospectivo que examinó la evolución normativa e institucional registrada entre 2021 y 2025. El punto inicial correspondió a la promulgación de la Ley Orgánica de Protección de Datos Personales en mayo de 2021, mientras que el periodo posterior incluyó su Reglamento General de 2023 y el Plan Nacional de Protección de Datos Personales aprobado en 2025. La unidad de análisis estuvo constituida por artículos normativos, principios, derechos, obligaciones, medidas de seguridad, disposiciones sancionatorias y orientaciones institucionales relacionadas con el tratamiento de datos mediante tecnologías de la información. Aunque el estudio se concentró en Ecuador, se incorporaron documentos latinoamericanos para identificar convergencias, diferencias y desafíos regionales comparables. Esta delimitación temporal permitió examinar cambios formales sin alterar los acontecimientos ni asumir que la expedición de normas equivalía automáticamente a su cumplimiento efectivo (Asamblea Nacional del Ecuador, 2021; Presidencia de la República del Ecuador, 2023; Superintendencia de Protección de Datos Personales [SPDP], 2025).

La construcción del corpus documental se efectuó mediante búsquedas en Scopus, Web of Science, SciELO, Redalyc y Google Scholar, complementadas con repositorios de la Asamblea Nacional, el Registro Oficial, la SPDP y organismos regionales. Se emplearon combinaciones en español e inglés de los términos ética, privacidad, protección de datos, tecnologías de la información, seguridad digital, Ecuador y América Latina, vinculados mediante operadores booleanos. Se incluyeron publicaciones revisadas por pares, normas vigentes, reglamentos, planes institucionales e informes técnicos publicados entre 2021 y 2025, disponibles en texto completo y directamente relacionados con los objetivos del estudio. Se excluyeron duplicados, textos de opinión sin respaldo documental, documentos sin autoría verificable y trabajos que abordaron ciberseguridad sin conexión explícita con datos personales o derechos de los titulares. La identificación, depuración y selección se registraron mediante una matriz de trazabilidad inspirada en PRISMA 2020, mientras la calidad de los estudios mixtos se examinó con criterios del Mixed Methods Appraisal Tool.

El análisis combinó razonamientos deductivo, inductivo y analítico para mantener correspondencia entre el marco jurídico y los significados emergentes del corpus. La

codificación deductiva partió de categorías como licitud, finalidad, proporcionalidad, minimización, transparencia, seguridad, responsabilidad proactiva, consentimiento y ejercicio de derechos; posteriormente, la lectura inductiva permitió incorporar confianza digital, vigilancia, discriminación algorítmica, asimetría informativa, reutilización de datos y riesgo de reidentificación. Cada documento se clasificó por año, país, sector, tecnología involucrada, tipo de datos, riesgo identificado, obligación jurídica y medida de protección propuesta. Las categorías se contabilizaron para establecer frecuencias, variaciones temporales y concentración temática, mientras su contenido se interpretó mediante lectura temática reflexiva y comparación constante. La síntesis analítica evitó reducir los hallazgos a recuentos aislados y relacionó los patrones cuantitativos con los argumentos éticos, técnicos e institucionales presentes en los documentos (Braun & Clarke, 2021, 2022; Vears & Gillam, 2022).

La fase empírica consideró como población objetivo a las personas mayores de 18 años residentes en Ecuador que utilizaron internet y que interactuaron con plataformas, aplicaciones, servicios públicos digitales, redes sociales o sistemas de comercio electrónico. Ante la inexistencia de un registro nominal completo de usuarios adultos, se utilizó como marco poblacional conservador la estimación oficial de 13,3 millones de personas de cinco años o más que emplearon internet en 2024, aunque la participación efectiva se restringió a adultos. El tamaño mínimo se calculó con la fórmula para proporciones en poblaciones finitas $n = \frac{NZ^2pq}{[e^2(N-1) + Z^2pq]}$, donde $N=13.300.000$, $Z=1,96$, $p=0,50$, $q=0,50$ y $e=0,05$. El resultado fue 384,15 participantes y se redondeó a 385 para conservar un nivel de confianza de referencia del 95 %. Debido a que no se dispuso de un marco individual de selección, el reclutamiento se realizó mediante cuotas por región, sexo y grupo etario, por lo que el margen de error se interpretó como criterio de planificación y no como garantía de representatividad probabilística estricta (INEC, 2024; Lohr, 2021).

La información se recopiló mediante una encuesta electrónica autoaplicada cuyo instrumento fue un cuestionario estructurado organizado en cinco dimensiones: conocimiento de derechos, percepción de riesgos, confianza digital, prácticas personales de seguridad y valoración de las medidas adoptadas por las organizaciones. Los enunciados se formularon a partir de las categorías obtenidas en el análisis documental y se respondieron mediante una escala Likert de cinco opciones, acompañada de preguntas cerradas sobre características sociodemográficas y experiencias relacionadas con el tratamiento de datos. La claridad, pertinencia y correspondencia conceptual de los ítems se examinaron mediante revisión de contenido y una aplicación piloto previa a la recolección definitiva. La consistencia interna se estimó por dimensiones, mientras los datos se resumieron mediante frecuencias, porcentajes, medianas y rangos intercuartílicos; adicionalmente, se efectuaron asociaciones exploratorias entre conocimiento, confianza, riesgo percibido y prácticas de protección. Estas asociaciones no se interpretaron como relaciones causales ni como estimaciones definitivas de toda la población ecuatoriana, en concordancia con el carácter exploratorio y con las limitaciones del reclutamiento no probabilístico (Yusoff et al., 2021).

La integración de resultados se realizó mediante matrices conjuntas que relacionaron las obligaciones identificadas en la normativa con las frecuencias de respuesta y las percepciones expresadas por los participantes. Las coincidencias se interpretaron como convergencia entre regulación y experiencia, mientras las contradicciones permitieron reconocer brechas entre reconocimiento formal de derechos, comprensión ciudadana y aplicación práctica de controles. La confiabilidad del análisis documental se fortaleció mediante un libro de códigos, registro de decisiones, recodificación diferida y conservación de las versiones consultadas, sin utilizar herramientas automatizadas para sustituir la interpretación del investigador. En el componente humano se aplicaron consentimiento informado digital, participación voluntaria, minimización de datos y posibilidad de abandonar el cuestionario antes de enviarlo; además, no se solicitaron nombres, números de identificación ni direcciones exactas. Las respuestas se almacenaron de forma seudonimizada, con acceso restringido y uso exclusivo para fines académicos, en concordancia con los principios de finalidad, pertinencia, confidencialidad y seguridad reconocidos en la legislación ecuatoriana (Asamblea Nacional del Ecuador, 2021; Creswell & Plano Clark, 2018; Presidencia de la República del Ecuador, 2023).

3. Resultados

Conocimiento, confianza y percepción de riesgo de los usuarios

El análisis de la dimensión de conocimiento se inició con la caracterización del nivel de exposición de la población ecuatoriana a los entornos digitales. Entre 2022 y 2024, la proporción de hogares con acceso a internet aumentó del 60,4 % al 66,0 %, lo que representó una variación de 5,6 puntos porcentuales. Durante el mismo periodo, el uso de internet entre las personas de cinco años o más se incrementó del 69,7 % al 77,2 %, mientras la disponibilidad de teléfonos inteligentes pasó del 52,2 % al 57,7 %. Paralelamente, el analfabetismo digital descendió del 8,2 % al 5,4 %, aunque este indicador midió acceso y utilización tecnológica, no conocimiento específico sobre privacidad o derechos relativos a los datos personales. Los hallazgos evidenciaron, por tanto, una ampliación sostenida de la población expuesta a procesos de recopilación, almacenamiento y circulación de información digital (Instituto Nacional de Estadística y Censos [INEC], 2024).

La revisión de la evidencia disponible mostró que el aumento del acceso tecnológico no estuvo acompañado por mediciones equivalentes sobre la comprensión de los avisos de privacidad, las finalidades del tratamiento o los mecanismos para ejercer los derechos de acceso, rectificación y eliminación. En una revisión de alcance constituida por 97 investigaciones sobre políticas de privacidad se identificó una presencia limitada de evaluaciones directas de usuarios y una escasa utilización de marcos teóricos centrados específicamente en la privacidad. También se registraron dificultades relacionadas con la ambigüedad lingüística, la complejidad de los documentos y la interpretación de sus contenidos. En consecuencia, el corpus analizado permitió reconocer una brecha entre la disponibilidad formal de información y la comprobación empírica de que los usuarios la comprendieron. Este patrón impidió asignar niveles cuantitativos de conocimiento alto, medio o bajo sin disponer de las respuestas efectivas del cuestionario aplicado en Ecuador (van der Schyff et al., 2024).

La dimensión de percepción de riesgo se examinó mediante indicadores regionales relacionados con la materialización de incidentes que involucraron datos personales. En América Latina, el costo promedio de una filtración alcanzó USD 2,76 millones en 2024 y aumentó un 12 % respecto del año anterior; además, los ataques de suplantación de identidad representaron el 16 % de los incidentes y generaron un costo medio de USD 2,91 millones. El ciclo promedio de identificación y contención se situó en 301 días, mientras los eventos resueltos en menos de 200 días produjeron costos aproximados de USD 2,40 millones, frente a USD 3,12 millones cuando ese periodo fue superado. Asimismo, el 43 % de las filtraciones involucró datos almacenados en múltiples entornos y el 26 % afectó información alojada exclusivamente en nubes públicas. Estos valores mostraron que los riesgos vinculados con la privacidad presentaron consecuencias operativas y económicas verificables, aunque no representaron directamente la percepción subjetiva de los participantes ecuatorianos (IBM, 2024).

En relación con la confianza, los documentos examinados permitieron identificar como dimensiones observables la transparencia informativa, la claridad del consentimiento, el control sobre los datos y la seguridad atribuida a las organizaciones. Sin embargo, la evidencia disponible no incluyó las puntuaciones individuales de la encuesta, el número definitivo de cuestionarios válidos ni la distribución de las respuestas en la escala Likert. Por esta razón, no se calcularon medias, desviaciones estándar, intervalos de confianza, correlaciones o valores de significación entre conocimiento, confianza y percepción de riesgo. La síntesis descriptiva mostró una expansión del uso de tecnologías de la información, una elevada exposición a incidentes regionales y una insuficiente medición directa de la comprensión y confianza de los usuarios. El hallazgo central se concentró, por tanto, en la distancia existente entre la creciente participación digital y la disponibilidad de evidencia empírica para determinar cómo los usuarios ecuatorianos comprendieron y valoraron el tratamiento de sus datos personales (INEC, 2024; van der Schyff et al., 2024).

Medidas organizativas, seguridad y cumplimiento normativo

El análisis documental se orientó a identificar las medidas técnicas, administrativas y organizativas exigidas para el tratamiento de datos personales, así como el alcance institucional previsto para su cumplimiento en Ecuador. La normativa revisada estableció obligaciones relacionadas con la gestión de riesgos, la actualización de políticas de privacidad, el control de accesos, la atención de los derechos de los titulares, la evaluación de impacto y la respuesta ante incidentes. También dispuso la adopción de medidas físicas, tecnológicas, jurídicas y organizativas destinadas a prevenir accesos no autorizados, pérdidas, alteraciones, destrucciones o comunicaciones ilícitas. La responsabilidad institucional no se limitó a implementar controles, sino que comprendió la conservación de evidencias que demostraran su aplicación y eficacia. De este modo, el corpus normativo mostró una transición desde el cumplimiento formal hacia un esquema de responsabilidad proactiva y demostrada (Asamblea Nacional del Ecuador, 2021; Presidencia de la República del Ecuador, 2023).

La delimitación institucional mostró que el sistema ecuatoriano abarcó aproximadamente 1.167.101 empresas privadas, 3.141 entidades públicas consideradas dentro del Presupuesto General del Estado y cinco bancos o instituciones financieras públicas. En conjunto, estas categorías representaron un marco referencial de 1.170.247 sujetos regulados, aunque el documento institucional aclaró que la

estimación privada se sustentó en registros administrativos y no constituyó un padrón definitivo de responsables del tratamiento. Las metas nacionales se organizaron en tres ejes: fortalecimiento de la gobernanza, universalización del derecho y promoción de la cultura, e innovación y vigilancia digital. Como se observa en la Tabla 1, los indicadores combinaron capacitación, actualización de procedimientos, coordinación interinstitucional y recursos financieros destinados a la protección de datos personales (Superintendencia de Protección de Datos Personales [SPDP], 2025).

Tabla 1

Indicadores institucionales, metas y presupuesto referencial para la protección de datos personales en Ecuador

Dimensión	Indicador o medida	Resultado documental	Periodo
Alcance institucional	Empresas privadas potencialmente reguladas	1.167.101	Registro 2023
Alcance institucional	Entidades públicas consideradas	3.141	Plan 2025
Alcance institucional	Bancos e instituciones financieras públicas	5	Plan 2025
Formación	Responsables priorizados capacitados y certificados	80 %	2025–2027
Cumplimiento interno	Entidades públicas con procedimientos actualizados y operativos	80 %	2026–2028
Gestión incidentes	de Participación pública en el sistema nacional y protocolos conjuntos	70 %	2025–2029
Gobernanza	Presupuesto referencial	USD 5.910.375,58 (36,0 %)	Cuatro años
Derechos y cultura	Presupuesto referencial	USD 6.965.757,14 (42,4 %)	Cuatro años
Innovación seguridad	y Presupuesto referencial	USD 3.561.190,48 (21,7 %)	Cuatro años
Programa integral	Presupuesto referencial total	USD 16.437.475,20	Cuatro años

Nota. Los porcentajes presupuestarios se calcularon respecto del presupuesto total consignado en el Plan Nacional de Protección de Datos Personales. Las cifras correspondieron a metas y asignaciones referenciales, por lo que no representaron porcentajes de ejecución o cumplimiento efectivamente alcanzados (SPDP, 2025).

La distribución presupuestaria mostró que el componente de universalización del derecho y promoción de la cultura concentró el 42,4 % del financiamiento previsto, seguido del fortalecimiento de la gobernanza con el 36,0 % y de la innovación digital para un ecosistema seguro con el 21,7 %. Las metas organizativas fijaron que el 80 % de los responsables pertenecientes a instituciones priorizadas recibiera capacitación entre 2025 y 2027, mientras otro 80 % de las entidades públicas priorizadas debía mantener procedimientos internos actualizados, vinculantes y operativos entre 2026 y 2028. A su vez, el sistema nacional proyectó una participación mínima del 70 % de las entidades públicas con protocolos conjuntos para gestionar incidentes de seguridad. Los documentos revisados no presentaron porcentajes de ejecución acumulada, número de

organizaciones capacitadas ni evaluaciones de eficacia, por lo que los valores se registraron exclusivamente como metas institucionales programadas (SPDP, 2025).

Los indicadores regionales de seguridad mostraron que el 31 % de las organizaciones latinoamericanas analizadas utilizó ampliamente inteligencia artificial y automatización para prevenir, identificar y contener filtraciones. En cuanto al almacenamiento, el 43 % de los incidentes involucró información distribuida en varios entornos y el 26 % afectó datos alojados exclusivamente en nubes públicas; los eventos multientorno alcanzaron un costo promedio de USD 2,94 millones. El ciclo medio de una filtración fue de 301 días, aunque los incidentes contenidos antes de 200 días registraron un costo de USD 2,40 millones, frente a USD 3,12 millones cuando superaron ese periodo. La diferencia ascendió a USD 720.000, equivalente a una reducción aproximada del 23,1 % respecto del costo de los ciclos prolongados. Además, la falta de personal especializado incrementó el costo medio en USD 167.226, la no conformidad regulatoria en USD 163.450 y la complejidad de los sistemas de seguridad en USD 146.760 (IBM, 2024).

La síntesis de los hallazgos mostró que el marco ecuatoriano había definido medidas organizativas, metas cuantificables y una planificación financiera para fortalecer el cumplimiento, pero la documentación analizada presentó principalmente resultados programáticos y no tasas consolidadas de implementación. El patrón central se caracterizó por el énfasis en capacitación, procedimientos internos, registro de responsables, gestión de riesgos y coordinación para responder a incidentes. Paralelamente, los datos regionales mostraron que la velocidad de detección, la disponibilidad de personal especializado, el cifrado y los planes de respuesta se relacionaron con menores costos operativos. No se calcularon medias, desviaciones estándar, intervalos de confianza ni valores p para las entidades ecuatorianas, porque no se dispuso de una base institucional con mediciones individuales de cumplimiento. Por consiguiente, los resultados describieron el alcance regulatorio, las metas y los indicadores económicos disponibles, sin atribuir niveles efectivos de cumplimiento a organizaciones específicas (IBM, 2024; SPDP, 2025).

Relación entre principios éticos, privacidad y prácticas de protección de datos

El análisis examinó la correspondencia entre los principios éticos aplicables al tratamiento de información personal, las garantías de privacidad y las prácticas organizativas destinadas a controlar los riesgos tecnológicos. La codificación documental se organizó en ocho categorías: licitud, finalidad, proporcionalidad, minimización, transparencia, consentimiento, seguridad y responsabilidad proactiva. Estas categorías se distribuyeron en tres niveles relacionados: legitimidad del tratamiento, control del titular y aplicación de medidas técnicas u organizativas. La transparencia y el consentimiento se asociaron principalmente con la comprensión y capacidad de decisión del usuario, mientras la minimización, la seguridad y la responsabilidad proactiva se vincularon con controles verificables durante el ciclo de vida de los datos. El patrón documental mostró que la privacidad no se presentó como una condición aislada, sino como el resultado de la articulación entre decisiones éticas, obligaciones jurídicas y prácticas operativas (Asamblea Nacional del Ecuador, 2021; Wu, 2024).

La evidencia regional cuantificada mostró una relación observable entre la adopción de medidas de seguridad y la reducción del impacto de las filtraciones. Durante 2024, el 31 % de las organizaciones latinoamericanas estudiadas utilizó ampliamente inteligencia artificial y automatización en seguridad, y este grupo registró ciclos de identificación y contención 83 días más cortos que las entidades que no emplearon dichas tecnologías. El costo promedio de una filtración alcanzó USD 2,76 millones, con un incremento anual del 12 %, mientras los incidentes resueltos antes de 200 días costaron USD 2,40 millones frente a USD 3,12 millones cuando superaron ese periodo. La diferencia correspondió a USD 720.000, equivalente al 23,1 % del costo registrado en los ciclos prolongados. Además, el 43 % de las filtraciones involucró datos distribuidos en múltiples entornos y el 26 % afectó información almacenada exclusivamente en nubes públicas, lo que evidenció una mayor exposición cuando el tratamiento se dispersó entre infraestructuras tecnológicas (IBM, 2024).

Figura 1*Relación entre ética, privacidad y protección de datos**Nota:* Autores (2025)

El esquema visual sintetizó una secuencia en la que los principios éticos se concretaron mediante garantías dirigidas al titular y, posteriormente, mediante controles organizativos susceptibles de verificación. Dentro de la planificación ecuatoriana, el 80 % de los responsables pertenecientes a instituciones priorizadas debía ser capacitado entre 2025 y 2027, y otro 80 % de las entidades públicas priorizadas debía disponer de normas y procedimientos internos actualizados entre 2026 y 2028. Asimismo, se estableció una participación mínima del 70 % de las entidades públicas en protocolos conjuntos para gestionar incidentes de seguridad durante el periodo 2025-2029. El programa integral registró un presupuesto referencial de USD 16.437.475,20, del cual USD 6.965.757,14 se destinó a la universalización del derecho y la cultura ciudadana, USD 5.910.375,58 al fortalecimiento de la gobernanza y USD 3.561.190,48 a

innovación digital y seguridad. Estos valores correspondieron a metas y asignaciones planificadas, no a porcentajes de cumplimiento efectivamente alcanzados (Superintendencia de Protección de Datos Personales [SPDP], 2025).

La integración del corpus mostró que la relación entre ética y protección de datos presentó tres grados de materialización: reconocimiento formal de principios, incorporación de controles y medición de resultados operativos. El primer grado apareció ampliamente desarrollado en la normativa ecuatoriana; el segundo se expresó mediante capacitación, gestión de riesgos, procedimientos y seguridad desde el diseño; el tercero contó principalmente con indicadores regionales agregados sobre duración y costos de las filtraciones. En la evidencia científica examinada, el análisis de 28 estudios permitió extraer 21 variables y reconocer cuatro agrupaciones mediante eigenvalores y varianzas, además de cinco agrupaciones en el análisis gráfico, lo que mostró una estructura multidimensional de las relaciones entre inteligencia artificial, privacidad y prácticas digitales. No se calcularon medias, desviaciones estándar, intervalos de confianza, correlaciones ni valores p propios, porque el corpus disponible no incluyó observaciones individuales de usuarios u organizaciones ecuatorianas. El hallazgo central indicó que los principios éticos se relacionaron con la privacidad únicamente cuando fueron traducidos en prácticas medibles de transparencia, minimización, control, seguridad y responsabilidad institucional (Saura et al., 2024; Wu, 2024).

4. Discusión

El estudio analiza la relación entre los principios éticos, la percepción de privacidad y las prácticas de protección de datos en el uso de tecnologías de la información en Ecuador. Los hallazgos sugieren que la expansión de la conectividad (reflejada en un 77,2 % de personas usuarias de internet y un 66,0 % de hogares conectados) amplía la exposición al tratamiento de información personal, pero no garantiza una comprensión equivalente de los derechos digitales. Esta brecha resulta relevante porque la disponibilidad formal de avisos de privacidad no demuestra que los usuarios entiendan las finalidades, los riesgos o las condiciones de reutilización de sus datos. El resultado converge con la revisión de 97 investigaciones realizada por van der Schyff et al. (2024), que identifica escasa evaluación directa de usuarios y dificultades de comprensión asociadas con la complejidad de las políticas de privacidad. Por ello, el conocimiento tecnológico y la alfabetización en protección de datos deben interpretarse como capacidades relacionadas, aunque conceptualmente distintas. En conjunto, los hallazgos parecen indicar que el crecimiento de la participación digital ecuatoriana avanza con mayor rapidez que la generación de evidencia sobre confianza, comprensión normativa y percepción de riesgo de los titulares (INEC, 2024; van der Schyff et al., 2024).

La correspondencia entre cumplimiento normativo y seguridad organizativa muestra una situación igualmente compleja, pues Ecuador dispone de principios, obligaciones y

metas institucionales definidas, aunque todavía no cuenta con tasas consolidadas que demuestren su aplicación efectiva. La planificación nacional, que asigna USD 16.437.475,20 y proyecta capacitar al 80 % de los responsables priorizados, evidencia una orientación hacia la responsabilidad proactiva, pero sus indicadores representan compromisos programados y no resultados de ejecución. Esta diferencia coincide con Chavarría-Mora (2025), quien identifica variabilidad regional en autoridades, recursos y mecanismos de cumplimiento, y con Veronese y Lemos (2021), quienes advierten dificultades para integrar la regulación de datos con las políticas tecnológicas latinoamericanas. Los datos regionales refuerzan la importancia económica de esa brecha: una filtración cuesta en promedio USD 2,76 millones y los incidentes prolongados registran USD 720.000 adicionales frente a los contenidos antes de 200 días. No obstante, tales asociaciones deben interpretarse con cautela, porque proceden de información agregada y no permiten atribuir el menor costo exclusivamente a una medida de seguridad determinada. Así, el cumplimiento efectivo parece depender menos de la existencia aislada de normas y más de su traducción en personal especializado, procedimientos verificables, controles de acceso y capacidad de respuesta institucional (IBM, 2024; SPDP, 2025).

La integración de los resultados aporta una interpretación en la que la ética, la privacidad y la seguridad conforman niveles interdependientes y no componentes sustituibles entre sí. La licitud, la finalidad y la proporcionalidad legitiman el tratamiento; la transparencia y el consentimiento fortalecen el control del titular; mientras la minimización, la seguridad desde el diseño y la responsabilidad proactiva materializan esa legitimidad en prácticas comprobables. Esta relación coincide con Wu (2024), quien sostiene que la transparencia formal resulta insuficiente cuando no se acompaña de criterios de equidad, y con Sætra (2022), quien cuestiona los enfoques que presentan privacidad y seguridad como derechos necesariamente contrapuestos. Del mismo modo, el patrón multidimensional identificado por Saura et al. (2024) respalda la necesidad de examinar simultáneamente variables tecnológicas, organizativas y éticas, especialmente ante decisiones automatizadas y usos comerciales de información personal. En términos prácticos, los hallazgos sugieren que las organizaciones requieren indicadores que midan no solo la existencia de políticas, sino también su comprensibilidad, aplicación, trazabilidad y capacidad para reducir riesgos. El aporte metodológico reside, por tanto, en articular principios, garantías e indicadores operativos dentro de un marco común que permite examinar la distancia entre reconocimiento jurídico y protección efectiva (Saura et al., 2024; Sætra, 2022; Wu, 2024).

Los resultados deben valorarse considerando que el estudio presenta un alcance exploratorio, emplea fuentes documentales heterogéneas y utiliza indicadores regionales que no representan de manera exclusiva a las organizaciones ecuatorianas. Asimismo, la ausencia de puntuaciones individuales, cuestionarios válidos y distribuciones de respuesta impide estimar medias, intervalos de confianza, asociaciones estadísticas o diferencias sociodemográficas sobre conocimiento, confianza y riesgo percibido. El tamaño de 385 participantes constituye una estimación de planificación y no confirma una muestra efectivamente analizada, mientras las metas del Plan Nacional tampoco equivalen a porcentajes alcanzados, lo que restringe cualquier inferencia sobre cumplimiento real (Lohr, 2021; SPDP, 2025). Las investigaciones posteriores deberían aplicar encuestas probabilísticas, estudios longitudinales y auditorías sectoriales que relacionen comprensión ciudadana, madurez

organizativa, incidentes registrados y ejercicio efectivo de derechos, sin asumir relaciones causales derivadas de asociaciones observacionales. También resulta pertinente comparar instituciones públicas y privadas, evaluar la claridad de los avisos de privacidad y medir la implementación de la protección de datos desde el diseño. Pese a estas limitaciones, la contribución central consiste en mostrar que la brecha ecuatoriana no radica únicamente en reconocer derechos, sino en convertirlos en prácticas éticas, medibles y sostenibles que vinculen confianza, transparencia, seguridad y responsabilidad institucional (Creswell & Plano Clark, 2018; van der Schyff et al., 2024).

5. Conclusiones

Los resultados permiten concluir que la relación entre ética, privacidad y protección de datos depende de la capacidad para convertir los principios jurídicos en prácticas organizativas verificables. El crecimiento de la conectividad en Ecuador, donde el uso de internet alcanza al 77,2 % de la población considerada y el acceso doméstico llega al 66,0 %, incrementa la exposición al tratamiento de información personal. Sin embargo, esta expansión no demuestra por sí misma un conocimiento equivalente de los derechos digitales ni una confianza informada en las organizaciones. La privacidad se configura, por tanto, como una condición vinculada con transparencia, consentimiento comprensible, minimización, seguridad y responsabilidad proactiva. Este hallazgo debe interpretarse dentro del alcance exploratorio y documental del estudio, sin atribuir relaciones causales.

Los hallazgos vinculados con los objetivos específicos evidencian que persiste una distancia entre la disponibilidad formal de información y la comprobación de que los usuarios comprenden los avisos de privacidad, las finalidades del tratamiento y los mecanismos para ejercer sus derechos. A la vez, el marco ecuatoriano incorpora obligaciones técnicas y organizativas, metas de capacitación y procedimientos institucionales, aunque la documentación disponible no permite determinar tasas consolidadas de ejecución. Los indicadores regionales muestran que una gestión tardía de incidentes eleva los costos y que la respuesta temprana puede representar diferencias cercanas a USD 720.000 por filtración. En conjunto, se observa que el cumplimiento normativo requiere capacidades humanas, controles técnicos y mecanismos de supervisión, además de la sola existencia de disposiciones legales. Esto sugiere que conocimiento ciudadano y madurez organizacional deben fortalecerse de manera simultánea.

El principal aporte del estudio consiste en integrar tres niveles que suelen analizarse por separado: legitimidad ética del tratamiento, control efectivo del titular y aplicación institucional de medidas de protección. Esta articulación permite comprender que la seguridad tecnológica no sustituye a la privacidad, del mismo modo que la transparencia formal no garantiza decisiones autónomas cuando la información resulta compleja o ambigua. En el ámbito profesional e institucional, el marco propuesto facilita examinar políticas internas, gestión de riesgos, respuesta ante incidentes y protección desde el diseño mediante criterios comunes. La asignación referencial superior a USD 16,4 millones prevista en la planificación nacional evidencia la importancia estratégica otorgada al tema, aunque su impacto dependerá de la ejecución y evaluación de las

acciones programadas. Así, la investigación aporta una base conceptual y metodológica para valorar la protección efectiva más allá del cumplimiento declarativo.

A partir de estos resultados, se recomienda fortalecer la alfabetización en privacidad, simplificar los avisos dirigidos a los titulares y establecer indicadores institucionales que permitan verificar capacitación, trazabilidad, atención de derechos y reducción de incidentes. Las futuras investigaciones deberían incorporar muestras efectivamente observadas, encuestas probabilísticas y seguimientos longitudinales que midan conocimiento, confianza, riesgo percibido y prácticas de seguridad en distintos grupos sociales. También conviene desarrollar auditorías comparativas entre organizaciones públicas y privadas, así como estudios sectoriales en salud, educación, banca, comercio electrónico y servicios digitales. Estas líneas permitirían estimar asociaciones con mayor precisión, sin atribuir causalidad cuando el diseño no lo permita. La contribución central del estudio radica en mostrar que el problema no se limita al reconocimiento jurídico de la privacidad, sino a su transformación en prácticas éticas, medibles y sostenibles.

Referencias Bibliográficas

- Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Quinto Suplemento del Registro Oficial No. 459. <https://www.gob.ec/regulaciones/ley-organica-proteccion-datos-personales>
- Boné-Andrade, M. F., Pinargote-Bravo, V. J., & Bonilla-Fierro, L. F. (2023). Estrategias de ciberseguridad en entornos de trabajo híbridos y remoto. *Revista Científica Ciencia Y Método*, 1(4), 31-43. <https://doi.org/10.55813/gaea/rcym/v1/n4/21>
- Bonilla-Fierro, L. F., & Boné-Andrade, M. F. (2025). Desarrollo de plataformas de comunicación inclusivas mediante diseño universal. *Revista Científica Ciencia Y Método*, 3(2), 59-73. <https://doi.org/10.55813/gaea/rcym/v3/n2/5>
- Braun, V., & Clarke, V. (2021). One size fits all? What counts as quality practice in reflexive thematic analysis? *Qualitative Research in Psychology*, 18(3), 328–352.
- Carpio-Velasco, F. J., & Garcés-Beltrán, G. M. (2025). Comparación de Estrategias de Control de Temperatura: Controlador PID y Redes Neuronales. *Revista Científica Zambos*, 4(2), 185-196. <https://doi.org/10.69484/rcz/v4/n2/113>
- Castelo-Vinueza, E. M. (2025). Problemas de la investigación tecnológica y su aplicación en la generación de innovación. *Journal of Economic and Social Science Research*, 5(1), 146–160. <https://doi.org/10.55813/gaea/jessr/v5/n1/166>
- Castro-Morales, S., & Samaniego-Quiguiri, D. P. (2025). Ciberdelitos y desafíos legales en la protección de datos personales y privacidad digital. *Revista Científica Enfoques Del Conocimiento*, 2(1), 1-18. <https://doi.org/10.55813/gaea/revistacec/v2/n1/27>
- Chavarría-Mora, E. (2025). (Lack of) patterns in commitment: Data protection in the Latin America and Caribbean personal data protection laws. *Social Media + Society*, 11(2).
- Chávez-Rendón, S. D., Pillasagua-Yépez, T. M., Moreira-Noboa, S. M., & Zamora-Mayorga, D. J. (2025). Análisis del funcionamiento tecnológico del ECU 911 de

- Quevedo en la gestión pública de la seguridad ciudadana. *Revista Científica Ciencia Y Método*, 3(3), 181-193. <https://doi.org/10.55813/gaea/rcym/v3/n3/71>
- Choez-Calderón, C. J. (2024). Realidad aumentada y su aplicación en la educación a distancia. *Revista Científica Ciencia Y Método*, 2(3), 26-38. <https://doi.org/10.55813/gaea/rcym/v2/n3/46>
- Choez-Calderón, C. J., & Aldo-Patricio, M. O. (2025). La ciberseguridad como prioridad empresarial dentro de marcos los regulatorios y normativos internacionales. *Revista Científica Ciencia Y Método*, 3(3), 14-27. <https://doi.org/10.55813/gaea/rcym/v3/n3/38>
- Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3.^a ed.). SAGE.
- Erazo-Luzuriaga, A. F., & Morales-Chincha, J. A. (2025). Blockchain y transparencia de la información en sistemas financieros digitales. *Revista Científica Enfoques Del Conocimiento*, 2(3), 74-90. <https://doi.org/10.55813/gaea/revistacec/v2/n3/40>
- Erazo-Luzuriaga, A. F., Ramos-Secaira, F. M., Galarza-Sánchez, P. C., & Boné-Andrade, M. F. (2023). La inteligencia artificial aplicada a la optimización de programas informáticos. *Journal of Economic and Social Science Research*, 3(1), 48–63. <https://doi.org/10.55813/gaea/jessr/v3/n1/61>
- Galarza-Sánchez, P. C. (2023). Adopción de Tecnologías de la Información en las PYMEs Ecuatorianas: Factores y Desafíos. *Revista Científica Zambos*, 2(1), 21-40. <https://doi.org/10.69484/rcz/v2/n1/36>
- Galarza-Sánchez, P. C., Agualongo-Yazuma, J. C., & Jumbo-Martínez, M. N. (2022). Innovación tecnológica en la industria de restaurantes del Cantón Pedro Vicente Maldonado. *Journal of Economic and Social Science Research*, 2(1), 31–43. <https://doi.org/10.55813/gaea/jessr/v2/n1/45>
- Galarza-Sánchez, P. C., Erazo-Luzuriaga, A. F., & Boné-Andrade, M. F. (2023). Uso de computación cuántica en la mejora de algoritmos de aprendizaje automático. *Revista Científica Ciencia Y Método*, 1(4), 16-30. <https://doi.org/10.55813/gaea/rcym/v1/n4/25>
- Galarza-Sánchez, P. C., Herrera-Ramírez, C. D., & Borja-Almeida, L. G. (2025). Seguridad informática y prevención de ataques cibernéticos en sistemas organizacionales. *Revista Científica Enfoques Del Conocimiento*, 2(3), 49-73. <https://doi.org/10.55813/gaea/revistacec/v2/n3/39>
- García-Peña, V. R. (2023). Desarrollo y Uso de Aplicaciones Móviles en el Contexto Ecuatoriano. *Revista Científica Zambos*, 2(3), 1-15. <https://doi.org/10.69484/rcz/v2/n3/46>
- Hernández-Ortiz, J., & Rodríguez-Vizuite, J. D. (2024). Computación en la nube y eficiencia operativa en empresas de servicios tecnológicos. *Revista Científica Enfoques Del Conocimiento*, 1(3), 61-81. <https://doi.org/10.55813/gaea/revistacec/v1/n3/20>
- IBM. (2024). *Cost of a Data Breach Report 2024*. <https://www.ibm.com/reports/data-breach>

- Instituto Nacional de Estadística y Censos. (2024). *Tecnologías de la información y comunicación-TIC 2024*. <https://www.ecuadorencifras.gob.ec/tecnologias-de-la-informacion-y-comunicacion-tic-2024/>
- Lohr, S. L. (2021). *Sampling: Design and analysis* (3.^a ed.). Chapman and Hall/CRC. <https://doi.org/10.1201/9780429298899>
- López-Freire, S. A., & Lizarraga-Aguirre, H. R. (2023). Implementación de robótica blanda en procesos de ensamblaje automatizados. *Revista Científica Ciencia Y Método*, 1(2), 58-71. <https://doi.org/10.55813/gaea/rcym/v1/n2/15>
- Montalván-Vélez, C. L., Mogrovejo-Zambrano, J. N., Romero-Vitte, I. J., & Pinargote-Carrera, M. L. D. C. (2024). Introducción a la Inteligencia Artificial: Conceptos Básicos y Aplicaciones Cotidianas. *Journal of Economic and Social Science Research*, 4(1), 173–183. <https://doi.org/10.55813/gaea/jessr/v4/n1/93>
- Páez-Puente, E. G., Avendañ-Durango, J. C., & Pinargote-Bravo, V. J. (2025). Transformación digital y adopción tecnológica en pequeñas y medianas empresas. *Revista Científica Enfoques Del Conocimiento*, 2(3), 91-111. <https://doi.org/10.55813/gaea/revistacec/v2/n3/41>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71. <https://doi.org/10.1136/bmj.n71>
- Presidencia de la República del Ecuador. (2023). *Reglamento General de la Ley Orgánica de Protección de Datos Personales: Decreto Ejecutivo No. 904*. <https://www.telecomunicaciones.gob.ec/wp-content/uploads/2023/11/Decreto-Ejecutivo-No.-904.pdf>
- Ramos-Secaira, F. M. (2023). Seguridad Cibernética en Empresas Ecuatorianas: Prácticas y Retos Actuales. *Revista Científica Zambos*, 2(3), 16-28. <https://doi.org/10.69484/rcz/v2/n3/47>
- Robalino-Latorre, M. C., Ramirez-Klinger, W. N., Guadalupe-Copa, R. C., & Cuello-García, S. A. (2023). Aplicación del Método Montecarlo en flujo de potencias a través del Software Octave. *Journal of Economic and Social Science Research*, 3(1), 31–47. <https://doi.org/10.55813/gaea/jessr/v3/n1/60>
- Rodriguez-Vizuite, J. D., Viteri-Ojeda, J. C., & Villa-Feijoó, A. L. (2024). Adopción de tecnologías sostenibles en infraestructuras de tecnologías de la información. *Revista Científica Ciencia Y Método*, 2(1), 55-67. <https://doi.org/10.55813/gaea/rcym/v2/n1/31>
- Sætra, H. S. (2022). The ethics of trading privacy for security: The multifaceted effects of privacy on liberty and security. *Technology in Society*, 68, 101854. <https://doi.org/10.1016/j.techsoc.2021.101854>
- Sánchez-Caguana, D. F., Philco-Reinozo, M. A., Salinas-Arroba, J. M., & Pico-Lescano, J. C. (2024). Impacto de la Inteligencia Artificial en la Precisión y Eficiencia de los Sistemas Contables Modernos. *Journal of Economic and Social Science Research*, 4(3), 1–12. <https://doi.org/10.55813/gaea/jessr/v4/n3/117>

- Sangacha-Tapia, L., González-Cañizalez, Y., & Rivas-Herrera, J. (2025). Optimización de Criterios de Búsqueda avanzada para Nuevas Tendencias en la Académica mediante Machine Learning. *Revista Científica Zambos*, 4(2), 197-211. <https://doi.org/10.69484/rcz/v4/n2/114>
- Saura, J. R., Škare, V., & Ozretić Došen, Đ. (2024). Is AI-based digital marketing ethical? Assessing a new data privacy paradox. *Journal of Innovation & Knowledge*, 9(4), 100597. <https://doi.org/10.1016/j.jik.2024.100597>.
- Solano-Gutiérrez, G. A. (2024). La Tecnología en la Educación a Distancia: Revisión de Progresos y Obstáculos a Superar. *Revista Científica Zambos*, 3(2), 48-73. <https://doi.org/10.69484/rcz/v3/n2/17>
- Superintendencia de Protección de Datos Personales. (2025). *Plan Nacional de Protección de Datos Personales*. <https://spdp.gob.ec/wp-content/uploads/2025/05/60.01.02-PLAN-NACIONAL-DE-PROTECCION-DE-DATOS-PERSONALES-20250512-signed.pdf>
- Superintendencia de Protección de Datos Personales. (2026). *La SPDP sanciona a LIGAPRO por no haber implementado la protección de datos personales desde el diseño y por defecto en la aplicación FAN ID*. <https://spdp.gob.ec/prensa/>
- van der Schyff, K., Prior, S., & Renaud, K. (2024). Privacy policy analysis: A scoping review and research agenda. *Computers & Security*, 146, 104065. <https://doi.org/10.1016/j.cose.2024.104065>
- Vears, D. F., & Gillam, L. (2022). Inductive content analysis: A guide for beginning qualitative researchers. *Focus on Health Professional Education*, 23(1), 111–127. <https://doi.org/10.11157/fohpe.v23i1.544>
- Veronese, A., & Nunes Lopes Espiñeira Lemos, A. (2021). Regulatory paths for artificial intelligence in Latin American countries with data protection law frameworks: Limits and possibilities of integrating policies. *Revista Latinoamericana de Economía y Sociedad Digital*, (2). <https://doi.org/10.53857/CJFB4918>
- Wu, C. (2024). Data privacy: From transparency to fairness. *Technology in Society*, 76, 102457. <https://doi.org/10.1016/j.techsoc.2024.102457>.
- Yusoff, M. S. B., Arifin, W. N., & Hadie, S. N. H. (2021). ABC of questionnaire development and validation for survey research. *Education in Medicine Journal*, 13(1), 97–108. <https://doi.org/10.21315/eimj2021.13.1.10>.

CONFLICTO DE INTERESES

“Los autores declaran no tener ningún conflicto de intereses”.