

DOI: <https://doi.org/10.63618/omd/revinvlid/v3/n1/50>

Protección de datos personales y privacidad digital en entornos de inteligencia artificial.

Protection of personal data and digital privacy in artificial intelligence environments.

Samaniego-Quigui, Delia Paulina ¹; Mina-Bone, Santos Geovanny ²; Mendoza-Armijos, Hugo Enrique ³; Bonilla-Morejón, Diego Marcelo ⁴.

¹ Fiscalía General del Estado; Ecuador; <https://orcid.org/0000-0002-2051-3431>; samaniegod@fiscalia.gob.ec.

² Universidad Técnica Luis Vargas Torres de Esmeraldas; Ecuador; <https://orcid.org/0000-0002-2526-3988>; santos.mina@utelvt.edu.ec.

³ Instituto Superior Tecnológico Los Andes; Ecuador; <https://orcid.org/0000-0001-7396-1687>; enrique.mendoza1@istla.edu.ec.

⁴ Consejo de la Judicatura; Ecuador; <https://orcid.org/0000-0001-5481-151X>; diegomar_1987@yahoo.es.

Cita: Samaniego-Quigui, D. P., Mina-Bone, S. G., Mendoza-Armijos, H. E., & Bonilla-Morejón, D. M. (2026). Protección de datos personales y privacidad digital en entornos de inteligencia artificial. *Revista De Investigación Y Liderazgo*, 3(1), 51-65. <https://doi.org/10.63618/omd/revinvlid/v3/n1/50>

Resumen

La expansión de la inteligencia artificial en Ecuador incrementó el tratamiento automatizado de datos personales y evidenció riesgos vinculados con opacidad, reutilización de información, decisiones automatizadas y desigualdad en el acceso digital. El estudio tuvo como objetivo analizar el cumplimiento de la protección de datos personales en organizaciones públicas y privadas que emplean inteligencia artificial y su relación con la madurez institucional, la confianza digital y la privacidad percibida. Se desarrolló una investigación mixta, documental, no experimental, transversal y exploratoria, basada en normas, informes técnicos y literatura científica publicada entre 2021 y junio de 2026, analizada mediante una matriz de categorías jurídicas, técnicas y organizacionales. Los resultados identificaron cinco obligaciones centrales, tres garantías frente al tratamiento automatizado y cuatro tipos de actores responsables; además, mostraron mayor desarrollo en adopción pública y capacidad normativa que en infraestructura, difusión empresarial y consolidación tecnológica. La discusión evidenció que la existencia de regulación no aseguró por sí sola una aplicación uniforme, mientras que las salvaguardas visibles, la transparencia, la auditoría y la supervisión humana se asociaron con mayor confianza declarada. Se concluyó que la privacidad digital dependió de una implementación verificable, continua y coordinada durante todo el ciclo de vida de los sistemas de inteligencia artificial.

Palabras clave: inteligencia artificial; protección de datos; privacidad digital; confianza digital; madurez institucional.

Abstract

The expansion of artificial intelligence in Ecuador increased the automated processing of personal data and highlighted risks related to opacity, information reuse, automated decisions, and inequality in digital access. The study aimed to analyze the compliance with personal data protection in public and private organizations that employ artificial intelligence and its relationship with institutional maturity, digital trust, and perceived privacy. A mixed, documentary, non-experimental, cross-sectional, and exploratory research was developed, based on standards, technical reports, and scientific literature published between 2021 and June 2026, analyzed thru a matrix of legal, technical, and organizational categories. The results identified five central obligations, three guarantees against automated processing, and four types of responsible actors; moreover, they showed greater development in public adoption and regulatory capacity than in infrastructure, business dissemination, and technological consolidation. The discussion revealed that the mere existence of regulation did not ensure uniform application, while visible safeguards, transparency, auditing, and human oversight were associated with greater declared trust. It was concluded that digital privacy depended on a verifiable, continuous, and coordinated implementation throughout the entire lifecycle of artificial intelligence systems.

Keywords: artificial intelligence; data protection; digital privacy; digital trust; institutional maturity.

1. Introducción

La expansión de la inteligencia artificial en Ecuador se desarrolla sobre una base digital amplia, aunque marcada por desigualdades territoriales y socioeconómicas. De los 5.146.753 hogares registrados en 2024, 3.395.595 disponen de conexión a internet, equivalentes al 66,0 %; sin embargo, la cobertura alcanza el 73,6 % en áreas urbanas y únicamente el 48,1 % en zonas rurales. Asimismo, 13,3 millones de los 17,2 millones de habitantes de cinco años o más utilizan internet, lo que representa el 77,2 % y amplía la generación de datos susceptibles de análisis automatizado (Instituto Nacional de Estadística y Censos [INEC], 2024). En el ámbito regional, Ecuador obtiene 34,59 puntos sobre 100 y ocupa el puesto 11 entre 19 países evaluados en el Índice Latinoamericano de Inteligencia Artificial, condición que refleja una adopción creciente acompañada de capacidades institucionales todavía limitadas (Centro Nacional de Inteligencia Artificial [CENIA], 2024). Bajo este escenario, la unidad de análisis comprende los procesos de tratamiento de datos personales incorporados en sistemas de inteligencia artificial utilizados por organizaciones públicas y privadas, mientras que la población de interés incluye a las personas adultas cuyos datos alimentan, validan o reciben los resultados de tales sistemas.

Este crecimiento del ecosistema digital coincide con la consolidación de una arquitectura jurídica ecuatoriana integrada por tres niveles: la Ley Orgánica de Protección de Datos Personales vigente desde 2021, su Reglamento General expedido en 2023 y la norma específica para sistemas de inteligencia artificial emitida en 2026 (Asamblea Nacional del Ecuador, 2021; Presidencia de la República del Ecuador, 2023; Superintendencia de Protección de Datos Personales [SPDP], 2026). La regulación más reciente contiene 10 artículos y extiende su aplicación a desarrolladores, implementadores, desplegados y proveedores que tratan datos de titulares ecuatorianos, independientemente de la ubicación del sistema o del proveedor. Su artículo 5 establece cinco obligaciones centrales: informar de manera transparente, gestionar riesgos y evaluaciones de impacto, aplicar medidas de seguridad, registrar los tratamientos y auditar el funcionamiento de la inteligencia artificial. A ello se suma el deber de notificar determinadas vulneraciones de seguridad en un plazo máximo de cinco días. El incumplimiento expone a entidades privadas y empresas públicas a multas de entre el 0,1 % y el 0,7 % de su volumen anual de negocios por infracciones leves, y de entre el 0,7 % y el 1 % por infracciones graves, de modo que la privacidad digital adquiere implicaciones jurídicas, financieras y reputacionales verificables.

El cumplimiento formal de este marco no elimina los riesgos técnicos derivados del entrenamiento, la inferencia y la reutilización de información personal, porque los modelos pueden memorizar y reproducir fragmentos de sus conjuntos de datos. Carlini et al. (2021) generan 1.800 muestras candidatas mediante 18 configuraciones de ataque y comprueban que 604 corresponden a ejemplos memorizados, con una tasa global del 33,5 % y un máximo del 67 % en la configuración más efectiva. Los autores también muestran que un modelo GPT-2 de 1.500 millones de parámetros memoriza más de 18 veces el contenido registrado por una versión de 124 millones de parámetros, incluyendo nombres, direcciones, teléfonos y correos electrónicos. La escala de los modelos, la opacidad de los conjuntos de entrenamiento y la concentración de recursos dificultan la trazabilidad y elevan el riesgo de reproducir información sensible o patrones discriminatorios. Aunque el aprendizaje federado reduce la transferencia centralizada

de datos, conserva amenazas relacionadas con inferencias, envenenamiento de modelos y filtración de actualizaciones, por lo que las medidas de privacidad producen compensaciones entre seguridad, precisión y utilidad analítica (Mothukuri et al., 2021).

Los efectos de estas vulnerabilidades trascienden la confidencialidad individual, pues el perfilamiento automatizado interviene en decisiones laborales, crediticias, sanitarias, educativas y administrativas capaces de condicionar derechos, oportunidades y acceso a servicios. En América Latina y el Caribe, entre el 26 % y el 38 % de los empleos se encuentra expuesto a la inteligencia artificial generativa; entre el 8 % y el 14 % presenta posibilidades de mejora productiva, mientras que entre el 2 % y el 5 % afronta un riesgo de automatización total (Gmyrek et al., 2024). Cuando estos procesos utilizan datos personales sin transparencia, supervisión humana o mecanismos de oposición, las ganancias productivas pueden coexistir con vigilancia laboral, segmentación injustificada y profundización de desigualdades digitales, especialmente entre grupos con menor conectividad o alfabetización tecnológica (UNESCO, 2021). Desde la dimensión económica, el costo promedio mundial de una vulneración de datos alcanza USD 4,88 millones en 2024, cifra que aumenta un 10 % respecto de 2023 y sirve como referencia sobre la magnitud financiera del riesgo, aunque no constituye una estimación específica para Ecuador (IBM, 2024). La ausencia de controles efectivos traslada estos costos a las organizaciones mediante sanciones e interrupciones operativas y a la ciudadanía mediante fraude, exclusión, pérdida de autonomía y deterioro de la confianza institucional.

Aunque la producción científica ofrece avances en extracción de datos, privacidad diferencial, aprendizaje federado y equidad algorítmica, la evidencia permanece fragmentada entre evaluaciones técnicas, análisis jurídicos e índices nacionales. La revisión de Shaham et al. (2025) muestra que privacidad y equidad interactúan mediante compensaciones que pueden mejorar una dimensión y perjudicar otra, lo cual cuestiona las evaluaciones que examinan ambos principios de manera aislada. En Ecuador, el ILIA 2024 registra 17 puntos en gobernanza frente a un promedio latinoamericano de 37,46, y 23,33 puntos en regulación frente a 45,28 en la región; no obstante, estos indicadores macro no determinan el cumplimiento organizacional ni la percepción de privacidad de los titulares (CENIA, 2024). La entrada en vigencia de una norma de inteligencia artificial con 10 artículos y cinco obligaciones desplaza la brecha desde la inexistencia regulatoria hacia la implementación verificable de sus disposiciones (SPDP, 2026). Persisten, por consiguiente, interrogantes sobre la relación entre madurez organizacional, tipo de modelo, categorías de datos, transparencia, evaluaciones de impacto, confianza digital y sector de aplicación, vacío que impide establecer si la protección declarada se traduce en privacidad efectiva.

La necesidad de cerrar esta brecha justifica una investigación con relevancia social, valor teórico y utilidad metodológica, porque permite vincular obligaciones jurídicas, controles técnicos y experiencias de los titulares dentro de un mismo esquema analítico. Su viabilidad se apoya en tres instrumentos normativos de acceso público, estadísticas oficiales sobre 13,3 millones de usuarios de internet y técnicas no intrusivas, como el cuestionario estructurado, que requieren recursos y tiempos razonables sin recurrir a datos sensibles innecesarios (INEC, 2024; SPDP, 2026). El proceso investigativo incorpora consentimiento informado, minimización, anonimización, almacenamiento seguro y uso exclusivo de la información para los fines declarados, en correspondencia

con la protección de la dignidad y la autonomía promovida por la UNESCO (2021). En este marco, el objetivo general consiste en analizar el cumplimiento de la protección de datos personales en organizaciones públicas y privadas que emplean inteligencia artificial en Ecuador y su relación con la privacidad percibida por las personas adultas usuarias de servicios digitales. El primer objetivo específico busca determinar el grado de aplicación de las obligaciones de transparencia, seguridad, evaluación de impacto, registro y auditoría. El segundo pretende comparar la madurez institucional y relacionarla con la confianza y la percepción de privacidad según el sector y el tipo de uso de la inteligencia artificial.

La contribución esperada se concentra en una matriz de evaluación compuesta por tres dimensiones (jurídica, técnica y organizacional) que operacionaliza las cinco obligaciones principales de la regulación ecuatoriana de inteligencia artificial. Esta estructura permite contrastar dos ámbitos institucionales, público y privado, e integrar el cumplimiento verificable con la percepción de las personas titulares, en lugar de limitar el análisis a la presencia documental de políticas. La originalidad del estudio reside en relacionar los 10 artículos de la norma vigente con variables de transparencia, gestión del riesgo, seguridad, auditoría y confianza digital, incorporando simultáneamente las tensiones entre privacidad y equidad identificadas por Shaham et al. (2025). Sus resultados pueden aportar indicadores replicables para la investigación académica y criterios de diagnóstico aplicables por responsables, encargados y delegados de protección de datos. De esta manera, el trabajo conecta la reciente evolución regulatoria ecuatoriana con evidencia empírica sobre su implementación y ofrece una respuesta contextualizada a una brecha que los análisis exclusivamente tecnológicos o normativos no resuelven por separado (SPDP, 2026; UNESCO, 2021).

2. Materiales y Métodos

La investigación integró procedimientos cualitativos y cuantitativos para examinar la protección de datos personales y la privacidad digital en sistemas de inteligencia artificial empleados o regulados en Ecuador, dentro del contexto latinoamericano. El componente cualitativo permitió interpretar principios, obligaciones, derechos, riesgos y mecanismos de responsabilidad contenidos en normas y publicaciones científicas, mientras que el cuantitativo permitió registrar frecuencias, proporciones y patrones de aparición de esas categorías. Ambos componentes se desarrollaron sobre un mismo corpus documental y se combinaron durante la interpretación mediante una estrategia convergente. Esta integración respondió al propósito de contrastar el contenido jurídico con la evidencia técnica y organizacional, sin reducir el fenómeno a indicadores aislados. La elección se sustentó en la capacidad de los métodos mixtos para relacionar resultados numéricos con significados contextuales y normativos (Creswell & Plano Clark, 2018).

La convergencia de ambas perspectivas condujo a un diseño no experimental y transversal, debido a que las variables no fueron manipuladas ni se introdujeron intervenciones sobre sistemas, organizaciones o titulares de datos personales. La información se examinó tal como apareció en documentos publicados y vigentes durante el periodo comprendido entre enero de 2021 y junio de 2026, lo que permitió obtener una representación delimitada del desarrollo regulatorio y científico. El alcance se

mantuvo exploratorio porque se buscó identificar categorías, relaciones y vacíos todavía insuficientemente estudiados en Ecuador y Latinoamérica. Por esta razón, el estudio no pretendió demostrar causalidad, estimar efectos poblacionales ni generalizar sus resultados a todas las organizaciones que utilizaron inteligencia artificial. La observación documental resultó coherente con fenómenos emergentes cuyo conocimiento se encontraba disperso entre fuentes jurídicas, académicas y técnicas (Morgan, 2022).

La lógica del diseño se extendió mediante una investigación documental que trató como unidad de análisis cada norma, guía, política pública, informe técnico o artículo científico relacionado directamente con inteligencia artificial, privacidad digital y tratamiento de datos personales. El razonamiento deductivo orientó la construcción inicial de categorías a partir de la Ley Orgánica de Protección de Datos Personales, su Reglamento General y la normativa ecuatoriana específica sobre sistemas de inteligencia artificial. De manera complementaria, el razonamiento inductivo permitió reconocer temas no previstos, como riesgos de reidentificación, opacidad algorítmica, transferencias internacionales, reutilización de información y tensiones entre precisión y minimización. La combinación de ambas rutas evitó imponer exclusivamente categorías jurídicas sobre problemas técnicos y, al mismo tiempo, impidió interpretar la evidencia sin un referente normativo verificable. El marco ecuatoriano se consideró especialmente pertinente porque reconoció derechos frente a decisiones automatizadas y extendió obligaciones a quienes desarrollaron, implementaron, desplegaron o proveyeron sistemas que trataron datos de titulares ecuatorianos (Asamblea Nacional del Ecuador, 2021; Superintendencia de Protección de Datos Personales [SPDP], 2026).

La delimitación anterior orientó una búsqueda estructurada en Scopus, Web of Science, SciELO, Redalyc y Google Scholar, complementada con consultas en los repositorios oficiales de la Asamblea Nacional, la Presidencia de la República, la SPDP, la UNESCO y organismos técnicos internacionales. Se utilizaron combinaciones en español e inglés de los términos “protección de datos”, “privacidad digital”, “inteligencia artificial”, “decisiones automatizadas”, “evaluación de impacto”, “data protection”, “digital privacy” y “artificial intelligence”, enlazados mediante los operadores AND y OR. La búsqueda cubrió publicaciones emitidas entre 2021 y junio de 2026, aunque se admitieron textos metodológicos publicados desde 2018 cuando no existió una alternativa reciente equivalente. Cada resultado se registró con autoría, año, jurisdicción, tipo de fuente, sector analizado y enlace permanente o DOI. La identificación, eliminación de duplicados, revisión de textos completos y justificación de exclusiones adaptó los criterios de trazabilidad de PRISMA 2020, sin presentar el trabajo como una revisión sistemática de efectos (Page et al., 2021).

La selección derivada de la búsqueda incluyó documentos disponibles en texto completo, publicados en español o inglés y centrados de manera sustantiva en el tratamiento de datos personales mediante inteligencia artificial. También se incorporaron normas ecuatorianas vigentes, instrumentos latinoamericanos pertinentes y estudios revisados por pares que analizaron riesgos, derechos, medidas de seguridad, transparencia, gobernanza o responsabilidad algorítmica. Se excluyeron registros duplicados, notas periodísticas, contenidos comerciales, publicaciones sin autoría identificable, textos de opinión carentes de procedimiento analítico y trabajos sobre inteligencia artificial que no abordaron privacidad o protección de datos. La población documental quedó constituida por el conjunto de fuentes potencialmente elegibles,

mientras que el corpus analítico se conformó mediante selección intencional basada en relevancia, autenticidad, credibilidad y representatividad. Debido a que la unidad de análisis estuvo compuesta por documentos y no por personas, no se aplicó una fórmula de muestreo para población finita ni se efectuó inferencia estadística poblacional (Morgan, 2022).

El corpus depurado se examinó mediante una matriz estructurada que reunió datos bibliográficos, características metodológicas, ámbito territorial, sector de aplicación, tipo de inteligencia artificial, categorías de datos tratados, riesgos identificados y salvaguardas propuestas. La codificación deductiva comprendió licitud, finalidad, transparencia, minimización, seguridad, privacidad desde el diseño, evaluación de impacto, derechos frente a decisiones automatizadas, auditoría y responsabilidad demostrada, categorías derivadas del marco ecuatoriano y de guías de gestión de riesgos (SPDP, 2025, 2026). El análisis cuantitativo calculó frecuencias absolutas y porcentajes de presencia de cada categoría, además de comparaciones descriptivas según año, jurisdicción, sector y tipo de documento. El componente cualitativo siguió las fases de familiarización, codificación, construcción, revisión y denominación de temas, junto con la elaboración de una interpretación articulada con los objetivos. La trazabilidad se reforzó mediante un libro de códigos, reglas operativas para cada categoría y un registro de las decisiones analíticas adoptadas durante la lectura (Braun & Clarke, 2021).

La integración final reunió los resultados cualitativos y cuantitativos en una matriz de convergencia que distinguió coincidencias, complementariedades y divergencias entre las obligaciones jurídicas, los riesgos técnicos y las prácticas organizacionales descritas. Las frecuencias se interpretaron como indicadores descriptivos del corpus y no como estimaciones del cumplimiento efectivo de todas las entidades ecuatorianas, en concordancia con el alcance exploratorio y la selección documental no probabilística. El análisis también contrastó las categorías nacionales con principios de gestión del riesgo, protección de la privacidad, supervisión humana, transparencia y rendición de cuentas reconocidos internacionalmente (National Institute of Standards and Technology [NIST], 2023; UNESCO, 2021). Como no se reclutaron participantes ni se recopilaban datos personales directamente, el estudio redujo los riesgos asociados al consentimiento y a la exposición de información sensible. Aun así, se respetaron la atribución de autoría, la finalidad investigativa, la minimización de reproducciones textuales y la anonimización de cualquier ejemplo documental que pudiera facilitar la identificación de personas naturales (Asamblea Nacional del Ecuador, 2021).

3. Resultados

Cumplimiento de las obligaciones de protección de datos en sistemas de inteligencia artificial

El análisis se orientó a identificar la estructura de cumplimiento exigida para el tratamiento de datos personales mediante inteligencia artificial en el núcleo normativo ecuatoriano. El corpus central quedó integrado por tres instrumentos: la Ley Orgánica de Protección de Datos Personales, su Reglamento General y la norma especializada sobre sistemas de inteligencia artificial. Esta última comprendió 10 artículos y delimitó

cuatro funciones sujetas a obligaciones: desarrollador, desplegador, distribuidor e implementador. Asimismo, se identificaron tres derechos expresamente vinculados con el tratamiento automatizado: información, oposición y protección frente a decisiones basadas total o parcialmente en valoraciones automatizadas. Los hallazgos describieron el estándar jurídico aplicable, pero no representaron una medición del cumplimiento efectivo de organizaciones públicas o privadas (Asamblea Nacional del Ecuador, 2021; Presidencia de la República del Ecuador, 2023; Superintendencia de Protección de Datos Personales [SPDP], 2026).

La codificación del artículo 5 de la norma especializada permitió registrar cinco obligaciones principales ($n = 5$) aplicables a responsables y encargados. Al reagruparlas según su finalidad operativa, dos correspondieron a prevención y reducción del riesgo (gestión de riesgos y evaluación de impacto, junto con medidas de seguridad), equivalentes al 40,0 %. Otras dos se relacionaron con trazabilidad y responsabilidad demostrada (registro de actividades de tratamiento y auditoría del sistema), también con una participación del 40,0 %. La obligación restante se concentró en la información clara, específica y transparente dirigida al titular, lo que representó el 20,0 % de las categorías codificadas. Esta distribución mostró un predominio conjunto del 80,0 % de obligaciones orientadas al control preventivo, la documentación y la verificación institucional (SPDP, 2026).

Figura 1

¿Cómo asegurar el cumplimiento en sistemas de IA en Ecuador?



Nota: Autores (2026)

La secuencia normativa evidenció que las obligaciones no se concentraron en una única fase del sistema, sino que se distribuyeron antes, durante y después de su funcionamiento. La evaluación de impacto y la gestión de riesgos se ubicaron antes del desarrollo cuando existió tratamiento de datos personales; en cambio, las medidas de seguridad, el registro y la mitigación de vulnerabilidades adquirieron un carácter permanente. El control posterior se sostuvo mediante auditorías proporcionales al riesgo y mediante la facultad de la autoridad para imponer medidas correctivas o cautelares. Además, el artículo 7 especificó tres medidas operativas continuas: registrar decisiones

automatizadas con efectos jurídicos, implementar controles de riesgo y seguridad, y ejecutar auditorías, equivalentes cada una al 33,3 % de ese conjunto complementario ($n = 3$) (SPDP, 2026).

La dimensión económica del cumplimiento quedó determinada por el régimen sancionatorio aplicable cuando las obligaciones normativas fueron incumplidas. Para servidores o funcionarios públicos, las infracciones leves estuvieron sujetas a multas de entre uno y 10 salarios básicos unificados, mientras que las graves se ubicaron entre 10 y 20 salarios básicos unificados. En entidades privadas y empresas públicas, las infracciones leves representaron entre el 0,1 % y el 0,7 % del volumen de negocio del ejercicio fiscal anterior, y las graves entre el 0,7 % y el 1,0 %. La graduación consideró intencionalidad, reiteración, naturaleza del perjuicio y reincidencia, por lo que no se identificó un monto monetario uniforme aplicable a todos los casos. En síntesis, los hallazgos mostraron una arquitectura regulatoria cuantificable de cinco obligaciones, tres garantías frente a la automatización y cuatro actores responsables, aunque el corpus disponible no permitió calcular medias, desviaciones estándar, intervalos de confianza, valores p ni porcentajes de cumplimiento institucional observado (Asamblea Nacional del Ecuador, 2021; SPDP, 2025, 2026).

Madurez institucional según sector y tipo de aplicación de la inteligencia artificial

El análisis examinó la madurez institucional mediante indicadores de capacidad normativa, gobernanza, infraestructura, adopción pública, desarrollo del ecosistema y resiliencia, debido a que el corpus no proporcionó una medición homogénea del cumplimiento por organización. Las fuentes identificaron la creación de un Comité de Inteligencia Artificial en 2024, la ejecución de una evaluación nacional de preparación y la posterior incorporación de disposiciones específicas sobre tratamiento de datos personales en sistemas automatizados. El proceso diagnóstico incluyó 10 talleres con 91 participantes de instituciones públicas, empresas, academia y sociedad civil, con una media descriptiva de 9,1 participantes por taller. Además, se formularon 29 recomendaciones de política pública, de las cuales 16 fueron clasificadas como prioritarias, equivalentes al 55,2 % del total (UNESCO, 2025; Superintendencia de Protección de Datos Personales [SPDP], 2026).

Los indicadores internacionales mostraron diferencias marcadas entre las dimensiones evaluadas. Ecuador ocupó la posición 66 del índice gubernamental de preparación para la inteligencia artificial y alcanzó su mayor puntuación en adopción del sector público, con 79,31 puntos, seguida de capacidad de política pública, con 76,50, y gobernanza, con 61,63. En contraste, desarrollo y difusión registró 27,94 puntos, mientras que infraestructura de inteligencia artificial obtuvo 47,34 y resiliencia 54,32. La media aritmética simple de los seis puntajes fue de 57,84, con una desviación estándar muestral de 19,18; la diferencia entre la dimensión máxima y la mínima llegó a 51,37 puntos. La distribución completa se presentó en la Tabla 1 (Oxford Insights, 2026).

Tabla 1

Indicadores de preparación institucional para la inteligencia artificial en Ecuador

Dimensión evaluada	Puntaje sobre 100	Orden dentro del perfil nacional
Adopción en el sector público	79,31	1
Capacidad de política pública	76,50	2
Gobernanza	61,63	3

Dimensión evaluada	Puntaje sobre 100	Orden dentro del perfil nacional
Resiliencia	54,32	4
Infraestructura de inteligencia artificial	47,34	5
Desarrollo y difusión	27,94	6
Media descriptiva	57,84	—
Desviación estándar	19,18	—

Nota. Los seis puntajes correspondieron a una escala de 0 a 100. La media y la desviación estándar fueron calculadas descriptivamente a partir de los valores publicados y no sustituyeron la puntuación compuesta oficial del índice. Fuente de los datos: Oxford Insights (2026).

La diferenciación por sector evidenció una mayor disponibilidad de indicadores para el ámbito gubernamental que para las organizaciones privadas. En el ecosistema empresarial se identificaron 25 empresas emergentes relacionadas con inteligencia artificial, mientras que la oferta formativa reunió 45 programas académicos especializados; no obstante, las fuentes no publicaron tasas de adopción empresarial comparables por tamaño, actividad económica o nivel de cumplimiento en protección de datos. Las aplicaciones documentadas se concentraron en cuatro ámbitos: salud, agronegocios, finanzas y banca, junto con usos públicos vinculados con servicios digitales y gestión administrativa. Esta clasificación describió la diversidad sectorial existente, pero los documentos no informaron frecuencias, porcentajes de implementación ni inversiones económicas desagregadas para cada tipo de aplicación (UNESCO, 2025).

Los indicadores habilitantes también mostraron diferencias internas en la capacidad para desplegar sistemas de inteligencia artificial. El país contó con nueve centros de datos, equivalentes a 0,514 por millón de habitantes, mientras que el uso de internet alcanzó al 77,2 % de la población. La conectividad de los hogares se situó en 73,6 % en las áreas urbanas y 48,1 % en las rurales, con una brecha de 25,5 puntos porcentuales; además, el 18,12 % de las personas graduadas de educación superior perteneció a áreas STEM. La evidencia empresarial regional confirmó que la adopción tecnológica varió según tamaño, sector, capital humano y recursos complementarios, aunque la encuesta ecuatoriana revisada no incluyó información específica que permitiera calcular tasas de uso de inteligencia artificial por empresa. En conjunto, los hallazgos describieron una madurez institucional desigual: los mayores puntajes se concentraron en adopción pública y capacidad política, mientras que el desarrollo del sector, la difusión empresarial y la infraestructura presentaron los valores más reducidos (Gutiérrez et al., 2025; UNESCO, 2025).

Relación entre madurez institucional, confianza digital y privacidad percibida

El análisis examinó la correspondencia documental entre la preparación institucional para gobernar la inteligencia artificial, la confianza digital y la percepción de protección sobre los datos personales. Ecuador obtuvo 41,46 puntos sobre 100 en el Índice de Preparación Gubernamental para la Inteligencia Artificial de 2024; sus pilares alcanzaron 34,27 puntos en gobierno, 29,31 en sector tecnológico y 60,79 en datos e infraestructura. La media descriptiva de los tres componentes fue de 41,46 puntos, con una desviación estándar muestral de 16,93 y un rango de 31,48 puntos. Por su parte, la evaluación nacional de la UNESCO comprendió 10 espacios de consulta con 91 participantes y produjo 29 recomendaciones, de las cuales 16 fueron prioritarias, equivalentes al 55,2 %. Las fuentes no incluyeron observaciones vinculadas sobre las

mismas personas u organizaciones, por lo que no se calcularon correlaciones, intervalos de confianza ni valores *p* entre madurez institucional y confianza digital (Oxford Insights, 2024; UNESCO, 2025).

La evidencia nacional mostró que el desarrollo de capacidades digitales coexistió con una valoración mayoritariamente favorable de la inteligencia artificial. El 66 % de las personas consideradas en el indicador citado por la evaluación de la UNESCO estimó que la inteligencia artificial ofrecía más beneficios que desventajas, mientras que el uso de internet alcanzó al 77,2 % de la población. Sin embargo, el diagnóstico también registró una gobernanza fragmentada, 25 empresas emergentes vinculadas con inteligencia artificial, 45 programas académicos especializados y únicamente nueve centros de datos, equivalentes a 0,514 por millón de habitantes. Estos valores revelaron que la aceptación general de la tecnología superó la disponibilidad documentada de capacidades organizacionales, formativas y de infraestructura. No se identificó en el corpus una encuesta ecuatoriana que midiera simultáneamente confianza en los sistemas de inteligencia artificial, conocimiento de la normativa y privacidad percibida, por lo que el 66 % se trató como un indicador de aceptación tecnológica y no como una medida directa de confianza en el tratamiento de datos personales (UNESCO, 2025).

La evidencia internacional incorporada al corpus permitió describir el patrón entre conocimiento normativo y capacidad percibida para proteger la información. El 53 % de las personas encuestadas conoció las leyes de privacidad de su país, proporción que aumentó siete puntos porcentuales respecto del 46 % registrado en 2023. Entre quienes conocieron dichas normas, el 81 % afirmó que podía proteger sus datos personales, frente al 44 % entre quienes las desconocieron, diferencia descriptiva de 37 puntos porcentuales. A su vez, el 59 % manifestó mayor comodidad para compartir información en aplicaciones de inteligencia artificial cuando existieron leyes sólidas de privacidad, mientras que el 62 % expresó esa respuesta ante regulaciones específicas de inteligencia artificial. Aunque el 63 % consideró que la tecnología podía mejorar su vida, el 78 % señaló que las organizaciones debían utilizarla éticamente, lo que vinculó la aceptación tecnológica con expectativas explícitas de protección y responsabilidad institucional (Cisco, 2024a).

El contraste organizacional mostró una brecha entre las prioridades institucionales y los elementos valorados por las personas usuarias. El 91 % de las organizaciones reconoció que necesitaba realizar mayores esfuerzos para garantizar que los datos empleados por la inteligencia artificial se destinaran únicamente a fines legítimos, mientras que el 62 % de los consumidores manifestó preocupación por el uso organizacional de la tecnología y el 60 % indicó haber perdido confianza debido a esas prácticas. La información clara sobre el uso de los datos fue prioritaria para el 37 % de los consumidores, pero las organizaciones concentraron sus respuestas en el cumplimiento normativo (25 %) y la prevención de vulneraciones (23 %). En términos económicos, la inversión organizacional promedio en privacidad fue de USD 2,7 millones y el beneficio estimado alcanzó USD 2,9 millones, con un retorno medio de 1,6 veces la inversión; además, entre el 77 % y el 80 % declaró mayor comodidad cuando se aplicaron supervisión humana, auditorías, transparencia y programas de ética. En síntesis, los hallazgos describieron una asociación consistente entre mayor conocimiento regulatorio, salvaguardas visibles y confianza declarada, aunque no

permitieron atribuir causalidad ni estimar estadísticamente esa relación para la población ecuatoriana (Cisco, 2024a, 2024b).

4. Discusión

El estudio analiza el cumplimiento de la protección de datos personales en entornos de inteligencia artificial y su articulación con la madurez institucional, la confianza digital y la privacidad percibida en Ecuador. Los hallazgos muestran que el país dispone de una arquitectura jurídica definida por cinco obligaciones centrales, tres garantías frente al tratamiento automatizado y cuatro tipos de actores responsables, aunque esta solidez normativa no equivale necesariamente a una implementación institucional efectiva. El predominio de obligaciones asociadas con prevención, seguridad, trazabilidad y auditoría (80 % de las categorías codificadas) sugiere que el modelo regulatorio prioriza la responsabilidad demostrada durante todo el ciclo de vida de los sistemas. Esta orientación resulta pertinente frente a la posibilidad de que los modelos memoricen, infieran o reproduzcan datos personales, incluso cuando se aplican mecanismos descentralizados de aprendizaje (Carlini et al., 2021; Mothukuri et al., 2021). Por tanto, el problema central parece desplazarse desde la ausencia de normas hacia la capacidad organizacional para traducirlas en controles verificables, evaluaciones de impacto y supervisión continua (SPDP, 2026).

La desigual madurez institucional identificada refuerza esta interpretación, debido a que los mayores puntajes se concentran en adopción pública y capacidad de política, mientras que el desarrollo y difusión de la inteligencia artificial, la infraestructura y el ecosistema empresarial presentan resultados inferiores. Esta configuración converge con el Índice Latinoamericano de Inteligencia Artificial, que ubica a Ecuador por debajo del promedio regional en gobernanza y regulación, y con la evaluación nacional que reconoce avances normativos junto con capacidades todavía fragmentadas (CENIA, 2024; UNESCO, 2025). La existencia de 45 programas académicos, 25 empresas emergentes y nueve centros de datos evidencia una base institucional en expansión, pero no garantiza una distribución homogénea de competencias técnicas ni de recursos. La brecha de conectividad de 25,5 puntos porcentuales entre hogares urbanos y rurales también parece indicar que la gobernanza de la privacidad se desarrolla sobre condiciones desiguales de acceso y alfabetización digital (INEC, 2024). Estos resultados coinciden con la evidencia regional que relaciona la adopción tecnológica con el tamaño organizacional, el capital humano y la disponibilidad de recursos complementarios (Gutiérrez et al., 2025).

La relación entre confianza digital y privacidad percibida presenta un patrón semejante: la aceptación general de la inteligencia artificial convive con preocupaciones sobre el uso organizacional de los datos. Aunque el 66 % de las personas incluidas en el indicador nacional considera que la inteligencia artificial ofrece más beneficios que desventajas, esta valoración no constituye una medida directa de confianza en el tratamiento automatizado de información personal (UNESCO, 2025). La evidencia internacional muestra que el conocimiento normativo se asocia con una mayor capacidad percibida para proteger los datos (81 % frente a 44 %) y que entre el 77 % y el 80 % de las personas expresa mayor comodidad cuando existen supervisión humana, auditorías, transparencia y programas de ética (Cisco, 2024a, 2024b). Esta

convergencia sugiere que la confianza no depende exclusivamente de la innovación tecnológica, sino de la visibilidad y credibilidad de las salvaguardas institucionales. Asimismo, la inversión promedio de USD 2,7 millones en privacidad y el beneficio estimado de USD 2,9 millones, con un retorno medio de 1,6 veces, indican que la protección de datos también puede representar valor económico y reputacional para las organizaciones (Cisco, 2024b). No obstante, la asociación debe interpretarse con cautela, porque el diseño documental y transversal no permite establecer causalidad entre madurez, confianza y privacidad percibida.

Las principales limitaciones se derivan de la selección documental no probabilística, la heterogeneidad de los indicadores y la ausencia de observaciones emparejadas sobre las mismas organizaciones y personas usuarias. El corpus tampoco proporciona tasas comparables de adopción o cumplimiento por sector, ni una encuesta ecuatoriana que mida simultáneamente conocimiento regulatorio, confianza en la inteligencia artificial y privacidad percibida, por lo que los resultados no se generalizan a todas las entidades públicas y privadas. Además, las cifras internacionales aportan patrones de referencia, pero no sustituyen evidencia empírica específica del contexto nacional. A partir de estas restricciones, futuras investigaciones deberían aplicar cuestionarios estructurados a personas adultas, auditorías organizacionales y diseños longitudinales que comparen sectores como salud, finanzas, educación y administración pública, incorporando variables de transparencia, equidad, seguridad y supervisión humana (Shaham et al., 2025; NIST, 2023). También resultaría pertinente contrastar el cumplimiento declarado con registros, evaluaciones de impacto y resultados de auditoría, con el fin de estimar la brecha entre regulación y práctica. La contribución central del estudio reside, así, en integrar dimensiones jurídicas, técnicas y organizacionales para mostrar que la privacidad efectiva depende menos de la existencia aislada de normas que de su implementación verificable y de su capacidad para sostener la confianza digital (SPDP, 2026; UNESCO, 2021).

5. Conclusiones

Los resultados permiten concluir que Ecuador dispone de una arquitectura jurídica suficiente para orientar la protección de datos personales en sistemas de inteligencia artificial, pero su eficacia depende de la capacidad institucional para convertir las disposiciones formales en prácticas verificables. Las cinco obligaciones centrales, las tres garantías frente al tratamiento automatizado y la delimitación de cuatro actores responsables configuran un marco integral de prevención, transparencia y rendición de cuentas. Sin embargo, el estudio no demuestra que estas exigencias se apliquen de manera uniforme en las organizaciones públicas y privadas. En consecuencia, la privacidad digital no queda asegurada únicamente por la existencia de normas, sino por la gestión continua de riesgos, la seguridad desde el diseño, la trazabilidad y la auditoría de los sistemas. Esta interpretación debe mantenerse dentro del alcance documental y exploratorio de la investigación.

La integración de los hallazgos vinculados con los objetivos específicos evidencia una madurez institucional desigual entre las dimensiones examinadas. La adopción pública y la capacidad para formular políticas presentan mayor desarrollo que la infraestructura, la difusión empresarial y la consolidación del ecosistema tecnológico, lo cual limita una

implementación homogénea de las obligaciones de protección. A ello se añade la brecha de conectividad de 25,5 puntos porcentuales entre hogares urbanos y rurales, que refleja condiciones diferenciadas para ejercer derechos digitales y comprender el tratamiento automatizado de la información. Asimismo, la aceptación favorable de la inteligencia artificial no equivale necesariamente a confianza en el uso organizacional de datos personales. En conjunto, los resultados sugieren que la confianza digital se fortalece cuando las salvaguardas institucionales son visibles, comprensibles y aplicadas de forma consistente.

El principal aporte del estudio reside en articular las dimensiones jurídica, técnica y organizacional dentro de un mismo marco de análisis, evitando que la privacidad se examine exclusivamente como cumplimiento documental o como problema de ciberseguridad. Esta integración permite reconocer que la protección efectiva requiere coordinación entre responsables, encargados, desarrolladores, desplegados y autoridades de control durante todo el ciclo de vida de la inteligencia artificial. También se observa que la inversión en privacidad puede generar beneficios institucionales, económicos y reputacionales, dado que la evidencia revisada registra una inversión promedio de USD 2,7 millones y un beneficio estimado de USD 2,9 millones. Tales valores no deben extrapolarse directamente a Ecuador, pero muestran que la protección de datos puede concebirse como una capacidad estratégica y no solo como una carga regulatoria. De este modo, la investigación aporta criterios aplicables al diagnóstico institucional y a la evaluación responsable de sistemas automatizados.

A partir de los resultados, se recomienda que las organizaciones prioricen evaluaciones de impacto, registros de decisiones automatizadas, auditorías periódicas, supervisión humana y mecanismos de información comprensibles para las personas titulares. También resulta pertinente fortalecer la formación especializada y reducir las brechas de infraestructura y conectividad que condicionan la participación equitativa en entornos digitales. Las futuras investigaciones deberían medir directamente el cumplimiento institucional y la privacidad percibida mediante cuestionarios, auditorías y diseños longitudinales aplicados a sectores como salud, finanzas, educación y administración pública. Asimismo, convendría contrastar las políticas declaradas con evidencias operativas de seguridad, trazabilidad y respuesta ante vulneraciones. La contribución central del estudio consiste, por tanto, en mostrar que la protección de datos en inteligencia artificial depende de una implementación verificable capaz de reducir riesgos y sostener la confianza digital.

Referencias Bibliográficas

- Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial No. 459, Quinto Suplemento. <https://www.asambleanacional.gob.ec/es/multimedios-legislativos/63464-ley-organica-de-proccion-de-datos>.
- Barahona-Martínez, G. E., Barzola-Plúas, Y. G., & Peñafiel-Muñoz, L. V. (2024). El Derecho a la Protección de Datos y el Avance de las Nuevas Tecnologías en Ecuador: Implicaciones Legales y Éticas. *Journal of Economic and Social Science Research*, 4(3), 46–64. <https://doi.org/10.55813/gaea/jessr/v4/n3/113>

- Barzola-Plúas, Y. G. (2022). Reformas Constitucionales en Ecuador: Impacto y Perspectivas. *Revista Científica Zambos*, 1(1), 86-101. <https://doi.org/10.69484/rcz/v1/n1/23>
- Barzola-Plúas, Y. G., Samaniego-Quigui, D. P., Núñez-Ribadeneyra, R. A., & Bonilla-Morejón, D. M. (2023). Protección de datos personales en la era de la computación cuántica y sus desafíos legales. *Revista Científica Ciencia Y Método*, 1(3), 45-57. <https://doi.org/10.55813/gaea/rcym/v1/n3/19>
- Bonilla-Morejón, D. M., Castro-Morales, S., Mendoza-Armijos, H. E., & Mina-Bone, S. G. (2024). Protección de los derechos fundamentales y control constitucional en Estados democráticos contemporáneos. *Revista Científica Enfoques Del Conocimiento*, 1(1), 73-88. <https://doi.org/10.55813/gaea/revistacec/v1/n1/11>
- Braun, V., & Clarke, V. (2021). *Thematic analysis: A practical guide*. SAGE Publications. <https://www.sagepub.com/shop/buy-a-book/thematic-analysis-1-248481>
- Carlini, N., Tramèr, F., Wallace, E., Jagielski, M., Herbert-Voss, A., Lee, K., Roberts, A., Brown, T. B., Song, D., Erlingsson, Ú., Oprea, A., & Raffel, C. (2021). Extracting training data from large language models. In *30th USENIX Security Symposium* (pp. 2633–2650). USENIX Association. <https://www.usenix.org/conference/usenixsecurity21/presentation/carlini-extracting>
- Castro-Morales, S., & Samaniego-Quigui, 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>
- Centro Nacional de Inteligencia Artificial. (2024). *Índice Latinoamericano de Inteligencia Artificial 2024*. https://indicelatam.cl/wp-content/uploads/2025/01/ILIA_2024_020125_compressed.pdf
- Cisco. (2024a). *Cisco 2024 consumer privacy survey*. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf
- Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3.ª ed.). SAGE Publications.
- Gmyrek, P., Winkler, H., & Garganta, S. (2024). *Buffer or bottleneck? Employment exposure to generative AI and the digital divide in Latin America* (ILO Working Paper No. 121). International Labour Organization & World Bank. <https://doi.org/10.54394/TFZY7681>
- Gutiérrez, L. H., Gallego, J. M., & Herrera Giraldo, M. F. (2025). *Exploring the drivers and performance impacts of advanced digital technologies in Latin American economies* (IDB Technical Note No. 3197). Inter-American Development Bank. <https://doi.org/10.18235/0013728>
- Herrera-Acosta, C. E., Quinancela-Vargas, B. P., Ashca-Vaca, M. K., León-Betancourt, D. M., & Guevara-Tubón, J. E. (2026). Herramientas jurídicas para garantizar los derechos de la naturaleza. *Revista Científica Ciencia Y Método*, 4(1), 209-224. <https://doi.org/10.55813/gaea/rcym/v4/n1/146>

- 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: Julio 2024*. https://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2024/202407_Tecnologia_de_la_Informacion_y_Comunicacion-TICs.pdf
- Jaramillo-Becerra, J. D., Gaibor-Vásconez, L. E., López-Soria, Y., & García-Segarra, H. G. (2025). La discrecionalidad administrativa en el Ecuador: Del uso legítimo a la arbitrariedad – Sentencia No. 1381-17-EP/22. *Revista Científica Ciencia Y Método*, 3(4), 292-308. <https://doi.org/10.55813/gaea/rcym/v3/n4/111>
- Jaramillo-Quezada, D. M., Jaramillo-Rivadeneira, A. M., & Freire-Gaibor, E. F. (2025). El uso indebido del arraigo personal en materia flagrante frente al principio de igualdad. *Revista Científica Ciencia Y Método*, 3(4), 278-291. <https://doi.org/10.55813/gaea/rcym/v3/n4/110>
- Jerez-Granados, J. L. (2026). Brechas entre normativa y práctica en la protección de trabajadores migratorios en Ecuador. *Revista Científica Ciencia Y Método*, 4(1), 14-34. <https://doi.org/10.55813/gaea/rcym/v4/n1/127>
- Lopez-Mallama, O. M., Lemos-Muñoz, A. J., & Córdova-Ardila, Y. P. (2023). Protección Social en la Región Caribe de Colombia: una Mirada desde la Equidad en 2021. *Journal of Economic and Social Science Research*, 3(3), 13–24. <https://doi.org/10.55813/gaea/jessr/v3/n3/70>
- Morgan, H. (2022). Conducting a qualitative document analysis. *The Qualitative Report*, 27(1), 64–77. <https://doi.org/10.46743/2160-3715/2022.5044>
- Mothukuri, V., Parizi, R. M., Pouriye, S., Huang, Y., Dehghantanha, A., & Srivastava, G. (2021). A survey on security and privacy of federated learning. *Future Generation Computer Systems*, 115, 619–640. <https://doi.org/10.1016/j.future.2020.10.007>
- National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.AI.100-1>
- Núñez-Ribadeneyra, R. A. (2023). Derechos Humanos y Justicia Social en el Contexto Ecuatoriano. *Revista Científica Zambos*, 2(3), 42-58. <https://doi.org/10.69484/rcz/v2/n3/49>
- Oxford Insights. (2024). *Government AI readiness index 2024*. <https://oxfordinsights.com/wp-content/uploads/2025/06/2024-Government-AI-Readiness-Index.pdf>
- 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>

- Plúas-Espinoza, D. C., Cabrera-Moreira, J. D., & Rendón-Guerra, G. del P. (2026). Dosimetría punitiva y responsabilidad proactiva: Régimen sancionatorio en el tratamiento de datos en Ecuador. *Revista Científica Ciencia Y Método*, 4(2), 362-382. <https://doi.org/10.55813/gaea/rcym/v4/n2/200>
- Presidencia de la República del Ecuador. (2023). *Decreto Ejecutivo No. 904: Reglamento General de la Ley Orgánica de Protección de Datos Personales*. <https://www.telecomunicaciones.gob.ec/wp-content/uploads/2023/11/Decreto-Ejecutivo-No.-904.pdf>
- Rodriguez-Angulo, D. E., Bajaan-Mendoza, M. V., & Fajardo-Vargas, J. E. (2026). Relación entre condiciones ergonómicas, bienestar laboral y productividad en trabajadores del sector empresarial. *Revista Científica Ciencia Y Método*, 4(2), 383-395. <https://doi.org/10.55813/gaea/rcym/v4/n2/201>
- Samaniego-Quigui, D. P. (2023). Acceso a la Justicia y Equidad en el Sistema Legal Ecuatoriano. *Revista Científica Zambos*, 2(2), 50-62. <https://doi.org/10.69484/rcz/v2/n2/45>
- Samaniego-Quigui, D. P., Gutiérrez-Márquez, E. E., & García-Moreno, M. (2024). Derecho internacional humanitario y protección de civiles en conflictos armados contemporáneos. *Revista Científica Enfoques Del Conocimiento*, 1(4), 41-57. <https://doi.org/10.55813/gaea/revistacec/v1/n4/24>
- Shaham, S., Hajisafi, A., Quan, M. K., Nguyen, D. C., Krishnamachari, B., Peris, C., Ghinita, G., Shahabi, C., & Pathirana, P. N. (2025). Privacy and fairness in machine learning: A survey. *IEEE Transactions on Artificial Intelligence*, 6(7), 1706–1726. <https://doi.org/10.1109/TAI.2025.3531326>
- Superintendencia de Protección de Datos Personales. (2025). *Resolución No. SPDP-SPD-2025-0003-R: Guía de gestión de riesgos y evaluación de impacto del tratamiento de datos personales*. <https://spdp.gob.ec/resolucion-n-spdp-spd-2025-0003-r-guia-de-gestion-de-riesgos-y-evaluacion-de-impacto-del-tratamiento-de-datos-personales-con-su-anexo/>
- Superintendencia de Protección de Datos Personales. (2026). *Norma general para la garantía del derecho de protección de datos personales en el uso de sistemas de inteligencia artificial*. <https://spdp.gob.ec/resoluciones2/>
- Superintendencia de Protección de Datos Personales. (2026). *Resolución No. SPDP-SPD-2026-0009-R: Norma general para la garantía del derecho de protección de datos personales en el uso de sistemas de inteligencia artificial*. <https://spdp.gob.ec/wp-content/uploads/2026/02/ResolliA.pdf>
- UNESCO. (2021). *Recomendación sobre la ética de la inteligencia artificial*. <https://www.unesco.org/es/legal-affairs/recommendation-ethics-artificial-intelligence>
- UNESCO. (2025). *Evaluación del estadio de preparación en materia de inteligencia artificial: Ecuador*. <https://unesdoc.unesco.org/ark:/48223/pf0000396465>

CONFLICTO DE INTERESES

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