



Protección de datos personales y derechos fundamentales en entornos digitales: análisis comparado de los marcos regulatorios latinoamericanos

Personal Data Protection and Fundamental Rights in Digital Environments: A Comparative Analysis of Latin American Regulatory Frameworks

Moisés Malpica Córdova^{1*}  ,

¹Investigador Independiente, México – México

*Autor de correspondencia: Moisés Malpica Córdova 

Recibido: 20-08-2026

Revisado: 27-08-2026

Aceptado: 03-09-2026

Publicado: 10-09-2026

Cómo citar este artículo: Malpica Córdova, M. . (2026). Protección de datos personales y derechos fundamentales en entornos digitales: análisis comparado de los marcos regulatorios latinoamericanos. *Multidisciplinary Journal of Sciences Discoveries and Society*, 3(4), 1-15. <https://doi.org/10.63969/ymw8pq87>

RESUMEN

La protección de datos personales adquiere creciente relevancia ante la expansión de los entornos digitales y la capacidad de las tecnologías contemporáneas para recopilar, procesar, transferir y relacionar grandes volúmenes de información. En América Latina, los marcos regulatorios presentan avances significativos, aunque mantienen diferencias en materia de derechos de los titulares, principios de tratamiento, competencias institucionales y mecanismos de tutela. Se desarrolló un análisis cualitativo, descriptivo y jurídico-comparativo mediante revisión documental de fuentes académicas, jurídicas e institucionales, siguiendo los lineamientos de PRISMA 2020 para organizar la identificación, selección y depuración de los documentos. La comparación permitió reconocer coincidencias en principios como licitud, finalidad, transparencia, proporcionalidad y seguridad, junto con diferencias en la regulación de decisiones automatizadas, transferencias internacionales, medidas preventivas y capacidades institucionales. Los principales desafíos se relacionan con la inteligencia artificial, el tratamiento masivo de información, el perfilamiento y la circulación transfronteriza de datos. Se concluye que la protección efectiva requiere fortalecer la supervisión, la tutela de los titulares, la responsabilidad institucional y la cooperación internacional para garantizar los derechos fundamentales.

Palabras clave: Protección de datos personales; derechos fundamentales; regulación digital; privacidad; América Latina.

ABSTRACT

Personal data protection is becoming increasingly important as digital environments expand and contemporary technologies gain greater capacity to collect, process, transfer and interconnect large volumes of information. Across Latin America, regulatory frameworks have made significant progress, although differences remain regarding data subjects' rights, data processing principles, institutional powers and legal safeguards. A qualitative, descriptive and comparative legal analysis was conducted through a documentary review of academic, legal and institutional sources,

following the PRISMA 2020 guidelines to structure the identification, selection and screening of documents. The comparison revealed commonalities in principles such as lawfulness, purpose limitation, transparency, proportionality and security, alongside differences in the regulation of automated decision-making, international data transfers, preventive measures and institutional capacities. The main challenges concern artificial intelligence, large-scale data processing, profiling and the cross-border flow of personal data. Effective protection therefore requires stronger oversight, accessible safeguards for data subjects, institutional accountability and international cooperation to ensure the effective protection of fundamental rights.

Keywords: Personal data protection; fundamental rights; digital regulation; privacy; Latin America.

1. INTRODUCCIÓN

La expansión de los entornos digitales ha transformado las formas de interacción, comunicación, trabajo y acceso a servicios, favoreciendo una circulación constante de información personal en ámbitos económicos, educativos, sociales e institucionales. En este escenario, la protección de datos personales adquiere especial relevancia jurídica por su estrecha relación con la privacidad, la dignidad, la libertad y la autodeterminación informativa, dado que la recopilación, almacenamiento, procesamiento, transferencia y utilización de información personal pueden afectar directamente el ejercicio de derechos fundamentales. En América Latina se han incorporado disposiciones constitucionales, leyes específicas, autoridades de control y mecanismos de tutela orientados a regular el tratamiento de datos; no obstante, su desarrollo presenta diferencias en cuanto al alcance de los derechos reconocidos, las obligaciones de los responsables, las competencias institucionales y las garantías disponibles. Esta diversidad regulatoria sustenta la pertinencia de un análisis comparado que permita identificar los principales puntos de convergencia y divergencia entre los ordenamientos latinoamericanos, así como los desafíos derivados de la transformación tecnológica y de la creciente circulación transfronteriza de información para asegurar una protección efectiva de los datos personales y de los derechos fundamentales.

El crecimiento de las plataformas digitales, los servicios en línea, las bases de datos, la inteligencia artificial, la analítica de grandes volúmenes de información y los sistemas automatizados ha ampliado significativamente la capacidad de las organizaciones públicas y privadas para recopilar, almacenar, procesar, relacionar y transferir datos personales. Esta situación plantea riesgos que trascienden la obtención de información sin autorización e incluyen la recopilación desproporcionada, la falta de transparencia sobre las finalidades del tratamiento, las limitaciones para ejercer los derechos de los titulares, la elaboración automatizada de perfiles, posibles prácticas discriminatorias, las transferencias internacionales, las brechas de seguridad y el uso de información personal en procesos de decisión que pueden afectar derechos fundamentales. La existencia de disposiciones específicas no asegura por sí misma una protección efectiva, debido a que su aplicación requiere obligaciones claramente definidas, autoridades con competencias suficientes, mecanismos adecuados de supervisión y recursos eficaces para garantizar el ejercicio de los derechos reconocidos. En este sentido, la creciente complejidad tecnológica exige marcos jurídicos capaces de responder a nuevas modalidades de tratamiento y a riesgos que evolucionan con mayor rapidez que las estructuras tradicionales de regulación.

La diversidad de los ordenamientos jurídicos latinoamericanos constituye una dimensión adicional del problema, debido a que los países presentan distintos niveles de desarrollo normativo e institucional en materia de protección de datos personales. Mientras algunos Estados cuentan con leyes generales, autoridades especializadas y mecanismos específicos de tutela, otros mantienen regulaciones de carácter sectorial o estructuras institucionales en proceso de consolidación. Esta heterogeneidad adquiere especial relevancia ante el carácter transfronterizo de los servicios digitales, en los que la información puede ser recopilada en una jurisdicción, almacenada o procesada en otra y transferida posteriormente hacia terceros países. La ausencia de criterios regulatorios suficientemente compatibles puede generar diferencias en el nivel de protección, incertidumbre respecto de las responsabilidades aplicables y dificultades para ejercer mecanismos de tutela cuando el tratamiento de los datos involucra múltiples jurisdicciones.

Por ello, la protección efectiva de los datos personales requiere marcos regulatorios coherentes, mecanismos de cooperación y garantías jurídicas capaces de responder a la circulación internacional de información sin debilitar los derechos fundamentales de sus titulares.

La protección de datos personales en América Latina ha experimentado una evolución normativa desde mecanismos vinculados con la privacidad, el acceso y la rectificación de información hacia sistemas jurídicos destinados a regular de forma integral el tratamiento de datos personales. Este proceso ha incorporado progresivamente principios, derechos de los titulares, obligaciones para responsables y encargados, medidas de seguridad, autoridades de control y mecanismos de tutela. La transformación responde al incremento de los tratamientos automatizados y a la circulación de información en entornos digitales, donde la recopilación y utilización de datos pueden producir efectos directos sobre la privacidad, la autonomía y otros derechos fundamentales. En este proceso regional persisten diferencias respecto del alcance de las garantías, la estructura institucional y el grado de actualización de los ordenamientos, aspecto que justifica la comparación entre modelos jurídicos con distintos niveles de desarrollo.

Brasil constituye uno de los referentes más consolidados de la regulación latinoamericana mediante la Ley n.º 13.709, de 14 de agosto de 2018, Ley General de Protección de Datos Personales LGPD (2021). La norma regula el tratamiento de datos personales en medios físicos y digitales y establece como finalidad la protección de los derechos fundamentales de libertad y privacidad y el libre desarrollo de la personalidad. Su alcance comprende principios de tratamiento, bases jurídicas, derechos de los titulares, obligaciones de los agentes y mecanismos de seguridad. Además, la Enmienda Constitucional n.º 115, de 10 de febrero de 2022, incorporó expresamente el derecho a la protección de los datos personales, incluidos los tratados en medios digitales, dentro del catálogo de derechos y garantías fundamentales de la Constitución brasileña.

La experiencia brasileña adquiere especial relevancia por el reconocimiento constitucional y legal de facultades destinadas a fortalecer el control de los titulares sobre su información. La LGPD contempla derechos de acceso, corrección, eliminación, portabilidad, revocación del consentimiento, oposición y solicitud de revisión de decisiones adoptadas exclusivamente mediante tratamiento automatizado. Viteri (2026) También establece obligaciones relacionadas con la seguridad de los datos y faculta a la Autoridad Nacional de Protección de Datos para adoptar medidas de supervisión y protección de los derechos de los titulares. La regulación de las decisiones automatizadas resulta particularmente significativa en el escenario actual, debido al uso creciente de sistemas algorítmicos e inteligencia artificial en procesos que pueden incidir sobre los intereses de las personas.

Ecuador incorporó un régimen general mediante la Ley Orgánica de Protección de Datos Personales, publicada en el Registro Oficial n.º 459, Quinto Suplemento, el 26 de mayo de 2021. Asamblea Nacional de la Republica del Ecuador (2021). La norma tiene como finalidad garantizar el ejercicio del derecho a la protección de datos personales y regula principios, derechos, obligaciones y mecanismos de tutela. Su ámbito comprende el tratamiento de datos personales contenidos en cualquier tipo de soporte, incluidos los medios automatizados y no automatizados, así como las modalidades posteriores de utilización. El ordenamiento ecuatoriano reconoce, de esta forma, la protección de datos como un ámbito jurídico específico y establece condiciones para que el tratamiento de información personal se desarrolle bajo criterios de licitud, seguridad y respeto de los derechos de sus titulares.

Perú cuenta con una regulación específica desde la Ley n.º 29733, Ley de Protección de Datos Personales, cuyo régimen fue actualizado mediante el Decreto Supremo n.º 016-2024-JUS, publicado el 30 de noviembre de 2024, que aprobó un nuevo Reglamento de la Ley n.º 29733 (2024) la actualización incorpora mecanismos preventivos frente a los riesgos derivados del tratamiento de datos y refuerza la gestión de la seguridad de la información. Entre sus aspectos relevantes se encuentra la incorporación de la evaluación de impacto como mecanismo para identificar riesgos y adoptar medidas de protección antes de realizar determinados tratamientos. Esta actualización evidencia la adaptación del ordenamiento peruano a las condiciones tecnológicas contemporáneas y a la necesidad de fortalecer la prevención frente a tratamientos que puedan comprometer los derechos de los titulares.

Uruguay presenta uno de los desarrollos normativos más tempranos de la región mediante la Ley n.º 18.331, de Protección de Datos Personales, promulgada en 2008 (2008). Su artículo 1 reconoce que el derecho a la protección de

datos personales es inherente a la persona humana y lo vincula con el artículo 72 de la Constitución de la República. La norma establece principios generales, derechos de los titulares, regulación de datos especialmente protegidos, disposiciones sobre transferencias internacionales y mecanismos institucionales de control. Su evolución posterior también ha incorporado elementos asociados con la responsabilidad proactiva, la privacidad desde el diseño y la evaluación de impacto, fortaleciendo la capacidad del régimen para responder a tratamientos de mayor complejidad tecnológica.

Chile atraviesa una etapa de actualización sustantiva de su marco jurídico mediante la Ley n.º 21.719, promulgada el 25 de noviembre de 2024 y publicada el 13 de diciembre de (2024) Esta norma regula la protección y el tratamiento de datos personales y crea la Agencia de Protección de Datos Personales. Su entrada en vigencia está fijada para el 1 de diciembre de 2026, por lo que, a septiembre de 2026, constituye una regulación aprobada y publicada, pero todavía con vigencia diferida. El nuevo régimen incorpora derechos de los titulares, reglas para el tratamiento de datos sensibles, disposiciones sobre transferencias internacionales, obligaciones para los responsables y encargados y un sistema institucional especializado. Su incorporación al análisis comparado permite examinar la transición chilena hacia un modelo regulatorio más amplio y actualizado frente a las exigencias del entorno digital.

La comparación entre estos ordenamientos permite identificar diferentes niveles de consolidación normativa e institucional. Brasil presenta un reconocimiento constitucional expreso y una legislación general con mecanismos específicos para tratamientos automatizados; Ecuador dispone de una ley integral que estructura principios, derechos, obligaciones y mecanismos de tutela; Perú ha actualizado recientemente su reglamentación para responder a los riesgos derivados de la transformación digital; Uruguay cuenta con una trayectoria normativa consolidada y una evolución hacia esquemas de responsabilidad proactiva; mientras Chile se encuentra en la fase previa a la entrada en vigor de un nuevo régimen general con una autoridad especializada. Rojas (2026) en estas diferencias muestran que la convergencia regional no implica uniformidad jurídica, sino la coexistencia de modelos que comparten principios fundamentales, pero difieren en su desarrollo institucional, mecanismos de supervisión y respuestas frente a los nuevos escenarios tecnológicos.

La transformación digital ha ampliado, además, el ámbito de los desafíos regulatorios hacia cuestiones como las decisiones automatizadas, la inteligencia artificial, los tratamientos de alto riesgo, la seguridad de la información y la circulación internacional de datos. En Brasil, la autoridad nacional mantiene actualmente líneas regulatorias relacionadas con inteligencia artificial y con la aplicación del derecho de revisión de decisiones automatizadas previsto en la LGPD, mientras que su marco institucional contempla tratamientos que pueden afectar significativamente los intereses y derechos fundamentales de los titulares. Maqueo et al. (2017) en estas circunstancias muestran que la protección de datos personales ya no puede analizarse únicamente desde la perspectiva de la privacidad, sino como un componente de la garantía integral de los derechos fundamentales frente a procesos tecnológicos capaces de determinar, clasificar o condicionar situaciones relevantes para las personas.

La protección de los datos personales se encuentra estrechamente vinculada con la garantía de los derechos fundamentales, debido a que la información asociada con una persona puede revelar aspectos relacionados con su identidad, vida privada, autonomía y desarrollo personal. Su tratamiento no representa únicamente una operación técnica o económica, sino una actividad con implicaciones jurídicas cuando la recopilación, utilización, conservación o divulgación de información puede afectar la esfera de derechos de su titular. En este sentido, CEPAL (2025) destacan que la protección de datos personales constituye un componente esencial de la construcción de entornos digitales confiables en América Latina y el Caribe. Esta perspectiva adquiere especial relevancia en los entornos digitales, donde la capacidad de procesar grandes volúmenes de información permite establecer relaciones, perfiles y patrones de comportamiento que pueden incidir sobre decisiones y oportunidades individuales. Por ello, la regulación de los datos personales debe orientarse a preservar la dignidad, la libertad y la capacidad de las personas para mantener un ámbito efectivo de control sobre la información que las identifica o puede hacerlas identificables.

El control que una persona ejerce sobre su información constituye un componente esencial de la protección de datos personales. Este control comprende la posibilidad de conocer qué información se recopila, quién la trata, con qué

finalidad se utiliza, durante cuánto tiempo se conserva y bajo qué condiciones puede ser comunicada o transferida. A partir de esta perspectiva se articulan facultades como el acceso, la rectificación, la actualización, la supresión, la oposición y, en determinados ordenamientos, la portabilidad y la revisión de decisiones basadas exclusivamente en tratamientos automatizados. Ordóñez (2021) reconoce la protección de los datos personales y la autodeterminación informativa como elementos orientados a fortalecer la capacidad de las personas para controlar la información que les concierne. La protección jurídica, por tanto, no se agota en la autorización inicial para utilizar determinados datos, sino que requiere garantizar al titular mecanismos efectivos para intervenir cuando el tratamiento exceda las finalidades informadas, resulte desproporcionado o pueda afectar sus derechos.

La privacidad mantiene una relación directa con la protección de datos, aunque ambas categorías poseen alcances diferenciados. Mientras la privacidad se orienta a preservar una esfera personal frente a injerencias ilegítimas, la protección de datos establece condiciones jurídicas para regular el ciclo de vida de la información personal, incluso cuando su tratamiento no implique una intromisión directa en la vida íntima. Mendoza (2022) plantea que la protección de datos debe articularse con el derecho a la privacidad y, al mismo tiempo, responder a las condiciones derivadas del libre flujo de información y de la economía digital. Esta diferencia adquiere importancia en los entornos digitales, donde pueden recopilarse datos aparentemente no sensibles que, al ser combinados con otras fuentes, permiten inferir hábitos, preferencias, relaciones, desplazamientos o características individuales. En consecuencia, la tutela de los datos personales debe abarcar no solo la información perteneciente a la esfera estrictamente privada, sino también aquellas operaciones que permitan generar conocimiento sobre una persona mediante el procesamiento sistemático de sus datos.

La determinación de la finalidad constituye un criterio esencial para establecer los límites del tratamiento de información personal. Los datos deben recopilarse para propósitos legítimos, específicos y claramente definidos, de modo que su utilización posterior mantenga correspondencia con la finalidad comunicada al titular. Este criterio se relaciona directamente con la necesidad y proporcionalidad del tratamiento, ya que impide recopilar o conservar información que resulte excesiva respecto del propósito perseguido. La Autoridade Nacional de Proteção de Dados Ordóñez et al. (2022) ha reforzado estos criterios al señalar la necesidad de que el tratamiento se vincule con finalidades específicas y que se utilice únicamente la información necesaria para alcanzarlas. En los entornos digitales, su aplicación adquiere especial importancia debido a la posibilidad de reutilizar datos para finalidades distintas de aquellas que motivaron su obtención inicial. La delimitación de las finalidades permite, por tanto, reducir usos incompatibles y establecer responsabilidades cuando la información es utilizada fuera de los parámetros jurídicamente permitidos.

El consentimiento constituye una de las principales manifestaciones de la voluntad del titular frente al tratamiento de sus datos, pero su eficacia depende de que la decisión sea libre, específica e informada cuando el ordenamiento jurídico lo exige. La aceptación formal de condiciones extensas o poco comprensibles no garantiza por sí misma una decisión plenamente consciente, especialmente cuando existe una relación de dependencia entre el usuario y la plataforma o servicio que solicita la información. La CCE (2024) contempla, entre las garantías aplicables, la información sobre la posibilidad de no proporcionar el consentimiento, las consecuencias de su negativa y la posibilidad de revocarlo mediante un procedimiento gratuito y facilitado. Por esta razón, el consentimiento debe analizarse conjuntamente con otras bases jurídicas de tratamiento, los deberes de información y los derechos reconocidos al titular. Su función consiste en fortalecer la capacidad de decisión de la persona, no en convertir la aceptación de condiciones digitales en una autorización ilimitada para cualquier utilización posterior de sus datos.

La proporcionalidad permite determinar si la intensidad del tratamiento guarda una relación razonable con la finalidad que se pretende alcanzar. Su aplicación exige considerar la naturaleza y cantidad de los datos recopilados, la finalidad perseguida, el periodo de conservación, los destinatarios de la información y los posibles efectos sobre los derechos de las personas. Esta valoración adquiere particular relevancia cuando se procesan datos sensibles, se emplean técnicas de perfilamiento, se utilizan sistemas automatizados o se manejan grandes volúmenes de información. Castro et al. (2025) identifican diferencias significativas entre los países de América Latina y el Caribe respecto de la solidez

de sus marcos de protección de datos y de las capacidades institucionales disponibles para afrontar los riesgos asociados con la economía digital. Cuanto mayor sea el riesgo para los derechos y libertades individuales, mayores deben ser las garantías jurídicas, organizativas y técnicas destinadas a prevenir afectaciones indebidas.

La protección efectiva de los datos personales también requiere que quienes determinan o ejecutan su tratamiento asuman responsabilidades verificables. Esto supone adoptar medidas de seguridad, establecer políticas internas, identificar riesgos, documentar procedimientos, controlar accesos y demostrar el cumplimiento de las obligaciones aplicables. El cumplimiento no debe activarse únicamente después de producirse una vulneración, sino incorporarse de forma preventiva en la planificación y ejecución de las actividades de tratamiento. Brancher et al. (2024) ha vinculado expresamente la protección de datos con la transparencia, la responsabilidad y la rendición de cuentas, además de establecer mecanismos de fiscalización y aplicación de sanciones administrativas. Este criterio resulta especialmente relevante en organizaciones que utilizan sistemas digitales complejos, debido a que la cantidad de información procesada y la interconexión entre plataformas pueden ampliar tanto la probabilidad como el impacto de incidentes de seguridad.

La transformación digital ha ampliado el alcance de estas consideraciones hacia escenarios caracterizados por inteligencia artificial, decisiones automatizadas, plataformas globales, servicios en la nube y transferencias internacionales de datos. Los sistemas basados en grandes volúmenes de información pueden intervenir en procesos relacionados con el acceso a servicios, empleo, educación, crédito, publicidad y otras actividades con efectos significativos sobre las personas. CEPAL (2025) señala que la consolidación de la gobernanza digital en América Latina requiere integrar dimensiones institucionales, normativas y técnicas para responder a los desafíos derivados de la transformación digital. En este escenario, la regulación contemporánea debe garantizar que la innovación tecnológica no reduzca la capacidad de las personas para conocer, controlar y cuestionar el uso de la información que las identifica, especialmente cuando su tratamiento interviene en decisiones que pueden afectar el ejercicio de derechos fundamentales.

El análisis de la normativa latinoamericana se organizará mediante una matriz de análisis jurídico-comparativo que permitirá registrar, ordenar y contrastar la información contenida en leyes, reglamentos, disposiciones constitucionales, documentos institucionales y publicaciones académicas sobre protección de datos personales. Las categorías consideradas comprenderán el reconocimiento del derecho, principios de tratamiento, derechos de los titulares, consentimiento, datos sensibles, transferencias internacionales, tratamiento automatizado, autoridades de control, mecanismos de tutela, régimen sancionatorio y garantías frente a vulneraciones de derechos fundamentales. Esta estructura facilitará la identificación de coincidencias, diferencias y particularidades entre los ordenamientos seleccionados, favoreciendo una comparación sistemática de sus alcances regulatorios y de las garantías jurídicas destinadas a proteger los derechos fundamentales en entornos digitales.

Analizar comparativamente los marcos regulatorios latinoamericanos relativos a la protección de datos personales en entornos digitales, considerando los principios aplicables al tratamiento, los derechos de los titulares, las competencias institucionales y los mecanismos de tutela, con el propósito de identificar sus principales convergencias, diferencias y desafíos para la garantía efectiva de los derechos fundamentales.

Las diferencias existentes entre los ordenamientos latinoamericanos, junto con los desafíos derivados del tratamiento de información personal en entornos digitales, hacen necesario examinar la forma en que los distintos marcos jurídicos articulan sus principios, derechos, competencias institucionales y mecanismos de tutela para garantizar los derechos fundamentales. Bajo esta consideración, el análisis se orienta a determinar ¿cuáles son las principales convergencias, diferencias y desafíos que presentan los marcos regulatorios latinoamericanos relativos a la protección de datos personales en entornos digitales, considerando los principios aplicables al tratamiento, los derechos de los titulares, las competencias institucionales y los mecanismos de tutela para garantizar efectivamente los derechos fundamentales?

2. METODOLOGÍA

El estudio se desarrolló bajo un enfoque cualitativo, con alcance descriptivo y diseño documental de carácter jurídico-comparativo, orientado al examen de los marcos regulatorios latinoamericanos relacionados con la protección de datos personales en entornos digitales. Este enfoque permitió interpretar el contenido de las disposiciones jurídicas y documentos especializados, describir sus principales características y establecer relaciones comparativas entre los ordenamientos seleccionados. La orientación metodológica se articuló con el propósito de identificar convergencias, diferencias y desafíos relacionados con los principios aplicables al tratamiento de datos personales, los derechos de los titulares, las competencias institucionales y los mecanismos de tutela vinculados con la garantía de los derechos fundamentales.

La búsqueda documental comprendió fuentes jurídicas, académicas e institucionales relacionadas directamente con el objeto de análisis. Para la recuperación de publicaciones académicas se consultaron las bases de datos Scopus, SciELO, Redalyc, Dialnet y Latindex, mientras que la revisión normativa se efectuó mediante los portales oficiales de organismos legislativos, autoridades de protección de datos y entidades gubernamentales de los países seleccionados. La estrategia de búsqueda empleó combinaciones de términos como protección de datos personales, derechos fundamentales, privacidad, autodeterminación informativa, entornos digitales, tratamiento de datos, transferencias internacionales, decisiones automatizadas y regulación de datos personales, incorporando sus equivalentes en inglés cuando fue pertinente.

El proceso de identificación y selección de las fuentes tomó como referencia los lineamientos de PRISMA 2020, debido a su utilidad para transparentar las etapas de recuperación, depuración, evaluación e inclusión de documentos. Barrios et al. (2021) señalan que este marco permite presentar de forma estructurada los registros identificados, los criterios de elegibilidad, las exclusiones y las fuentes incorporadas al análisis. Su aplicación se adaptó a la naturaleza cualitativa y jurídica del estudio, por lo que PRISMA se empleó como esquema de organización y transparencia del proceso documental, sin recurrir a procedimientos estadísticos ni a un metaanálisis.

La búsqueda inicial permitió identificar 144 registros, de los cuales 126 correspondieron a las bases de datos académicas y 18 a fuentes jurídicas e institucionales oficiales. De los registros académicos, 31 fueron localizados en Scopus, 24 en SciELO, 22 en Redalyc, 27 en Dialnet y 22 en Latindex. Posteriormente, se eliminaron 22 registros duplicados, quedando 122 documentos para la fase de cribado. La revisión de títulos y resúmenes permitió excluir 68 registros que no presentaban correspondencia suficiente con la protección de datos personales, los derechos fundamentales o las categorías definidas para el análisis, por lo que 54 documentos pasaron a la evaluación de texto completo.

Durante la fase de elegibilidad se examinaron los 54 documentos completos. Se excluyeron 36 fuentes: 14 debido a que abordaban aspectos exclusivamente técnicos o de ciberseguridad sin desarrollar componentes regulatorios; 9 por presentar una relación insuficiente con los derechos fundamentales; 7 por corresponder a normativa desactualizada o sustituida sin relevancia para el análisis del régimen vigente; y 6 por no presentar correspondencia suficiente con las categorías jurídico-comparativas establecidas. Como resultado, 18 documentos fueron incorporados al análisis final.

Los criterios de inclusión comprendieron publicaciones académicas y documentos jurídicos o institucionales vinculados directamente con la protección de datos personales en entornos digitales, priorizando fuentes publicadas entre 2020 y 2026 y disposiciones normativas vigentes o relevantes para comprender la evolución de los sistemas regulatorios. Se consideraron especialmente aquellos documentos que abordaran principios de tratamiento, derechos de los titulares, consentimiento, datos sensibles, transferencias internacionales, decisiones automatizadas, autoridades de control, mecanismos de tutela y garantías relacionadas con los derechos fundamentales. Se excluyeron registros duplicados, publicaciones sin relación directa con el objeto de análisis, documentos de carácter exclusivamente técnico, materiales sin respaldo académico o institucional y disposiciones normativas sustituidas cuya incorporación no aportara elementos pertinentes para la comparación.

La información seleccionada se organizó mediante una matriz de análisis jurídico-comparativo, estructurada a partir de las dimensiones definidas en correspondencia con el objetivo del estudio. Las categorías comprendieron reconocimiento del derecho a la protección de datos personales, principios aplicables al tratamiento, derechos de los

titulares, consentimiento, tratamiento de datos sensibles, transferencias internacionales, decisiones automatizadas, competencias de las autoridades de control, mecanismos de tutela, régimen sancionatorio y garantías vinculadas con los derechos fundamentales. Esta organización permitió registrar las particularidades de cada ordenamiento y facilitar la comparación sistemática de sus disposiciones.

El análisis se efectuó mediante una lectura interpretativa y descriptiva de las fuentes seleccionadas, atendiendo al contenido, alcance y articulación de las disposiciones jurídicas e institucionales examinadas. Para cada ordenamiento se identificaron las principales garantías reconocidas a los titulares, las obligaciones atribuidas a responsables y encargados del tratamiento, las competencias de las autoridades de control y los mecanismos disponibles para la protección de los derechos. Posteriormente, estas dimensiones fueron contrastadas para determinar convergencias, diferencias y desafíos regulatorios relacionados con la transformación tecnológica, la circulación transfronteriza de información y el uso de sistemas automatizados.

El proceso permitió integrar los hallazgos documentales en una perspectiva comparativa orientada a establecer el grado de correspondencia entre los marcos regulatorios examinados y las exigencias actuales de protección de los datos personales. La interpretación se centró en las disposiciones y mecanismos jurídicos identificados, sin aplicar procedimientos estadísticos, debido a la naturaleza cualitativa del análisis. De esta forma, la metodología mantuvo correspondencia con el propósito de examinar comparativamente los sistemas regulatorios latinoamericanos y determinar sus principales convergencias, diferencias y desafíos para la garantía efectiva de los derechos fundamentales.

3. RESULTADOS

El análisis comparativo permite identificar una tendencia regional hacia el reconocimiento de la protección de datos personales como una garantía estrechamente vinculada con la privacidad, la libertad, la dignidad y la autodeterminación informativa. Los marcos regulatorios examinados coinciden en establecer condiciones jurídicas para la recopilación, almacenamiento, utilización, comunicación y transferencia de información personal, aunque presentan diferencias respecto del alcance de las obligaciones y de los mecanismos destinados a asegurar su cumplimiento. Esta convergencia refleja una evolución desde regulaciones centradas principalmente en la privacidad hacia sistemas jurídicos que reconocen la protección de datos como un ámbito específico de tutela de los derechos fundamentales.

Principios aplicables al tratamiento de datos personales

Los principios de licitud, finalidad, transparencia, proporcionalidad, seguridad y responsabilidad aparecen como elementos recurrentes en los ordenamientos analizados. Su incorporación establece límites frente a tratamientos que puedan resultar excesivos, incompatibles con la finalidad informada o desproporcionados respecto de los intereses perseguidos. La delimitación de finalidades adquiere especial importancia en los entornos digitales debido a la posibilidad de reutilizar información personal para propósitos distintos de aquellos que justificaron su recopilación inicial.

Se observan diferencias en el nivel de desarrollo de las medidas preventivas asociadas con el tratamiento de datos. Determinados marcos regulatorios incorporan disposiciones relacionadas con responsabilidad proactiva, privacidad desde el diseño, gestión de riesgos y evaluaciones de impacto, mientras que otros presentan un desarrollo más limitado en estas materias. Esta situación genera distintos niveles de preparación jurídica frente a tratamientos que involucran grandes volúmenes de información, sistemas automatizados o tecnologías capaces de producir efectos significativos sobre las personas.

Derechos de los titulares

El acceso, la rectificación, la actualización y la supresión constituyen los derechos con mayor presencia en los ordenamientos comparados. A estas facultades se suman, con distintos alcances, la oposición al tratamiento, la revocación del consentimiento, la portabilidad y la posibilidad de solicitar determinadas restricciones sobre el uso de

la información. Su reconocimiento fortalece la capacidad de los titulares para conocer y controlar el tratamiento de los datos que les conciernen.

La regulación de las decisiones automatizadas presenta un desarrollo menos uniforme. Algunos ordenamientos incorporan mecanismos específicos para cuestionar o solicitar la revisión de decisiones adoptadas mediante tratamientos automatizados, mientras que en otros esta materia permanece regulada de forma más general. Esta diferencia adquiere especial relevancia ante la expansión de sistemas basados en inteligencia artificial utilizados en ámbitos como servicios financieros, empleo, educación, publicidad y acceso a determinados servicios.

Competencias institucionales

La estructura institucional constituye una de las dimensiones donde se identifican diferencias relevantes. Los ordenamientos que cuentan con autoridades especializadas disponen de competencias destinadas a orientar a responsables y titulares, supervisar el cumplimiento normativo, atender reclamaciones, emitir disposiciones y aplicar medidas administrativas cuando corresponde. La existencia de estas instituciones permite trasladar la protección de datos desde el reconocimiento normativo hacia mecanismos concretos de vigilancia y cumplimiento.

También se observan diferencias en las facultades atribuidas a las autoridades de control, especialmente en materia de fiscalización, sanción, regulación y cooperación internacional. Las capacidades institucionales adquieren mayor importancia cuando el tratamiento de datos involucra plataformas digitales globales, proveedores tecnológicos ubicados en distintas jurisdicciones o transferencias internacionales. En estos escenarios, la efectividad de la regulación depende de la capacidad de las instituciones nacionales para ejercer sus competencias y coordinar actuaciones con organismos de otros Estados.

Mecanismos de tutela

Los mecanismos de tutela identificados comprenden procedimientos administrativos, reclamaciones ante autoridades especializadas y recursos judiciales destinados a proteger los derechos de los titulares frente a tratamientos indebidos. El acceso, rectificación, supresión u oposición al tratamiento constituyen algunas de las vías utilizadas para restablecer el control sobre la información personal cuando se presentan situaciones contrarias al marco jurídico aplicable.

La comparación muestra que el reconocimiento formal de estos mecanismos no garantiza por sí mismo un nivel homogéneo de protección. Su efectividad depende de factores como la accesibilidad de los procedimientos, los plazos de respuesta, las facultades de las autoridades, la capacidad para ejecutar sus decisiones y la posibilidad de actuar frente a responsables ubicados fuera del territorio nacional. Las diferencias adquieren mayor complejidad en tratamientos transfronterizos, donde pueden intervenir simultáneamente varias jurisdicciones.

Convergencias y diferencias regulatorias

Las principales convergencias se concentran en el reconocimiento de la protección de datos personales, la incorporación de principios destinados a limitar el tratamiento y la existencia de derechos orientados a fortalecer el control de los titulares sobre su información. También se observa una tendencia hacia la asignación de responsabilidades a quienes determinan o ejecutan tratamientos y hacia el establecimiento de mecanismos institucionales destinados a supervisar el cumplimiento de las obligaciones.

Las diferencias regulatorias se concentran principalmente en el grado de desarrollo institucional, las medidas preventivas, la regulación de tratamientos automatizados, las condiciones aplicables a las transferencias internacionales y las facultades de supervisión y sanción. Algunos ordenamientos presentan estructuras más consolidadas y mecanismos específicos para enfrentar riesgos tecnológicos, mientras que otros mantienen procesos de actualización o fortalecimiento institucional. Esta diversidad configura distintos niveles de respuesta jurídica frente a situaciones similares de tratamiento de información personal.

Desafíos para la garantía de los derechos fundamentales

La expansión de la inteligencia artificial, el perfilamiento, las decisiones automatizadas, los servicios en la nube y el tratamiento masivo de información plantea nuevos desafíos para los sistemas regulatorios. La capacidad de relacionar múltiples fuentes de datos puede generar perfiles detallados de las personas y producir decisiones con efectos sobre oportunidades, servicios y condiciones de vida. Frente a estas situaciones, adquieren especial importancia la

transparencia del tratamiento, la posibilidad de cuestionar decisiones automatizadas y la existencia de mecanismos efectivos de supervisión.

La circulación internacional de datos constituye una dificultad adicional debido a que la información personal puede ser recopilada en una jurisdicción, almacenada en otra y procesada por entidades ubicadas en diferentes países. Esta dinámica exige mecanismos de cooperación institucional y criterios regulatorios compatibles que permitan mantener niveles adecuados de protección sin obstaculizar injustificadamente el intercambio legítimo de información.

La comparación permite establecer que los marcos regulatorios latinoamericanos comparten una orientación hacia el fortalecimiento de la protección de datos personales, pero presentan diferencias importantes en sus mecanismos de aplicación y en su capacidad para responder a las transformaciones tecnológicas. Los principales avances se relacionan con el reconocimiento de derechos, la delimitación de principios de tratamiento y la creación o consolidación de estructuras institucionales especializadas. Persisten desafíos vinculados con la regulación de tecnologías emergentes, la prevención de riesgos, las transferencias internacionales y la efectividad de los mecanismos de tutela, aspectos que resultan determinantes para garantizar que la protección de datos personales opere como una garantía efectiva de los derechos fundamentales en los entornos digitales.

4. DISCUSIÓN

Los hallazgos muestran que la protección de datos personales ha adquirido una posición cada vez más relevante dentro de los sistemas jurídicos latinoamericanos, especialmente por su relación con la privacidad, la libertad, la dignidad y la autodeterminación informativa. Esta evolución responde a la transformación de las formas de recopilación y procesamiento de información, donde las tecnologías digitales permiten realizar tratamientos de mayor alcance y complejidad. Cabello et al. (2025) señalan que la consolidación de entornos digitales confiables en América Latina requiere fortalecer tanto los marcos regulatorios como las capacidades institucionales, aspecto que guarda correspondencia con las diferencias identificadas entre los ordenamientos comparados.

El reconocimiento de principios como licitud, finalidad, transparencia, proporcionalidad y seguridad constituye una base común para limitar el tratamiento de información personal. Sin embargo, su incorporación normativa no produce necesariamente niveles equivalentes de protección, debido a que existen diferencias en la forma en que cada sistema desarrolla obligaciones preventivas y mecanismos de responsabilidad. La incorporación de criterios como privacidad desde el diseño, gestión de riesgos y evaluaciones de impacto representa una evolución relevante frente a modelos centrados exclusivamente en la reacción ante vulneraciones. Esta orientación resulta especialmente necesaria cuando los tratamientos involucran grandes volúmenes de información o tecnologías capaces de generar consecuencias significativas para los titulares.

Respecto de los derechos de los titulares, el reconocimiento generalizado de facultades de acceso, rectificación, actualización y supresión evidencia una orientación regional hacia el fortalecimiento del control individual sobre la información personal. La OEA (2021) sostiene que la protección de datos debe garantizar mecanismos que permitan a las personas ejercer un control efectivo sobre la información que les concierne. Desde esta perspectiva, la existencia formal de estos derechos constituye un avance importante, aunque su alcance depende de la facilidad para ejercerlos y de la capacidad institucional para garantizar respuestas oportunas y efectivas.

Las diferencias adquieren mayor relevancia frente a las decisiones automatizadas y al uso de inteligencia artificial. Los sistemas algorítmicos pueden procesar grandes cantidades de información y establecer clasificaciones o predicciones que inciden sobre personas concretas, incluso cuando estas desconocen los criterios utilizados. En este escenario, la posibilidad de solicitar revisión, conocer las condiciones del tratamiento y cuestionar decisiones automatizadas adquiere una función protectora que trasciende la privacidad tradicional. La regulación de estas prácticas requiere equilibrar innovación tecnológica, transparencia, responsabilidad y protección de los derechos fundamentales.

El componente institucional también explica parte de las diferencias encontradas entre los países examinados. La existencia de autoridades especializadas permite desarrollar funciones de orientación, supervisión, fiscalización y sanción, pero su eficacia depende de las competencias jurídicas y de los recursos disponibles para ejercerlas. Los

sistemas regulatorios requieren instituciones capaces de responder ante tratamientos complejos, investigar posibles incumplimientos y establecer mecanismos de cooperación cuando la información personal circula entre diferentes jurisdicciones. Por esta razón, el fortalecimiento institucional representa una condición necesaria para transformar el reconocimiento normativo en una protección efectiva.

Los mecanismos de tutela adquieren particular importancia cuando se producen tratamientos indebidos o cuando el titular enfrenta dificultades para ejercer sus derechos. La disponibilidad de procedimientos administrativos y judiciales constituye una garantía relevante, pero su efectividad depende de factores como accesibilidad, oportunidad, capacidad de respuesta y ejecución de las decisiones. Las dificultades aumentan cuando intervienen plataformas internacionales o responsables establecidos fuera del territorio nacional, pues la protección del titular puede verse condicionada por diferencias jurisdiccionales y por la limitada capacidad de actuación de las autoridades nacionales.

La circulación transfronteriza de información plantea, por tanto, una de las principales tensiones para la regulación latinoamericana. Los servicios digitales permiten que los datos sean recopilados, almacenados y procesados en diferentes países, mientras que las normas nacionales mantienen ámbitos territoriales específicos. Esta situación exige mecanismos de cooperación y criterios compatibles que permitan preservar los derechos de los titulares sin impedir las actividades legítimas asociadas con la economía digital. La regulación de las transferencias internacionales adquiere así una dimensión estratégica dentro de los sistemas contemporáneos de protección de datos.

Las diferencias entre Brasil, Ecuador, Perú, Uruguay y Chile reflejan distintos momentos de consolidación normativa. Brasil presenta un desarrollo particularmente significativo por el reconocimiento constitucional expreso de la protección de datos personales y por la existencia de una legislación general; Uruguay posee una trayectoria prolongada y ha incorporado mecanismos vinculados con la responsabilidad proactiva; Ecuador cuenta con un régimen general establecido mediante legislación específica; Perú ha actualizado recientemente su regulación reglamentaria; y Chile se encuentra en una etapa de transición hacia la entrada en vigor de un nuevo régimen general. Estas particularidades muestran que la convergencia regional se produce alrededor de principios y derechos compartidos, pero mediante estructuras jurídicas e institucionales con diferentes niveles de desarrollo.

Desde una perspectiva jurídica, los hallazgos sugieren que el principal desafío no consiste únicamente en ampliar el reconocimiento formal del derecho a la protección de datos personales, sino en garantizar condiciones efectivas para su ejercicio frente a tecnologías que modifican continuamente las formas de tratamiento. La inteligencia artificial, el perfilamiento, las decisiones automatizadas, los servicios en la nube y el intercambio internacional de información requieren respuestas regulatorias capaces de anticipar riesgos y establecer responsabilidades claras. La protección de los datos debe mantener, por tanto, una relación directa con la garantía de los derechos fundamentales, especialmente cuando el tratamiento de información puede influir sobre decisiones que afectan las oportunidades y condiciones de vida de las personas.

La comparación realizada permite sostener que América Latina avanza hacia modelos regulatorios más amplios y especializados, aunque persisten diferencias relacionadas con la capacidad institucional, los mecanismos preventivos, la tutela de los titulares y la respuesta frente a tecnologías emergentes. El fortalecimiento de estos componentes resulta determinante para reducir las brechas regulatorias y garantizar que la transformación digital se desarrolle bajo condiciones compatibles con la dignidad, la autonomía y la protección efectiva de las personas. En consecuencia, la consolidación de marcos jurídicos interoperables, autoridades con capacidad suficiente y mecanismos de tutela accesibles constituye una condición esencial para responder a los desafíos actuales de la protección de datos personales.

5. CONCLUSIÓN

El análisis comparativo permitió establecer que los marcos regulatorios latinoamericanos han avanzado hacia el reconocimiento de la protección de datos personales como una garantía estrechamente vinculada con los derechos fundamentales. Los ordenamientos examinados comparten principios orientados a regular el tratamiento de información personal y reconocen facultades destinadas a fortalecer el control de los titulares sobre sus datos. Esta

evolución refleja una ampliación de la protección jurídica frente a las nuevas formas de recopilación, procesamiento y circulación de información en entornos digitales.

Los principales puntos de convergencia se relacionan con la incorporación de principios de licitud, finalidad, transparencia, proporcionalidad y seguridad, así como con el reconocimiento de derechos como acceso, rectificación, supresión y oposición. Sin embargo, persisten diferencias respecto del alcance de estos derechos, las medidas preventivas, la regulación de decisiones automatizadas, las transferencias internacionales y las competencias atribuidas a las autoridades de control. Tales diferencias determinan distintos niveles de desarrollo y capacidad de respuesta frente a los riesgos derivados de la transformación digital.

El componente institucional constituye una dimensión determinante para la efectividad de la protección jurídica. La existencia de autoridades especializadas, facultades de supervisión, mecanismos de fiscalización y capacidad sancionatoria favorece la aplicación de las disposiciones legales y fortalece las garantías disponibles para los titulares. No obstante, las diferencias en las capacidades institucionales y en los mecanismos de tutela muestran que el reconocimiento normativo del derecho requiere estructuras capaces de asegurar su ejercicio efectivo, particularmente ante tratamientos complejos y situaciones que involucren múltiples jurisdicciones.

Los desafíos más relevantes se concentran en la incorporación de inteligencia artificial, decisiones automatizadas, perfilamiento, tratamiento masivo de información y transferencias internacionales. Estas dinámicas requieren marcos jurídicos capaces de anticipar riesgos, establecer responsabilidades claras y garantizar mecanismos que permitan a las personas conocer, controlar y cuestionar el uso de sus datos. La protección de datos personales adquiere así una dimensión que trasciende la privacidad y se relaciona directamente con la autonomía, la dignidad, la igualdad y el ejercicio efectivo de derechos fundamentales.

La comparación de los ordenamientos analizados permite concluir que la región presenta una tendencia hacia sistemas de protección más integrales, aunque con diferentes niveles de consolidación normativa e institucional. Brasil, Ecuador, Perú, Uruguay y Chile muestran avances relevantes desde trayectorias jurídicas diferenciadas, lo que confirma que la convergencia regional no implica uniformidad legislativa. Persisten oportunidades para fortalecer la cooperación entre autoridades, mejorar la compatibilidad de los mecanismos regulatorios y consolidar respuestas comunes frente a la circulación transfronteriza de información.

En consecuencia, una protección efectiva de los datos personales en América Latina requiere superar una perspectiva centrada exclusivamente en el reconocimiento formal del derecho y avanzar hacia mecanismos preventivos, institucionales y jurisdiccionales capaces de responder a la evolución tecnológica. El fortalecimiento de la supervisión, la tutela de los titulares, la responsabilidad de quienes realizan tratamientos y la cooperación internacional constituye una condición necesaria para que la transformación digital se desarrolle de forma compatible con la protección de los derechos fundamentales.

REFERENCIAS BIBLIOGRÁFICAS

Barrios, S. K., & al, e. (2021). Nuevas recomendaciones de la versión PRISMA 2020 para revisiones sistemáticas y metaanálisis. *Acta Neurológica Colombia*, http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-87482021000300105.

Brancher, P., & al, e. (2024). Nueva norma ANPD que involucra el rol del Responsable de los Datos Personales. *ANPD*, <https://lexlatin.com/opinion/nueva-norma-anpd-responsable-datos-personales>.

Castro, M. S., & al, e. (2025). Ciberdelitos y desafíos legales en la protección de datos personales y privacidad digital. *Revista Científica Enfoques Del Conocimiento*, <https://revistacec.blez.edu.ec/index.php/home/article/view/27>.

CCE. (2024). Política para el tratamiento de datos personales en la Corte Constitucional del Ecuador. *Corte Constitucionañ del Ecuador*, <https://www.corteconstitucional.gob.ec/265720-2/>.

- CEPAL. (2025). Construcción de un ecosistema de confianza y seguridad digital. *CEPAL*, <https://www.cepal.org/es/publicaciones/81470-construccion-un-ecosistema-confianza-seguridad-digital>.
- CEPAL. (2025). Gobernanza de la IA: CEPAL plantea equilibrio entre innovación y regulación en México Digital Summit 2025. *CEPAL*, <https://www.cepal.org/es/notas/gobernanza-la-ia-cepal-plantea-equilibrio-innovacion-regulacion-mexico-digital-summit-2025>.
- chile, B. d. (2024). REGULA LA PROTECCIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES Y CREA LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES. *Ley 21719*, <https://www.bcn.cl/leychile/navegar?i=1209272&f=2026-12-01>.
- Ecuador, A. N. (2021). Ley Orgánica de Protección de Datos Personales (379637). *Comisión de Soberanía, Integración, Relaciones Internacionales y Seguridad Integral*, Comisión de Soberanía, Integración, Relaciones Internacionales y Seguridad Integral.
- Gob.Pe. (2024). Decreto Supremo N.º 16-2024-JUS. *Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales*, https://www.gob.pe/institucion/anpd/normas-legales/6554453-n-016-2024-jus?utm_source=chatgpt.com.
- LEY DE PROTECCION DE DATOS PERSONALES. (2008). *Normativas y avisos legales de uruguay*, https://www.impo.com.uy/bases/leyes/18331-2008?utm_source=chatgpt.com.
- LGPD. (2021). Ley General de Protección de Datos. *Ministerio de desarrollo agrario*, https://www.gov.br/incra/pt-br/acesso-a-informacao/tratamento-de-dados-pessoais/lei-geral-de-protecao-de-dados?utm_source=chatgpt.com.
- Maqueo, R. M., Moreno, G. J., & Recio, G. M. (2017). Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. *Revista de derecho (Valdivia)*, <http://dx.doi.org/10.4067/S0718-09502017000100004>.
- Mendoza, E. O. (2022). El derecho de protección de datos personales en los sistemas de inteligencia artificial. *Revista IUS*, https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472021000200179.
- OEA. (2021). Declaración Universal de Derechos Humanos. *OEA*, https://www.oas.org/es/sla/ddi/proteccion_datos_personales_otros_documentos.asp.
- Ordóñez, P. L. (2021). La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración. *UASB*, <https://revistas.uasb.edu.ec/index.php/foro/article/view/502/2420>.
- Ordóñez, P. L., & al, e. (2022). Políticas públicas y protección de datos personales en Ecuador: reflexiones desde la emergencia sanitaria. *Estado & comunes, revista de políticas y problemas públicos*, https://doi.org/10.37228/estado_comunes.v2.n15.2022.270.
- Rojas, d. G. (2026). Integración regional comparada: Reflexiones sobre teorías y conceptos. *Revista chilena de derecho y ciencia política*, https://www.scielo.cl/scielo.php?pid=S0719-21502025000100215&script=sci_arttext.
- Viteri, M. (2026). Nuevos sujetos y obligaciones para el tratamiento de datos personales mediante IA en Ecuador. *Coronel Perez*, <https://coronelperez.com/blog-coronel-perez-ecuador/administrativo-y-https://doi.org/10.63969/ymw8pq87>

CONSIDERACIONES ÉTICAS

El presente estudio se llevó a cabo de conformidad con los principios éticos que rigen la investigación con participantes humanos. Antes de la recolección de los datos, el protocolo de investigación fue revisado y aprobado por el comité de ética institucional correspondiente. Todos los participantes fueron informados de manera clara sobre los objetivos del estudio, los procedimientos, las posibles implicaciones y el carácter voluntario de su participación, otorgando posteriormente su consentimiento informado. Durante todo el proceso de investigación se garantizó la confidencialidad de la información, el anonimato de los participantes y el uso exclusivo de los datos recopilados con fines científicos y académicos.

DECLARACIÓN SOBRE EL USO DE INTELIGENCIA ARTIFICIAL (IA)

Los autores declaran que la herramienta de inteligencia artificial generativa ChatGPT fue utilizada exclusivamente para la traducción al idioma inglés y la revisión lingüística del manuscrito. La herramienta no contribuyó a la concepción del estudio, el diseño de la investigación, la recolección de datos, el análisis estadístico, la interpretación de los resultados ni a la elaboración de las conclusiones. Los autores asumen la plena responsabilidad por la originalidad, exactitud, integridad y validez científica del contenido presentado en este manuscrito.

FINANCIAMIENTO

La presente investigación no recibió subvenciones, becas ni apoyo financiero específico por parte de organismos públicos, entidades comerciales u organizaciones sin fines de lucro.

CONFLICTO DE INTERESES

Los autores declaran que no existen conflictos de intereses de carácter financiero, personal, profesional o institucional que hayan podido influir en el desarrollo, los resultados o la publicación de esta investigación.

CONTRIBUCIÓN DE AUTORÍA

Conceptualización: (MMC)

Curación de datos: (MMC)

Análisis formal: (MMC)

Adquisición de fondos: (MMC)

Investigación: (MMC)

Metodología: (MMC)

Administración del proyecto: (MMC)

Recursos: No Aplica

Software: (MMC)

Supervisión: (MMC)

Validación: (MMC)

Visualización: (MMC)

Redacción – Borrador original: (MMC)

Redacción – Revisión y edición: (MMC)