

GOBERNANZA RESPONSABLE DE LA INTELIGENCIA ARTIFICIAL EN MIPYMES: ANÁLISIS COMPARADO DE COLOMBIA, PERÚ, URUGUAY Y CHILE

RESPONSIBLE GOVERNANCE OF ARTIFICIAL INTELLIGENCE MSMES: A COMPARATIVE ANALYSIS OF COLOMBIA, PERU, URUGUAY AND CHILE

Marco Antonio Ruiz Nieves¹
Jairo Jamith Palacios Rozo²
Lugo Manuel Barbosa Guerrero³

Cómo citar: Ruiz Nieves, M. A., Palacios Rozo, J. J., & Barbosa Guerrero, L. M. (2026). Gobernanza responsable de la inteligencia artificial en Mipymes: análisis comparado de Colombia, Perú, Uruguay y Chile. *Conocimiento Global*, 11(S1), 464-475. <https://doi.org/10.70165/cglobal.v11iS1.711>

Resumen

En este artículo se realiza un análisis comparativo de la capacidad de los marcos de gobernanza de inteligencia artificial (IA) de Colombia, Perú, Uruguay y Chile para convertir principios de uso responsable en controles aplicables a micro, pequeñas y medianas empresas (mipymes). La presente investigación fue cualitativa, documental y jurídico-comparada, organizada en las siguientes seis categorías: fuerza vinculante de los instrumentos, gestión del riesgo, gobernanza de datos, transparencia y trazabilidad, supervisión humana y responsabilidad y proporcionalidad empresarial. A través del análisis, se pudo evidenciar una convergencia regional en cuanto a protección de datos, seguridad, transparencia y control humano; por otro lado, se identificaron diferencias en la naturaleza jurídica y la obligatoriedad de los instrumentos. Asimismo, se observó que las restricciones de infraestructura, formación y capacidad organizacional representan una problemática para convertir dichos principios en procedimientos internos; también se identifica una brecha de trazabilidad organizacional entre la declaración de uso responsable y la posibilidad de reconstruir la selección, la autorización, la utilización y la supervisión del sistema. En este estudio se concluye que la gobernanza aplicable a las mipymes requiere un núcleo mínimo de controles graduados de acuerdo con los riesgos, que no disminuya la garantía de la protección de los derechos debido al tamaño de la organización.

Palabras clave: gobernanza; inteligencia artificial; mipymes; responsabilidad; trazabilidad.

Abstract

This paper presents a comparative analysis of the capacity of artificial intelligence (AI) governance frameworks in Colombia, Peru, Uruguay, and Chile to translate responsible use

Recepción: 25 de junio de 2026 / Evaluación: 28 de julio de 2026 / Aprobado: 26 de septiembre de 2026

¹Magíster en Derechos Humanos y Derecho Internacional Humanitario. Docente-Investigador de la Universidad Es docente investigador y profesor asociado de la Corporación Unificada Nacional de Educación Superior (CUN), Email: marco_ruiz@cun.edu.co ORCID: <https://orcid.org/0000-0001-5963-5180>

² Magister en Administración de Negocios Internacionales Docente-Investigador de la Universidad Colegio Mayor de Cundinamarca Email: jipalacios@universidadmayor.edu.co ; ORCID: <https://orcid.org/0000-0002-1437-9838>

³ Doctor en Administración de Empresas. Docente-Investigador de la Universidad Colegio Mayor de Cundinamarca Email: lmbarbosa@universidadmayor.edu.co ORCID: <https://orcid.org/0000-0002-0871-8637>



principles into controls applicable to micro, small, and medium-sized enterprises (MSMEs). This qualitative, documentary, and legal-comparative research was organized into the following six categories: binding force of the instruments, risk management, data governance, transparency and traceability, human oversight, and corporate responsibility and proportionality. The analysis revealed regional convergence in data protection, security, transparency, and human oversight; however, differences were identified in the legal nature and enforceability of the instruments. Furthermore, infrastructure, training, and organizational capacity limitations were observed as obstacles to translating these principles into internal procedures. An organizational traceability gap was also identified between the declaration of responsible use and the ability to reconstruct the selection, authorization, use, and oversight of the system. In conclusion, governance applicable to SMEs requires a minimum core of risk-based graduated controls, without reducing the protection of rights due to the size of the organization.

Keywords: accountability; artificial intelligence; governance; MSMEs; traceability.

Introducción

La incorporación de sistemas de inteligencia artificial en las micro, pequeñas y medianas empresas ha dejado de estar reservada a organizaciones con amplias capacidades tecnológicas. Las plataformas generativas, los asistentes virtuales y las herramientas de análisis predictivo permiten automatizar actividades de mercadeo, servicio al cliente, gestión financiera, selección de personal y administración de inventarios. Sin embargo, la reducción de las barreras de acceso no implica que las empresas hayan desarrollado simultáneamente capacidades para comprender el funcionamiento de los sistemas, controlar los datos utilizados, evaluar sus riesgos o asignar responsabilidades por los resultados obtenidos. En América Latina, la adopción empresarial de inteligencia artificial enfrenta dificultades relacionadas con la infraestructura tecnológica, el talento especializado, los costos de implementación y la integración con los sistemas existentes (Bravo et al., 2026). Hernández et al. (2026) coincide en que el proceso para incorporar estas tecnologías se ve limitado por barreras económicas, técnicas y formativas, pese al aumento de la producción científica sobre este tema (Yaranga y Olórtiga, 2025). Lo anterior no influye solamente en el desempeño financiero, sino que disminuye la capacidad de las mipymes para identificar las herramientas usadas, analizar las condiciones de sus proveedores y revisar los resultados antes de la toma de decisiones; es por esto que la transformación digital necesita que se articulen, de acuerdo con los objetivos, tecnología, personas, cultura y estructura organizacional (del Do et al., 2023).

A nivel jurídico, la gobernanza de la IA no se limita a formular principios éticos, sino que su efectividad depende de que se puedan verificar la supervisión humana, la transparencia y la responsabilidad. Divino (2024), en ese sentido, identificó problemas para individualizar al responsable, sesgos, acciones discriminatorias y posibles afectaciones a la privacidad; además, el procesamiento automatizado de mucha información requiere un tratamiento responsable y transparente para proteger los derechos de sus titulares (Martínez, 2019), lo que es más relevante en sistemas generativos que pueden recopilar, recombinar o inferir datos personales (Sánchez, 2024). Entonces, la gobernanza responsable incluye determinar el objetivo del sistema, los datos que puede procesar, la persona que supervisa y las condiciones bajo las cuales sus resultados pueden usarse. Esta problemática se vuelve especialmente relevante en las mipymes, donde las decisiones son tomadas por pocas personas y dependen, generalmente, de proveedores externos. Lo descrito no las exenta de riesgos jurídicos, aunque sí impide trasladar mecánicamente

estructuras de cumplimiento diseñadas para grandes organizaciones. La proporcionalidad requiere la graduación de los controles con base en el propósito del sistema, la información sensible y la gravedad de sus efectos, sin que el tamaño empresarial las exima de la protección de datos, la transparencia o la responsabilidad.

El presente artículo realiza una comparación jurídica funcional entre Colombia, Perú, Uruguay y Chile, sin generalizar los resultados a Latinoamérica. La pregunta orientadora de esta investigación es: ¿En qué medida los marcos de gobernanza de la IA adoptados en estos países ofrecen mecanismos proporcionales, operativos y verificables para gestionar los riesgos derivados de su uso en las mipymes? El objetivo es analizar comparativamente estos marcos para determinar su capacidad de traducir los principios de IA responsable en controles aplicables a estas organizaciones. La investigación tiene un enfoque cualitativo, documental y jurídico-comparado y se estructura en las siguientes seis categorías: naturaleza jurídica y fuerza vinculante de los instrumentos; gestión del riesgo; protección y gobernanza de datos; transparencia y trazabilidad; supervisión humana y responsabilidad; proporcionalidad frente a las capacidades de las mipymes. Se parte de la proposición de que la convergencia regional en principios no garantiza su implementación efectiva, dado que puede persistir una brecha de trazabilidad entre la declaración empresarial de uso responsable y la capacidad de reconstruir cómo se seleccionó, autorizó, utilizó y supervisó un sistema de IA.

Marco teórico

La gobernanza de la IA es el conjunto de principios, procesos, responsabilidades y mecanismos de control que permite diseñar, implementar y supervisar sistemas automatizados; tiene un alcance que sobrepasa lo técnico, puesto que las decisiones relacionadas con dichos sistemas pueden repercutir en la privacidad, la seguridad y el acceso a bienes o servicios. La gobernanza de la IA hace referencia a definir bajo qué condiciones esta puede implementarse en una organización sin desplazar el juicio humano ni debilitar la responsabilidad.

En primer lugar, la IA es un sistema heterogéneo, por lo que no deben ofrecerse respuestas jurídicas homogéneas, también es cuestionable que las declaraciones éticas sustituyan el discurso jurídico, al no contar con instrumentos institucionales que garanticen su cumplimiento (Robles, 2020); los principios buscan orientar a desarrolladores, proveedores y usuarios, su eficiencia depende de la transparencia, la supervisión humana y de asumir responsabilidades. En la gobernanza de la IA se requiere precisar la toma de decisiones, la finalidad de su uso, sus fuentes de información, los posibles riesgos y la supervisión; también incorporar reglas de gobierno y cumplimiento en los procesos corporativos (Divino, 2024). Desde esa perspectiva, el uso responsable de la IA representa la capacidad institucional para guiarla, analizarla y responder por sus posibles riesgos.

Con respecto a dicha capacidad, Castañeda (2024) afirma que la gobernanza de la IA puede articularse con estructuras de gobierno de tecnologías de la información, siempre que estas se adapten a las responsabilidades, la toma de decisiones y los procesos de seguimiento. Es preciso aclarar que la investigación de este autor se desarrolla en educación superior, pero es útil para las mipymes, debido a que plantea que las organizaciones pueden incorporar controles de IA en adquisición de tecnología, seguridad y administración de la información.

Por otro lado, Martínez y Vega (2020) exponen una situación en la que autoridades, sector privado, academia y sociedad toman parte en la discusión sobre protección de datos, ciberseguridad, derechos humanos y sesgos. Esto no solo resulta efectivo cuando influye en la determinación de responsabilidades, criterios de evaluación y mecanismos de rendición de

cuentas, sino que corre el riesgo de seguir siendo una instancia consultiva que no influye en las decisiones tecnológicas. En ese orden de ideas, el enfoque basado en riesgo parte de reconocer que los sistemas de IA producen los mismos daños ni traen consigo las mismas consecuencias, puesto que los controles varían según su finalidad, los datos procesados, la autonomía, los afectados y la posibilidad de revertir las afectaciones; esto evita someter todas las aplicaciones a las mismas cargas e impide que la innovación sea la base para una autorregulación sin garantías jurídicas.

Ahora bien, se debe mencionar el Reglamento Europeo, que distingue prácticas prohibidas, sistemas de alto riesgo y obligaciones diferenciadas para proveedores e implementadores (Díaz, 2024; Espinosa de los Monteros y Sanz, 2024; Grijalva, 2024); para este análisis, resulta útil porque expone que la proporcionalidad puede concretarse a través de clasificación previa, documentación, supervisión y vigilancia. Además, investigaciones recientes, como las de Otero et al. (2026) y Quirós (2025), establecen que la estabilidad del marco debe relacionarse con la capacidad de adaptación a los avances tecnológicos y sus efectos a nivel financiero.

Por otra parte, es posible diferenciar entre las respuestas a las amenazas extraordinarias y las sustentadas en la gestión del riesgo; las últimas permiten incorporar las preocupaciones tecnológicas en regulaciones ordinarias y tomar medidas preventivas sin afectar la deliberación pública (Ulloa y Bas, 2025). Asimismo, el riesgo debe incluir fallas técnicas, opacidad, tratamiento inadecuado de datos, discriminación, dependencia del proveedor e imposibilidad de determinar quién toma las decisiones.

Una adecuada gestión de los sistemas de IA necesita mecanismos de trazabilidad, lo que se refiere a la posibilidad de reconstruir el ciclo de utilización a través de evidencia sobre su objetivo, proveedor, versión, datos usados, resultados, supervisión humana y decisiones. Esto se debe a que se requiere seleccionar la información que permita explicar el procedimiento, identificar errores y atribuir responsabilidades. La experiencia de documentación de sistemas algorítmicos públicos en Latinoamérica ratifica el valor institucional de inventariar herramientas, entidades responsables, finalidades y características importancia para hacer visible su uso (Gutiérrez et al., 2025). Si bien ello no incluye mipymes, ofrece un criterio transferible al ámbito privado y es que sin un registro mínimo de los sistemas incorporados, la organización no puede contar con una base estable para la evaluación de riesgos, la atención de reclamaciones y el control ejercido.

Martínez (2019), con relación al principio de responsabilidad en materia de protección de datos, sostiene que el procesamiento de información por medio de IA requiere medidas éticas, responsables y transparentes, al ser difícil controlar grandes volúmenes de información y sus posibles reutilizaciones. Es por esto que no es suficiente que una organización afirme que respeta la privacidad, sino que debe dar evidenciar de los datos que usa, para qué, cuánto tiempo los conserva y que no son reutilizados. En este punto, conviene mencionar que la supervisión humana complementa la trazabilidad y permite conservar un ámbito efectivo de deliberación, es necesario garantizar una intervención competente, informada y con capacidad de cuestionamiento, tomando en cuenta que la efectividad del control requiere que el responsable conozca los límites del sistema, tenga información suficiente y pueda detener, cambiar o rechazar la decisión. Cuando esa revisión solo busca confirmar la salida producida, la organización aparenta que hay intervención humana mientras le otorga el poder de decisión al sistema o su proveedor.

En esa línea de ideas, la responsabilidad organizacional debe asegurar que la distribución de funciones entre desarrolladores, proveedores, administradores y usuarios no produzca

indeterminación. Esto quiere decir que, aunque la organización usuaria no controle necesariamente esta tecnología, puede decidir si la incorpora a sus procesos y utiliza sus resultados. Como se ha dicho, esto requiere establecer deberes en cuanto a selección del sistema, delimitación de su objetivo, evaluación de las condiciones contractuales y revisión de sus posibles efectos. En organizaciones pequeñas, la proporcionalidad permite adecuar dichos deberes a la naturaleza del caso y las capacidades institucionales. Las limitaciones en cuanto a recursos, infraestructura y personal capacitado dificultan que una mipyme reproduzca modelos complejos de cumplimiento, pero no disminuye la protección a trabajadores, consumidores o titulares de datos. Por tanto, lo correcto en términos jurídicos no es excluir a estas empresas de responsabilidad, sino formular controles simplificados.

Al respecto, se ha evidenciado que las pymes enfrentan incertidumbre sobre cómo empezar estos procesos, restricciones económicas y ausencia de liderazgo digital (del Do et al., 2023). De forma similar, Bravo et al. (2026) identificaron problemas de infraestructura, formación, costos e integración tecnológica entre las mipymes de Latinoamérica. Por su parte, Romero et al. (2024) muestran que el aprovechamiento de información en pequeñas empresas requiere la transformación de registros operativos en datos para la toma de decisiones, lo que exige calidad, integración y principios de administración de información. Estas condiciones corroboran la necesidad de un esquema que pueda operar a través de registros básicos de herramientas, clasificación de usos, responsables identificados, reglas mínimas sobre datos y revisión reforzada para decisiones que puedan tener mayores efectos. De acuerdo con lo anterior, la proporcionalidad no quiere decir flexibilización indiscriminada del cumplimiento, sino concentrar los controles más rigurosos sobre aplicaciones que puedan afectar derechos o tener efectos relevantes. Una herramienta usada para organizar información pública no demanda el mismo nivel de documentación que un sistema utilizado para escoger trabajadores, evaluar clientes o elaborar perfiles financieros. Esta graduación permite armonizar capacidad empresarial y protección jurídica, además de brindar un criterio para analizar si los marcos de Colombia, Perú, Uruguay y Chile cuentan con mecanismos accesibles y verificables para las mipymes.

Metodología

Esta investigación se llevó a cabo con la finalidad de examinar la gobernanza responsable de la IA en mipymes de Colombia, Perú, Uruguay y Chile, por medio de la articulación de un componente documental comparado y uno de carácter empírico. El primero se orientó a identificar los marcos jurídicos, políticos e institucionales sobre gestión del riesgo, protección de datos, transparencia, supervisión humana y responsabilidad. Para lo cual se definió una matriz común de revisión por país, junto a controles nacionales diferenciados cuando las particularidades normativas lo requirieran; esto permitió delimitar las categorías para la comparación y los criterios incorporados al instrumento de recolección.

Por otro lado, el componente empírico fue diseñado con base en un instrumento de diagnóstico sobre adopción y gobernanza responsable de IA. Los documentos de planeación establecieron como objetivo obtener 400 respuestas válidas y la vinculación de 30 mipymes, además de un piloto de intervención con al menos 10 empresas; estas cifras corresponden a propósitos metodológicos, mas no a resultados alcanzados. Los documentos revisados no precisan el procedimiento definitivo de selección de participantes, la distribución de cuotas entre países ni la composición efectiva de la muestra, por lo que dichos elementos no se completan por medio de estimaciones o inferencias. El instrumento se construyó a partir de dimensiones, hipótesis, indicadores y una ficha estadística, razón por la cual, antes de aplicarse, se previó

realizar un juicio de expertos, con un objetivo de validez de contenido igual o superior a 0,80, una prueba piloto para examinar la confiabilidad inicial, la pertinencia de los ítems y las condiciones operativas del trabajo de campo. La guía de actores asignó al equipo metodológico validar el instrumento, revisar sesgos y definir criterios de aceptación, mientras que la mesa técnico-metodológica tuvo a su cargo conceptualizar el instrumento, la base de datos y el análisis. Teniendo en cuenta que los documentos señalan que estas actividades todavía están pendientes, no se atribuye al instrumento un índice de validez o confiabilidad que no haya sido calculado efectivamente. La recolección se realizó mediante formularios y registros sometidos a controles semanales de cobertura, consistencia y completitud. De igual forma, el protocolo tuvo en cuenta consentimiento, minimización de datos, anonimización de ser necesaria, diccionario de variables y bloqueo de registros que no cumplieran los requisitos técnicos y/o jurídicos. Previo al análisis, se fijó una calidad mínima del 95 % de registros válidos; debajo de ese umbral, los documentos disponen la suspensión de procesamiento hasta completar la depuración.

Para el tratamiento de los datos se previó el uso de JASP y técnicas de modelación de ecuaciones estructurales, a fin de analizar las relaciones entre las dimensiones determinadas en el instrumento. Los resultados se organizarían a través de indicadores de madurez, brechas, cobertura, calidad, formación y trazabilidad, para ser representados en un tablero de Power BI. Empero, los documentos aportados no contienen todavía una base cerrada, estimaciones estadísticas ni resultados de modelación; por tanto, este apartado expone el diseño metodológico previsto y debe actualizarse cuando termine la validación, se ejecute el trabajo de campo y se verifique la calidad de los datos.

Resultados

Este análisis documental evidenció que la gobernanza de la IA en Colombia, Perú, Uruguay y Chile no se desarrolla a través de un instrumento jurídico homogéneo, dado que los cuatro países poseen normas de protección de información personal, políticas públicas, lineamientos administrativos y recomendaciones técnicas con aplicaciones y fuerzas vinculantes diferentes. Esa pluralidad no permite hablar de un régimen regional uniforme, pero sí identificar una orientación compartida hacia el uso responsable, la prevención de riesgos, la transparencia y la protección de los afectados. El primer resultado es una convergencia material de principios acompañada por una divergencia jurídica sobre los instrumentos utilizados.

En Colombia, se identificaron como referentes la Ley 1581 de 2012, la Circular Externa 002 de 2024 de la Superintendencia de Industria y Comercio y el CONPES 4144 de 2025. Al compararlos, se pudieron distinguir tres planos: el régimen vinculante de protección de datos personales, las instrucciones administrativas sobre tratamiento de información en sistemas de IA y la orientación programática de la política nacional. Lo descrito resultó necesario porque el CONPES formula objetivos de política pública, pero no sustituye las obligaciones legales aplicables a responsables y encargados del tratamiento. La responsabilidad demostrada, el objetivo, la autorización, la seguridad y la circulación restringida de los datos se evidenciaron como elementos jurídicos capaces de proyectarse sobre el uso empresarial de herramientas automatizadas, incluso cuando la regulación no se haya diseñado solo para mipymes.

Los estudios jurídicos del contexto colombiano permitieron notar que el tratamiento de grandes volúmenes de datos a través de sistemas automatizados modifica las condiciones de garantía de derechos de sus titulares. Martínez (2019) se refirió a problemas para controlar la reutilización, circulación y combinación de información personal en un régimen de un contexto tecnológico distinto; además, Sánchez (2024) indica que los sistemas generativos incrementan la

vulnerabilidad cuando la innovación es más rápida que las respuestas regulatorias. López y Quintero (2025), en términos penales, analizan la exposición de la intimidad frente a usos tecnológicos que puedan tener riesgos sobre el tratamiento de información personal; por otra parte, Delgado y Espinoza (2024) resaltan que el hecho de que una herramienta sea lícita no la excluye de los daños derivados de su uso inadecuado. Por lo anterior, la problemática identificada no fue solo de tipo normativa, sino que se relacionó con la capacidad empresarial para documentar el cumplimiento y prevenir sus efectos.

En el Perú, se analizaron la Ley 29733 sobre protección de datos personales y su reglamentación, la Ley 31814 y el Decreto Supremo 115-2025-PCM, y se pudo notar que en este país se clasifican los usos con base en los riesgos y se incluyen consecuencias de acuerdo con el impacto del sistema, a diferencia de un modelo sustentado en orientación política. Esto favorece la identificación de aplicaciones prohibidas, posibles riesgos y uso ordinario; sin embargo, no se pudo establecer cómo las mipymes han implementado esas categorías ni cómo pueden cumplir los requerimientos, de manera que no se considera evidencia de aplicación empresarial efectiva.

En el caso de Uruguay, se identificaron la Ley 18.331, el Decreto 64/020 y la Estrategia Nacional de Inteligencia Artificial 2024-2030, cuyo análisis permitió identificar una articulación entre protección de datos, responsabilidad, privacidad y gobernanza multiactor, de modo que su enfoque está en construir capacidades, institucionalidad y coordinación. No obstante, su naturaleza programática requiere diferenciar entre líneas de política pública y obligaciones jurídicamente exigibles, lo que es significativo para las mipymes.

En el caso chileno, se encontraron la Ley 19.628, la Ley 21.719, la Política Nacional de Inteligencia Artificial y un documento del Banco Interamericano de Desarrollo (BID) que contribuyó a la formulación de dicha política. En este último documento, de Martínez y Vega (2020) para el BID, los autores plantearon integrar gobernanza de datos, transparencia, participación ciudadana, calidad de información, prevención de sesgos y formación de capacidades técnicas, lo cual demuestra que el modelo de Chile combina la participación con el fortalecimiento progresivo de la protección de datos. Entonces, las recomendaciones formuladas en espacios participativos no se fortalecen por sí misma, sino que buscan orientar decisiones públicas y mostrar las condiciones institucionales que requiere una implementación adecuada.

El contraste entre estos cuatro países dio como resultado la identificación de cinco elementos comunes, a saber: protección de datos, gestión del riesgo, supervisión humana, transparencia y atribución de responsabilidad; aunque cabe aclarar que no son equivalentes, pues en ciertos casos se evidenciaron como obligaciones jurídicas y en otros como objetivos de política, criterios técnicos o recomendaciones institucionales. Mientras que una norma establece deberes y consecuencias, una estrategia contiene orientaciones que dependen de decisiones posteriores, por lo que el uso indiscriminado de regulación, política, gobernanza o lineamiento puede dar la apariencia de una homogeneidad que no se identificó en los documentos.

En segundo lugar, se identificó una brecha entre el diseño de los marcos y las capacidades de las mipymes, puesto que son notorias las limitaciones de infraestructura, falta de capacitación, costos de implementación y problemas de integración tecnológica en empresas de Latinoamérica (Bravo et al. 2026), además de que la transformación digital necesita coordinar liderazgo, cultura, estructura y procesos organizacionales (del Do et al., 2023). Lo anterior demuestra que las disposiciones nacionales no garantizan que una empresa pequeña pueda usarlas como protocolo y conservar evidencia sobre cómo las aplican.

Para delimitar esa brecha, es posible relacionar la implementación de IA en pymes colombianas con mejoras en eficiencia, precisión y adaptabilidad, además preocupaciones sobre

dependencia tecnológica, transparencia y capacidad de supervisión (Socarrás, 2024); Chicaiza et al. (2025) advirtieron sobre las confusiones y la indeterminación de los sujetos obligados como riesgos cuando el software empresarial incluye decisiones automatizadas, sobre todo si hay poca supervisión humana. Por lo tanto, los beneficios operativos no suprimen los riesgos jurídicos, pero incrementan su complejidad cuando la organización no justifica el uso de resultados.

También se identificó, de forma transversal, la dificultad que supone la dependencia de proveedores externos, dado que muchas mipymes no tienen sistemas propios y deben contratar plataformas con funciones, localización de datos y actualizaciones controladas por terceros. Es de señalar que, aunque el proveedor controle el sistema, la empresa decide usarlo, de manera que la distribución de funciones no la exime de responsabilidad.

Del mismo modo, destaca la seguridad de la información, debido a que las mipymes del sector terciario son muy vulnerables, por lo que deben tomar medidas de ciberseguridad ajustadas a su realidad (Gordillo, 2024), teniendo en cuenta que la gobernanza de datos no se debe tratar solamente como un asunto de autorización jurídica sino que la organización debe examinar acceso, incidentes y prácticas del proveedor, dado que un error puede afectar la continuidad empresarial y los derechos de los titulares.

El tercer punto es la insuficiencia de la supervisión humana cuando se considera solo un requisito formal; la supervisión responsable requiere comprender los límites del sistema, acceder a la información y poder modificar, detener o rechazar la decisión. En ese panorama, Divino (2024) se refirió a la producción de resultados con sesgos o discriminatorios, la garantía de la privacidad y la dificultad para determinar quién asume responsabilidad; de tal modo, la presencia de una persona en el proceso no asegura un control efectivo si esta no tiene información suficiente, competencias o capacidad para cuestionar los resultados.

Los anteriores resultados permitieron identificar una brecha de trazabilidad organizacional, que consiste en la distancia entre la declaración empresarial de utilizar IA de forma responsable y la capacidad para indicar cómo fue escogido, autorizado, usado y supervisado el sistema. La brecha es notoria cuando no hay evidencia sobre el objetivo, el proveedor, la versión tecnológica, la información procesada, las instrucciones, la revisión humana o la decisión.

El proyecto ofreció una respuesta inicial a esta problemática, a través de inventarios de casos de uso, matrices de riesgo, registros de herramientas, responsables humanos, controles de datos y fichas de intervención. La distribución prevista otorgó roles diferenciados a decanaturas, equipos jurídicos, responsables de datos, líderes técnicos, consultorios universitarios y mipymes; asimismo, estableció evidencia mínima para cada fase, aunque es de resaltar que pertenecen a un modelo pendiente de validación. La revisión del estado de ejecución indica que el instrumento, la muestra, el trabajo de campo, el análisis estadístico y el piloto no se han completado, por lo que las metas se exponen como resultados. Por medio de este análisis, se pudo establecer que un modelo proporcional para mipymes debe centrarse en controles básicos y verificables, como determinar la finalidad, examinar la herramienta y el proveedor, clasificar riesgos, revisar el tratamiento de datos, tener un supervisor humano competente, guardar evidencia y gestionar incidentes. Ahora bien, tales controles deben incrementar su intensidad cuando el sistema intervenga en selección, evaluación económica, segmentación de personas y otras decisiones cruciales; mientras que un registro simple y una revisión humana documentada pueden ser suficientes en ámbitos más sencillos.

Para terminar, se puede afirmar que la proporcionalidad no causa reducción del cumplimiento, sino la distribución razonable de cargas de acuerdo con el riesgo y las capacidades empresariales, pues el tamaño de la organización no implica la protección que deben

brindar las personas sea menor, pero condiciona la complejidad de los procesos. Por esto, la comparación no permitió asegurar que alguna de las cuatro naciones estudiadas haya resuelto la aplicación de la gobernanza responsable en las mipymes; además, se identificaron principios y mecanismos relevantes, aunque hay una brecha latente entre su formulación y la capacidad para convertirlos en prácticas comprensibles, documentadas y controladas.

Discusión

En los cuatro países estudiados, los instrumentos muestran recurrentemente los términos transparencia, seguridad, protección de datos, supervisión humana y responsabilidad, pero se debe tener presente que su contenido y exigibilidad dependen de la naturaleza jurídica de cada fuente, lo que reafirma la necesidad de separar los consensos éticos de las obligaciones que requieren control institucional. Como señala Robles (2020), la multiplicación de iniciativas y declaraciones no resuelve los problemas jurídicos concernientes a la IA cuando no hay articulación, mecanismos de aplicación o pautas sobre responsabilidad; por tanto, la confluencia entre Colombia, Perú, Uruguay y Chile se halla en los principios, sin que se cree un sistema regional homogéneo de gobernanza de la IA. La limitación principal de estos marcos es la dificultad para que sus principios se usen en el funcionamiento cotidiano de organizaciones con recursos limitados, pues que las mipymes establezcan deberes no implica que haya un real conocimiento sobre identificar un sistema, documentar su propósito, evaluar al proveedor o guardar evidencia; reconocer estas carencias no justifica la falta de protección, porque el principio de proporcionalidad debe estar presente en la complejidad de los controles.

Considerar a la IA como una amenaza extraordinaria puede traer respuestas insólitas y la gestión institucional del riesgo conlleva medidas preventivas integradas en regulaciones ordinarias (Ulloa y Bas, 2025), lo que permite que las mipymes descarten la prohibición indiscriminada y la confianza en la autorregulación. Entonces, una visión gradual traslada el control más fuerte en aplicaciones que hacen uso de información sensible, crean perfiles o median las decisiones que influyen en los derechos, es por ello que la proporcionalidad requiere que no haya oposición entre innovación y regulación.

En este punto, la trazabilidad se considera un componente articulador y una prueba de cumplimiento, tomando en cuenta que la protección de datos, la supervisión humana y la responsabilidad no se articulan si la empresa no justifica la toma de decisión. Precisamente, en el estudio de Martínez (2019) se relaciona la responsabilidad asumida con la necesidad de acreditar medidas efectivas para tratar los datos, lo que requiere conservar evidencia, revisar y verificar el uso de resultados. La brecha de trazabilidad permite explicar por qué una empresa puede adoptar principios de IA responsable y, a su vez, no justificar su uso; esta brecha incluye registros existentes, separación de funciones, dependencia del proveedor y supervisión humana ineficiente; su utilidad analítica es relacionar el contenido de los marcos nacionales con las prácticas internas que apoyan su verificación. En relación con lo anterior, el modelo propuesto no pretende homogeneizar los ordenamientos, sino plantear un núcleo mínimo que permita identificar la finalidad, registrar herramientas y proveedores, clasificar riesgos, supervisar, guardar evidencia y gestionar incidentes; cada país puede agregar requerimientos con base en su normativa. En este proceso, los consultorios universitarios pueden apoyar diagnosticando usos, elaborando matrices de riesgo, revisando cláusulas contractuales y ofreciendo capacitaciones, sobre todo cuando las organizaciones no tienen equipos jurídicos o técnicos. Esta intervención es una propuesta sin ejecutar, por lo que su efectividad no se ha comprobado y debe ser evaluada a través del piloto y la evidencia que se obtenga.

Conviene destacar que la política editorial de la FIGRI evidencia la forma en que una organización puede delimitar usos, responsabilidades y deberes de declaración en un proceso (Universidad Externado de Colombia, 2025); por su parte, la Guía Empresarial de GOM Network (2025) privilegia aplicaciones y beneficios operativos de la IA, pero no le da importancia a la evidencia, las responsabilidades y la reclamación. Esto comprueba que una orientación práctica no es un sistema de gobernanza, ya que requiere principios de decisión, controles y evidencia verificable. A nivel jurídico, la incorporación institucional de la IA requiere normativas que articulen riesgos y garantías, sin que el sistema tome las decisiones; si bien se hace referencia a la jurisdicción contencioso-administrativa, esta idea afianza un elemento aplicable a las mipymes y es que la asistencia tecnológica apoya el análisis, pero no requiere justificar la decisión y asumir la responsabilidad de su utilización (Bermeo, 2023).

Finalmente, la gobernanza responsable no depende únicamente de ampliar la regulación ni que las mipymes implementen modelos de organizaciones más grandes, sino de vincular al ámbito jurídico los instrumentos con capacidades organizacionales, los controles y la evidencia. Asimismo, el análisis identifica la trazabilidad como núcleo de esa relación, pues a través de esta la organización puede justificar sus decisiones, corregir fallos y tomar la responsabilidad por el uso de la IA.

Conclusiones

En este análisis se pudo establecer que los marcos de gobernanza de la IA de Colombia, Perú, Uruguay y Chile comparten principios de protección de datos, transparencia, seguridad, gestión de riesgos, supervisión humana y responsabilidad, lo que no resulta en un sistema homogéneo, dadas las diferencias entre normas vinculantes, políticas públicas, lineamientos administrativos y recomendaciones institucionales. La capacidad de estos instrumentos para orientar el uso empresarial de la IA depende de su fortaleza en términos jurídicos y los mecanismos que permitan verificar sus acciones.

Los marcos estudiados tienen principios esenciales para una gobernanza responsable, pero también limitaciones para las mipymes en aspectos como infraestructura, capacitación, recursos y dependencia de proveedores, lo que merma su capacidad para identificar riesgos, controlar el tratamiento de datos, supervisar y conservar evidencia, lo que responde a la pregunta planteada.

Igualmente, se evidenció la brecha de trazabilidad organizacional, entendida como la distancia entre la declaración empresarial de usar IA de forma responsable y la posibilidad de reproducir cómo un sistema fue seleccionado, utilizado y supervisado. Ello relaciona el contenido de las regulaciones nacionales con las prácticas internas que se requieren para justificar decisiones, identificar errores y asumir responsabilidades, por lo cual la trazabilidad adquiere un carácter jurídico y probatorio.

Así, se propone un modelo proporcional basado en un núcleo mínimo que incluye determinar la finalidad, registrar herramientas y proveedores, clasificar riesgos, controlar datos, designar supervisores humanos, guardar evidencias y gestionar incidentes; es preciso recalcar que proporcionalidad significa ajustar la complejidad de los procesos. Como se había indicado, el alcance de estos hallazgos es documental y jurídico-comparado, pues el instrumento de diagnóstico, la vinculación de las mipymes, las respuestas recolectadas y el piloto de intervención deben ser ejecutados más adelante. Por esto, todavía no se puede asegurar la eficacia práctica del modelo planteado, la validación de este requerirá completar el trabajo de campo, verificar la calidad de los datos y contrastar las categorías construidas con las experiencias de las organizaciones vinculadas; dicha fase permitirá establecer si los controles

identificados son comprensibles, aplicables y suficientes para lograr que se reduzcan las brechas de gobernanza evidenciadas.

Referencias bibliográficas

- Bermeo, L. (2023). *Inteligencia artificial en la jurisdicción contenciosa administrativa* [Tesis doctoral, Pontificia Universidad Javeriana].
- Bravo, O., Cabanilla, G., y Cabanilla, M. (2026). Uso de inteligencia artificial (IA) en mipymes de América Latina. *European Public & Social Innovation Review*, 11, 1–18. <https://doi.org/10.31637/epsir-2026-2334>
- Castañeda, L. M. (2024). Gobernanza de la inteligencia artificial mediada por gobierno de TIC en la educación superior: Literatura científica y no convencional, 2020–2023. *TIES, Revista de Tecnología e Innovación en Educación Superior*, 10, 86–98. <https://doi.org/10.22201/dgtic.26832968e.2024.10.20>
- Chicaiza, G. D., Romero, J. V., y Salazar, C. E. (2025). Riesgos éticos en el uso de inteligencia artificial en decisiones automatizadas dentro del software empresarial. *Arandu UTIC*, 12(2), 2896–2907. <https://doi.org/10.69639/arandu.v12i2.1115>
- del Do, A. M., Villagra, A., y Pandolfi, D. (2023). Desafíos de la transformación digital en las PYMES. *Informes Científicos Técnicos–UNPA*, 15(1), 200–229. <https://doi.org/10.22305/ict-unpa.v15.n1.941>
- Delgado, J. J., y Espinoza, J. A. (2024). Impacto de la inteligencia artificial en derecho a la intimidad y protección de datos personales. *Ciencia Latina Revista Científica Multidisciplinar*, 8(5), 11136–11147. https://doi.org/10.37811/cl_rcm.v8i5.14497
- Díaz, J. P. (2024). Panorámica internacional de la regulación de la inteligencia artificial: Reglamento Europeo de Inteligencia Artificial (AI Act). *Revista CESCO de Derecho de Consumo*, 49, 117–130. https://doi.org/10.18239/RCDC_2024.49.3473
- Divino, S. (2024). Governance and compliance recommendations for artificial intelligence in business management. *Nuevo Derecho*, 20(35), 1–17. <https://doi.org/10.25057/2500672X.1665>
- Espinosa de los Monteros, S., y Sanz, G. (2024). El Reglamento de IA: El primer paso del camino hacia una regulación completa de la inteligencia artificial. *Actualidad Jurídica Uría Menéndez*, 65, 180–196.
- GOM Network. (2025). *Guía de inteligencia artificial para PYMEs en Colombia 2025*.
- Gordillo, A. (2024). Estrategias de ciberseguridad para MiPymes del sector terciario. *European Public & Social Innovation Review*, 9, 1–19. <https://doi.org/10.31637/epsir-2024-293>
- Grijalva, J. R. (2024). Trazando el camino hacia una regulación efectiva: Breve análisis del Reglamento Europeo de Inteligencia Artificial de 2024. *Revista Internacional y Comparada de Derechos Humanos*, 7(1), 123–160.
- Gutiérrez, J. D., Muñoz-Cadena, S., Castellanos-Sánchez, M., y Hurtado, S. (2025). *Informe de los Repositorios 1.0*. Proyecto Sistemas de Algoritmos Públicos, Escuela de Gobierno Alberto Lleras Camargo, Universidad de los Andes.
- Hernández, O., Parra, C. G., y de la Rosa, C. C. (2026). La inteligencia artificial en las PYMES: Una revisión de literatura para América Latina. *Ciencia y Reflexión*, 5(1), 1080–1098. <https://doi.org/10.70747/cr.v5i1.713>
- López, G. A., y Quintero, L. M. (2025). Delitos contra la intimidad personal en el marco de la inteligencia artificial en Colombia. *Postulados Revista Sociojurídica*, 2(2), 57–71. <https://doi.org/10.22463/29816866.4300>

- Martínez, A. (2019). La inteligencia artificial, el big data y la era digital: ¿Una amenaza para los datos personales? *Revista La Propiedad Inmaterial*, 27, 5–23. <https://doi.org/10.18601/16571959.n27.01>
- Martínez, Y., y Vega, M. (2020). *Gobernanza participativa de la inteligencia artificial*. Banco Interamericano de Desarrollo.
- Otero, J. D., Martín, F. J., y Velasco, P. (2026). *Inteligencia artificial: Impacto económico, competencia y regulación* (Documento de Trabajo 2026/03). Fundación de Estudios de Economía Aplicada.
- Quirós, J. (2025). *Regulación de la inteligencia artificial en la Unión Europea* [Trabajo fin de grado, Universidad de Oviedo].
- Robles, M. (2020). La gobernanza de la inteligencia artificial: Contexto y parámetros generales. *Revista Electrónica de Estudios Internacionales*, 39, 1–42.
- Romero, J., Arias, V. M., León, D. M., del Ángel, H., Valdez, M. L., y Hernández, C. (2024). Modelo de inteligencia de negocios para PYMES: Una propuesta de desarrollo. *Innovación y Desarrollo Tecnológico Revista Digital*, 16(2), 899–912.
- Sánchez, M. F. (2024). Inteligencia artificial generativa y los retos en la protección de los datos personales. *Estudios en Derecho a la Información*, 9(18), 179–205. <https://doi.org/10.22201/ijj.25940082e.2024.18.18852>
- Socarrás, L. (2024). Inteligencia artificial para la toma de decisiones en PYMES colombianas: Innovación estratégica y desarrollo regional. *Telématiche*, 23(2), 82–103.
- Ulloa, M. A., y Bas, G. (2025). La securitización de la inteligencia artificial: Un análisis de sus impulsores y sus consecuencias. *Revista de Estudios Sociales*, 93, 67–84. <https://doi.org/10.7440/res93.2025.04>
- Universidad Externado de Colombia, Facultad de Finanzas, Gobierno y Relaciones Internacionales. (2025). *Política sobre el uso de inteligencia artificial en los procesos editoriales de la Facultad de Finanzas, Gobierno y Relaciones Internacionales–FIGRI* (Versión 1.0).
- Yaranga, I. P., y Olórtiga, L. W. (2025). Inteligencia artificial para aumentar la productividad en las empresas: Un estudio bibliométrico. *Revista InveCom*, 5(4), 1–11. <https://doi.org/10.5281/zenodo.14846656>