RED IBEROAMERICANA DE PROTECCION DE DATOS

Red Iberoamericana
Rede Ibero-Americana

Órganos reguladores y auditoría algorítmica en el espacio iberoamericano

Guía para Autoridades de Control · Recomendaciones para Legisladores · Independencia efectiva · Capacidad técnica · Auditoría algorítmica · Fortalecimiento institucional

*Autor: Luis García Balcarce**

Elaborado en el marco de la Convocatoria "Trabajar en Red" 2025-2026

Septiembre 2026.

Publicado con el apoyo de la Agencia Española de Cooperación Internacional para el Desarrollo AECID

"Las opiniones, análisis y conclusiones expresados en este documento pertenecen exclusivamente a su autor en calidad de experto independiente y no reflejan necesariamente la postura o criterio de la Red Iberoamericana de Protección de Datos (RIPD). Esta publicación no implica la aprobación de su contenido ni representa la posición institucional de la RIPD, la cual no se hace responsable del uso que pueda darse a la información aquí expuesta."

Cómo usar este documento

Este documento tiene dos audiencias primarias y una estructura pensada para que cada una encuentre lo que necesita sin tener que recorrer el texto completo.

Para autoridades de control de Protección de Datos Personales	Para legisladores y Ejecutivo
Sección 3 - Supervisar tratamientos de datos personales en sistemas de IA con poderes de PDP vigentes **Sección 5 - Herramienta de autoevaluación (30 indicadores)** **Sección 6 - Auditoría algorítmica: tipos, poderes, metodologías** **Sección 7 - Buenas prácticas entre pares** **Sección 8 - Hoja de ruta operativa por etapas** **Sección 9 - Recomendaciones (acciones sin reforma legislativa)**	**Sección 2 - Diagnóstico regional** **Sección 4 - Modelos institucionales comparados** **Sección 5 - Indicadores para evaluar diseños normativos** **Sección 9 - Recomendaciones (requieren reforma legislativa)**

A lo largo del documento, las recomendaciones están etiquetadas con dos marcas visuales: **Autoridad - acción inmediata** para lo que una autoridad puede implementar dentro de su mandato existente, y **Legislador - reforma requerida** para lo que requiere intervención del poder legislativo o ejecutivo.

Sumario ejecutivo

Una mayor efectividad de cualquier marco regulatorio de privacidad sobre inteligencia artificial depende de dos condiciones institucionales inseparables. Primero, la autonomía e independencia efectiva de la autoridad que lo aplica, y segundo, su capacidad técnica para supervisar sistemas cuya complejidad supera los instrumentos tradicionales de control administrativo. Este documento aborda ambas condiciones de manera integrada, ofreciendo tanto un análisis normativo de diseño institucional como una guía operativa para las autoridades que ya existen y necesitan fortalecer su función supervisora.

El documento está dirigido de manera simultánea a dos audiencias. Las autoridades de control de datos personales encontrarán un diagnóstico comparado, una herramienta de autoevaluación con 30 indicadores, una guía operativa para supervisar los tratamientos de datos personales efectuados mediante sistemas de IA, dentro de sus mandatos existentes, y una hoja de ruta de fortalecimiento por etapas. Los legisladores y poderes ejecutivos encontrarán un análisis de modelos institucionales, lecciones del derecho comparado y recomendaciones para el diseño o reforma de sus marcos normativos.

A partir del análisis de diez jurisdicciones iberoamericanas se llega a cuatro conclusiones. La primera es que la supervisión de los tratamientos de datos personales efectuados mediante sistemas de IA no requiere un nuevo organismo. Las autoridades de protección de datos personales pueden ejercerla con sus competencias existentes, dentro del ámbito material que les atribuye su legislación nacional, y con las herramientas metodológicas adecuadas. Esa competencia no equivale, por sí sola, a un mandato general de supervisión de los sistemas de IA. En segundo lugar, la independencia institucional tiene cuatro dimensiones -orgánica, funcional, presupuestaria e interpretativa- y cuantas más dimensiones se cumplan, mayor es la eficacia del sistema. Tercero, la brecha más crítica en las autoridades analizadas no es normativa sino técnica. La capacidad de auditar sistemas de IA sofisticados requiere perfiles que la mayoría de las autoridades no tienen. Cuarto, la cooperación regional es el multiplicador de capacidad más eficiente para las autoridades.

1. Introducción

La masividad de la inteligencia artificial plantea a las autoridades de protección de datos personales un doble desafío. El primer desafío es técnico, ya que los sistemas de IA son cajas negras que producen resultados no directamente observables, que evolucionan en el tiempo y que requieren herramientas de análisis muy distintas de las usadas en la supervisión tradicional de bases de datos. El segundo desafío es institucional, dado que muchas de las autoridades analizadas que deberían supervisar estos sistemas no tienen los recursos, los poderes de acceso ni la capacidad técnica para hacerlo de manera efectiva.

En las jurisdicciones analizadas, en muchos casos, el primer desafío no requiere esperar al legislador. Sus marcos de protección de datos personales vigentes -la LGPD brasileña-, la Ley 18.331 uruguaya, la Ley Orgánica de Protección de Datos Personales (LOPDP) ecuatoriana y la propia Ley 25.326 argentina- contienen herramientas que ya permiten supervisar los tratamientos de datos personales efectuados mediante sistemas de IA, dentro del ámbito material y de las competencias que cada legislación nacional atribuye a su autoridad. A modo enunciativo, el principio de finalidad impide los usos de IA incompatibles con la finalidad para la que se recolectaron los datos, en los términos de cada legislación, el principio de minimización restringe los datos de entrenamiento, el derecho a no ser objeto de decisiones exclusivamente automatizadas es directamente aplicable en las jurisdicciones que lo reconocen, y la evaluación de impacto en la privacidad puede extenderse a una evaluación de impacto algorítmico, allí donde la normativa no la prevé ya de manera expresa. Dentro de ese ámbito, lo que falta en la mayoría de los casos analizados no es el poder legal sino la metodología y la capacidad técnica para ejercerlo. Fuera de él, la supervisión de sistemas de IA requiere un mandato legal expreso.

Este documento parte de esa constatación para ofrecer una guía operativa para las autoridades que ya existen. Por otro lado, el análisis de modelos institucionales y las recomendaciones para legisladores son el complemento necesario para los casos en que los poderes de las autoridades de protección de datos resultan insuficientes, y para que las propias autoridades puedan identificar con precisión qué necesitan del legislador y por qué.

2. Diagnóstico regional: mapa de autoridades de supervisión

El siguiente cuadro sintetiza el estado de las autoridades de supervisión en diez jurisdicciones iberoamericanas: Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, México, Perú y Uruguay. Estas jurisdicciones constituyen una muestra del espacio iberoamericano. Las conclusiones y las referencias a la región que se formulan en este documento se circunscriben a las jurisdicciones analizadas. Es el caso de Andorra, cuya Ley 29/2021, de protección de datos personales, regula, entre otras cuestiones, las decisiones individuales automatizadas, las evaluaciones de impacto, las vulneraciones de seguridad y las funciones y garantías de independencia de la autoridad de control.

País	Autoridad	Modelo	Evaluación y observaciones
Argentina	AAIP	PDP (sin mandato legal específico de IA)	Adecuación UE. Autonomía funcional. Programa de Transparencia en IA activo (tres pilares: Observatorio, Gobernanza, Fortalecimiento). Guía sept. 2024.

País	Autoridad	Modelo	Evaluación y observaciones
			Resolución 2/2023 sobre IA fiable. Proyecto Stargate Argentina (OpenAI/Sur Energy, USD 25.000M anunciado en 2025) exige fortalecimiento. Reforma Ley 25.326 pendiente.
Brasil	ANPD	Autarquía especial; agencia reguladora desde la Ley Nº 15.352/2026	Adecuación UE. Autonomía funcional, técnica, decisoria, administrativa y financiera. Capacidad sancionatoria activa. Sandbox Regulatorio de Inteligencia Artificial y Protección de Datos. Radares Tecnológicos sobre IA generativa y sobre deepfakes. Guía sobre el Uso Ético de la IA, en elaboración, vinculada al PBIA (Plan Brasileño de Inteligencia Artificial). Guía sobre IA generativa del MGI. Nota Técnica Nº 12/2025/CON1/CGN/ANPD, consulta para recabar aportes sobre decisiones automatizadas.
Chile	Agencia PDP (a crear)	Convergente - vigencia dic. 2026, con proyecto de postergación en trámite	Agencia autónoma creada por la Ley 21.719. Pendiente de implementación. Deberá supervisar los tratamientos de datos personales efectuados mediante sistemas de IA. Desafío: construir capacidad técnica desde cero. Proyecto Boletín 15869-19 en tramitación para IA específica. El Boletín 18623-07, presentado el 1 de septiembre de 2026, propone postergar la entrada en vigencia de la Ley 21.719 hasta diciembre de 2027 y dispone que la primera designación de los consejeros del Consejo Directivo de la Agencia se efectúe, a más tardar, doce meses antes de esa entrada en vigencia[1].
Colombia	SIC	Sectorial multifunción	Activa en IA: Circular 002 de ago. 2024 sobre IA y datos. Tensión entre funciones heterogéneas. Marco Ético IA 2021 como referencia soft law.
Costa Rica	Prodhab	PDP independiente	Dos proyectos de ley proponen ARIA como nueva autoridad de IA (PL 23.771 y PL 23.919). Debate entre crear nuevo organismo o fortalecer Prodhab.
Ecuador	Superintendencia de Protección de Datos Personales (SPDP)	PDP con regulación sectorial de IA	Creada por la LOPDP (2021). Resolución Nº SPDP-SPD-2026-0009-R, Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial, reformada por la Resolución Nº SPDP-SPD-2026-0037-R, que precisa el alcance de las obligaciones de responsables y encargados. La norma contempla auditorías de los sistemas de IA conforme a la LOPDP, el RGLOPDP y la normativa secundaria. Sandbox regulatorio impulsado por el MINTEL, con fundamento en el artículo 8 de la

[1] https://tramitacion.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=18623-07

País	Autoridad	Modelo	Evaluación y observaciones
			Ley Orgánica para la Transformación Digital y Audiovisual, distinto de las competencias de supervisión y control de la SPDP[2]. Evaluación AIRA-PNUD 2024[3].
El Salvador	ANIA (fomento de IA) y ACE - Agencia de Ciberseguridad del Estado (protección de datos)	Ley específica de IA; supervisión del tratamiento de datos personales en la autoridad de datos	Ley de Fomento a la Inteligencia Artificial: la ANIA es rectora del fomento de la IA. Los arts. 22 y 28 reconocen la supervisión de la ACE respecto del tratamiento de datos personales mediante modelos de IA. El art. 17 encomienda a la ANIA un Marco Integral de Evaluación de Riesgos, cuyos requisitos son obligatorios para los sistemas que traten datos confidenciales, reservados o personales. El art. 18 exige, cuando la IA se use con fines comerciales o para acceder a derechos o servicios, informar si la decisión fue adoptada o impulsada por un sistema de IA, dar una explicación comprensible y transparente del proceso y habilitar su impugnación ante una persona natural competente para confirmarla, modificarla o revocarla.
México	Secretaría Anticorrupción y Buen Gobierno (SABG) - Unidad de Protección de Datos Personales	PDP en el Ejecutivo, con autonomía técnica y operativa	Extinción del INAI por la reforma constitucional 'Simplificación Orgánica' (DOF 20/12/2024). Leyes previas abrogadas y sustituidas por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley Federal de Protección de Datos Personales en Posesión de Particulares. En el sector privado la supervisión corresponde a la SABG a través de la Unidad de Protección de Datos Personales. No existe autoridad específica de supervisión de IA: la gobernanza es interinstitucional, con participación de la Agencia de Transformación Digital y Telecomunicaciones y de la SECIHTI. Actualización en curso de la LFPDPPP, con disposiciones sobre tecnologías emergentes e IA en supuestos que involucren tratamiento de datos personales. Iniciativas: Consejo Nacional de IA, PNAA, RENSIA.
Perú	SGTD (PCM)	Técnico-normativa - Ejecutivo	Designada por Ley 31814 como autoridad de IA. Reglamento DS 115-2025-PCM. Centro Nacional de Innovación Digital e IA[4].

[2] https://www.telecomunicaciones.gob.ec/gobierno-de-daniel-noboa-impulsa-un-sandbox-regulatorio-para-el-desarrollo-responsable-de-la-inteligencia-artificial-en-el-ecuador/
[3] https://www.undp.org/es/ecuador/comunicados-de-prensa/el-ecuador-se-enrumba-aprovechar-la-inteligencia-artificial-bajo-un-enfoque-de-inclusion
[4] https://www.gob.pe/institucion/pcm/noticias/482491-gobierno-implementara-el-centro-nacional-de-innovacion-digital-e-inteligencia-artificial

País	Autoridad	Modelo	Evaluación y observaciones
Uruguay	URCDP	PDP autónoma consolidada	Adecuación UE. Resoluciones sobre transferencias, DPO, brechas. Estrategia Nacional de Inteligencia Artificial del Uruguay 2024 - 2030[5]. Firma del tratado sobre inteligencia artificial del Consejo de Europa[6]

El diagnóstico permite distinguir dos grupos entre las autoridades analizadas. Las del primer grupo (Brasil y Uruguay) operan con independencia y capacidad técnica consolidadas y pueden asumir de manera inmediata la supervisión de los tratamientos de datos personales efectuados mediante sistemas de IA, con ajustes metodológicos. Las del segundo grupo (Argentina, Colombia, Costa Rica y Ecuador) tienen marcos funcionales con brechas específicas identificables, abordables con fortalecimiento interno y cooperación regional. La clasificación se apoya en el grado de consolidación normativa e institucional relevado en el cuadro anterior, no en una evaluación del desempeño de cada autoridad.

3. Supervisar tratamientos de datos personales en sistemas de IA con poderes de PDP vigentes. Guía operativa para autoridades

Esta sección está dirigida a las autoridades en protección de datos, y parte de la premisa de que justamente los marcos de protección de datos personales vigentes en las jurisdicciones analizadas ya contienen herramientas para supervisar los tratamientos de datos personales efectuados mediante sistemas de IA. A continuación se identifican algunas precisiones sobre qué puede hacerse hoy -y qué no-, como punto de partida para una estrategia de fortalecimiento institucional.

Esta supervisión se ejerce dentro del ámbito material y de las competencias que la legislación nacional atribuye a cada autoridad. La existencia de competencias en materia de protección de datos no equivale, por sí sola, a un mandato general de supervisión de los sistemas de IA. La distinción preserva el principio de competencia. Ninguna de las herramientas o recomendaciones de este documento habilita a extender por vía interpretativa el mandato legal de las autoridades.

3.1. Lo que los poderes de PDP ya habilitan

El siguiente cuadro detalla cómo los principios y derechos reconocidos en los marcos de protección de datos de las jurisdicciones analizadas se aplican sobre el ciclo de vida de los sistemas de IA, en la medida

[5] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-nacional-inteligencia-artificial-del-uruguay-2024-2030

[6] https://www.coe.int/es/web/portal/-/uruguay-signs-council-of-europe-s-global-ai-treaty

en que ese ciclo involucre tratamiento de datos personales, e identifica las habilitaciones más relevantes:

Herramienta de PDP	Proyección sobre sistemas de IA	Acciones disponibles para la autoridad
Principio de finalidad	Los datos de entrenamiento no pueden tratarse para fines incompatibles con la finalidad de su recolección. La reutilización de datasets para entrenar modelos con fines distintos a los originales está prohibida cuando resulta incompatible con la finalidad inicial, en los términos de cada legislación.	Investigar de oficio si el uso de datos para entrenar sistemas de IA es compatible con la finalidad de su recolección.
Principio de minimización	El modelo debe entrenarse solo con los datos estrictamente necesarios. Se prohíbe el uso de datos sensibles que no sean necesarios o que carezcan de una base de legitimación prevista para esta categoría en la legislación aplicable.	Auditar si el diseño del sistema incorpora más datos de los necesarios. Exigir justificación de cada categoría de dato utilizado en entrenamiento.
Derecho a no ser objeto de decisiones automatizadas	Reconocido en algunas legislaciones y proyectos de ley. Donde se reconoce, exige supervisión humana significativa en decisiones con efectos jurídicos, con el alcance y las excepciones que establece cada legislación. Requiere supervisión humana significativa en decisiones con efectos jurídicos.	Investigar sistemas que adoptan decisiones vinculantes sin intervención humana. Exigir descripción del mecanismo de supervisión humana y su efectividad real.
Evaluación de impacto en privacidad (DPIA)	Algunas normas ya prevén de manera expresa la evaluación de impacto de los sistemas de IA. Donde no lo hacen, la DPIA puede extenderse metodológicamente para cubrir impactos algorítmicos: sesgo, discriminación, transparencia.	Requerir la DPIA en los casos en que la ley la prevé. Desarrollar guías que orienten la extensión de la metodología de DPIA a impactos algorítmicos.
Derecho de acceso e información	En los términos de cada legislación, el derecho de acceso permite al titular conocer si sus datos fueron tratados para entrenar un modelo. Incluye información sobre las decisiones automatizadas adoptadas sobre él solo donde la legislación lo prevé.	Supervisar que los responsables informan adecuadamente sobre el uso de IA. En las jurisdicciones que reconocen ese derecho, investigar reclamos de titulares que no reciben explicación de decisiones automatizadas.
Responsabilidad proactiva (accountability)	El responsable debe poder demostrar en todo momento el cumplimiento. Incluye documentar el diseño del sistema de IA y sus medidas de mitigación de riesgos.	Requerir la documentación del sistema de IA necesaria para verificar el tratamiento de datos personales (propósito, datos, arquitectura, métricas de rendimiento). Verificar que la política de privacidad cubre el tratamiento algorítmico.

Herramienta de PDP	Proyección sobre sistemas de IA	Acciones disponibles para la autoridad
Datos sensibles	Esta categoría de datos tiene protección reforzada. Su uso para entrenamiento de IA requiere una base legal prevista para esta categoría en la legislación aplicable.	Investigar sistemas que infieren atributos sensibles (etnia, salud, orientación sexual) a partir de datos no sensibles. Determinar la infracción cuando se usan proxies para eludir la protección reforzada.
Notificación de brechas	Donde la ley prevé la obligación de notificar brechas de seguridad, esa obligación alcanza a los ataques adversariales, las alteraciones de modelos y los incidentes que afecten su integridad solo cuando constituyan o den lugar a una vulneración de la seguridad de datos personales, como la filtración de datos personales usados en el entrenamiento.	Supervisar los protocolos de seguridad de sistemas de IA que traten datos personales. Requerir la notificación de los incidentes que constituyan o den lugar a una vulneración de la seguridad de datos personales.

3.2. Herramientas operativas por área de supervisión

Más allá del mapeo principal, estas son algunas de las herramientas operativas que podrían implementar hoy las autoridades de PDP sin necesidad de una reforma legislativa:

3.2.1. Guías y recomendaciones sectoriales

Las guías técnicas sectoriales son el instrumento de menor costo y mayor alcance disponible para las autoridades, por ejemplo la Guía para el Uso Responsable de IA de la AAIP y la Circular 002/2024 de la SIC colombiana. Una guía sectorial bien diseñada puede: (i) desarrollar criterios interpretativos de la normativa de protección de datos aplicable a sistemas de IA antes de que exista ley específica de IA; (ii) generar una doctrina administrativa que oriente a los operadores; y (iii) orientar el cumplimiento y dar previsibilidad a las investigaciones. Una guía no constituye por sí misma el fundamento jurídico de obligaciones sancionables. Las obligaciones cuya infracción acarrea sanciones deben tener fundamento suficiente en el ordenamiento jurídico aplicable.

Algunas de las áreas prioritarias para las guías sectoriales son: sistemas de IA en selección laboral, sistemas de scoring crediticio, sistemas de reconocimiento facial, IA en diagnóstico médico, y sistemas de IA en educación. Además, a nivel regional se puede coordinar el desarrollo de guías modelo que luego cada autoridad adapte a su contexto.

3.2.2. Investigaciones de oficio basadas en datos

En general, las autoridades de PDP de las jurisdicciones analizadas tienen poder de investigación de oficio. Este poder puede aplicarse a los tratamientos de datos personales efectuados mediante sistemas de IA, a través del análisis de patrones de reclamos ciudadanos que sugieran discriminación algorítmica sistemática, la supervisión de los avisos de privacidad de servicios digitales masivos que usan IA, y la revisión de los registros de tratamiento de responsables que operan sistemas de IA de impacto

significativo. La ANPD brasileña ha documentado metodologías de investigación de oficio basadas en análisis estadístico de reclamos que pueden adoptarse por referencia[7]. La misma autoridad abrió, mediante la Nota Técnica Nº 12/2025/CON1/CGN/ANPD[8], una consulta para recabar aportes sobre decisiones automatizadas. La consulta previa tiene dos beneficios, por un lado releva el estado real del uso de estos sistemas antes de fijar criterios, y por el otro evidencia la posición de la autoridad a la discusión pública, lo que refuerza la previsibilidad de las investigaciones que se inicien después.

3.2.3. Evaluación de impacto algorítmico: extensión de la DPIA y obligaciones ya vigentes

Algunas normas de las jurisdicciones analizadas ya prevén expresamente la evaluación de impacto y las auditorías respecto de los sistemas de IA que tratan datos personales. Es el caso de la Resolución Nº SPDP-SPD-2026-0009-R de Ecuador, que establece la implementación de gestión de riesgos, la evaluación de impacto cuando proceda y auditorías de los sistemas de IA. Donde no existe una disposición de ese tipo, las evaluaciones de impacto en la privacidad previstas en los marcos de protección de datos más modernos pueden extenderse metodológicamente para cubrir impactos algorítmicos. La autoridad puede emitir una guía que oriente a las organizaciones que operen sistemas de IA de alto riesgo sobre el contenido de su DPIA: análisis de representatividad del dataset, métricas de equidad algorítmica por grupos demográficos, descripción del mecanismo de supervisión humana y protocolo de monitoreo post-despliegue. Esta extensión se apoya en el principio de responsabilidad proactiva. Para que la omisión de estos contenidos sea sancionable, la obligación debe tener fundamento en la ley o en una norma dictada con habilitación legal.

3.2.4. Registro voluntario de sistemas de IA

Sin necesidad de legislación específica, las autoridades pueden promover el registro voluntario de sistemas de IA de alto riesgo que traten datos personales en su jurisdicción. Este registro genera visibilidad sobre el ecosistema de IA existente, facilita la priorización de las investigaciones, permite desarrollar estadísticas sectoriales, y puede ser un elemento a considerar para reducir sanciones en caso de que las haya. El Registro Nacional de Sistemas de IA (RENSIA) propuesto en México[9] es un ejemplo de este tipo de implementaciones. Una vía complementaria es trasladar la publicidad a los propios organismos: en Chile, el Consejo para la Transparencia recomendó, mediante la Resolución Exenta Nº 372 de 2024, que los sujetos obligados mantengan a disposición permanente del público, por sus canales de transparencia activa y con actualización al menos mensual, los antecedentes de los sistemas de decisión automatizada o semiautomatizada que tengan efectos en los derechos fundamentales o en el

[7] https://iapp.org/news/a/ia-generativa-y-protecci-n-de-datos-en-brasil-posicionamiento-de-la-anpd-en-la-nota-t-cnica-n-1-2026

[8] https://www.gov.br/anpd/pt-br/acesso-a-informacao/participacao-social/outras-acoes/documentos/ts-06-2024-nt-12-2025-consolidacao-das-contribuicoes.pdf

[9] https://sil.gobernacion.gob.mx/Archivos/Documentos/2025/04/asun_4896460_20250430_1747757009.pdf

acceso a servicios, programas sociales, subsidios, fondos y otros beneficios que el organismo entregue o preste[10].

3.2.5. Programas de formación y certificación

Las autoridades pueden desarrollar programas de formación en protección de datos e IA dirigidos a organizaciones, con énfasis en los sectores de mayor riesgo. La certificación de cumplimiento mediante programas de reconocimiento voluntario -similar a los sellos de privacidad que algunas autoridades ya otorgan- puede constituir un incentivo efectivo para la adopción de buenas prácticas sin coerción normativa.

3.3. Lo que los poderes de PDP no alcanzan

A partir de las capacidades del apartado anterior, se identificaron también los límites de las agencias en protección de datos. Hay al menos cinco áreas donde los poderes de PDP existentes de las jurisdicciones analizadas resultarían insuficientes para una supervisión completa de los sistemas de IA:

- Acceso técnico a sistemas: los poderes de inspección de PDP suelen estar diseñados para revisar bases de datos y registros de tratamiento, no para acceder a la arquitectura de un modelo de Machine Learning, sus logs de inferencia desagregados o sus parámetros de ajuste. Este poder debe ser conferido expresamente.

- Auditoría de algoritmos que no tratan datos personales: un sistema de IA puede tomar decisiones que afectan a personas sin tratar sus datos personales de manera directa (p. ej., sistemas de asignación de recursos públicos basados en datos agregados). El marco de PDP no cubre estos casos.

- Poderes cautelares sobre sistemas: la mayoría de los marcos de PDP no prevé la suspensión preventiva de un sistema de IA como medida cautelar antes de concluir una investigación, para que así sea se debe habilitar expresamente.

- Sanciones proporcionales al impacto de la IA: en general, los techos sancionatorios previstos en las leyes de PDP analizadas resultan insuficientes como disuasores para grandes operadores tecnológicos. El estándar del AI Act europeo (hasta el 7% del volumen de negocio global), por ejemplo, requiere reforma legislativa para ser adoptado.

[10] https://www.bcn.cl/leychile/navegar?idNorma=1206232

- Regulación de modelos de propósito general (LLMs): los modelos de lenguaje de gran escala presentan riesgos sistémicos que trascienden el tratamiento de datos personales y requieren obligaciones específicas que no pueden inferirse del marco de PDP.

En conclusión, las autoridades de control no necesitan esperar al legislador para supervisar los tratamientos de datos personales efectuados mediante sistemas de IA. Pueden actuar hoy con sus poderes de protección de datos vigentes, fortaleciéndose con metodologías, guías sectoriales y cooperación regional. Las cinco áreas descritas en este apartado exceden ese ámbito y requieren habilitación legal expresa.

4. Modelos institucionales comparados

Para los poderes legislativos y ejecutivos que diseñan o reforman marcos institucionales de supervisión de IA, el siguiente análisis comparado ofrece los cuatro modelos principales disponibles y sus ventajas y limitaciones relativas.

Atributo	Convergente PDP+IA	Agencia IA dedicada	Red sectorial coordinada	Comité interministerial
Independencia	Alta, si el mandato es claro	Alta, si se garantiza por ley	Media, depende de coordinación	Baja: subordinación ejecutiva
Capacidad técnica	Concentrada; riesgo de sobrecarga	Especializada en IA; coordinación con PDP compleja	Distribuida; heterogénea	Dispersa; difícil de acumular
Costo de creación	Bajo (adaptar existente)	Alto (nueva institución)	Medio (coordinación)	Muy bajo (sin nueva estructura)
Coherencia normativa	Alta: una sola interpretación	Alta en IA; posibles conflictos con PDP	Media: riesgo de fragmentación	Baja: múltiples criterios
Recomendado para	Países con autoridad PDP sólida y mandato ampliable	Grandes mercados digitales con recursos suficientes	Países con reguladores sectoriales maduros	Solo como solución transitoria
Riesgo principal	Sobrecarga sin recursos adicionales	Duplicación con autoridad PDP existente	Arbitraje regulatorio intersectorial	Captura ejecutiva; falta de enforcement

Para la mayoría de los países analizados, el Modelo A -convergente PDP+IA- sería el más adecuado en la fase actual. Sus condiciones de éxito son que la autoridad de PDP preexistente tenga un grado razonable de independencia, que su mandato sea ampliado explícitamente para incluir supervisión de IA, y que reciba recursos técnicos y presupuestarios proporcionales al nuevo mandato.

4.1. Modelo A: Convergente PDP+IA

Una autoridad de PDP bien diseñada puede asumir la supervisión de IA sin crear una nueva institución, siempre que la ley amplíe expresamente su mandato, con el doble beneficio de la coherencia normativa -IA y datos personales son inseparables- y el aprovechamiento del expertise institucional acumulado. La condición crítica es el refuerzo proporcional de recursos: incorporar el mandato de IA sin aumentar presupuesto, personal técnico y poderes de acceso es la principal causa de fracaso de este modelo.

4.2. Modelo B: Agencia de IA independiente

Este modelo es adecuado para jurisdicciones con grandes mercados digitales y capacidad presupuestaria suficiente. Su desventaja es el costo de creación desde cero y el riesgo de duplicación con la autoridad de PDP preexistente. Para la mayoría de los países analizados, en la fase actual, este modelo parecería prematuro.

4.3. Modelo C: Red de reguladores sectoriales

En este modelo la supervisión de IA se distribuye entre reguladores ya existentes según el sector donde el sistema opera: la autoridad bancaria supervisa los algoritmos de scoring crediticio, la autoridad sanitaria supervisa los sistemas de diagnóstico médico, la autoridad laboral supervisa las herramientas de selección de personal, y así sucesivamente. Una entidad coordinadora, que puede ser una agencia específica de IA o simplemente una secretaría técnica interministerial, se encarga de fijar lineamientos transversales y dirimir conflictos de competencia.

Su principal desafío es la coherencia normativa. Sin una autoridad central con capacidad de fijar criterios interpretativos vinculantes de alcance general, el riesgo de vacíos regulatorios es elevado, ya que un operador puede diseñar su sistema de forma que quede en la frontera entre dos jurisdicciones sectoriales y así eludir la supervisión efectiva de ambas.

4.4. Modelo D: Comité interministerial

La supervisión de IA recae en una estructura interna al Ejecutivo, típicamente una comisión, secretaría técnica o consejo formado por representantes de distintos ministerios -de tecnología, de justicia, de economía- que elabora políticas, emite lineamientos y coordina la aplicación de normas entre las distintas ramas del gobierno. No tiene personería propia ni presupuesto independiente; funciona con los recursos y el personal de los ministerios que lo integran.

Su principal ventaja es el bajo costo de creación al no requerir legislación especial, nueva infraestructura ni procesos de designación complejos. Es también un instrumento ágil para coordinar posiciones del Ejecutivo frente a procesos legislativos en curso. En cuanto a sus limitaciones estructurales, son significativas: al depender del Ejecutivo, carece de independencia para supervisar las propias prácticas de IA del gobierno, que en muchos países son las de mayor escala e impacto. Por estas razones, sería

una opción viable como solución transitoria mientras se construye la capacidad institucional necesaria para un modelo más robusto, y debería considerarse explícitamente como una etapa, no como un destino.

5. Herramienta de autoevaluación: 30 indicadores de fortaleza institucional

Los siguientes 30 indicadores constituyen una herramienta de autoevaluación que cada autoridad puede aplicar a su propia situación. La escala es de 0 a 3 en cada indicador, donde 0 es ausente, 1 es parcial o en proceso, 2 está presente con brechas, 3 está plenamente implementado. El puntaje máximo es 90. La interpretación del resultado se detalla al final de la sección.

5.1. Dimensión I: Independencia (máx. 18 puntos)

	Indicador	Dimensión	Escala(0-3)	Nivel mínimo operativo
I.1	Rango normativo de la autonomía (constitucional u orgánica con mayoría calificada)	Independencia orgánica	0-3	Mínimo operativo: 2 (ley ordinaria con mayoría calificada)
I.2	Mecanismo de nombramiento con participación multisectorial o parlamentaria y mandatos fijos	Independencia orgánica	0-3	Mínimo operativo: 2 (mandatos fijos, sin discrecionalidad ejecutiva)
I.3	Causales de remoción taxativas y sujetas a control judicial	Independencia orgánica	0-3	Mínimo operativo: 2 (causales tasadas, aunque no todas con control judicial automático)
I.4	Presupuesto propio consignado directamente en ley de presupuesto	Independencia presupuestaria	0-3	Mínimo operativo: 2 (presupuesto propio, aunque con influencia ejecutiva sobre el monto)
I.5	Facultad de impugnar normas ante tribunales judiciales o administrativos	Independencia funcional	0-3	Mínimo operativo: 1 (legitimación activa en al menos algunas materias)
I.6	Incompatibilidades y período de enfriamiento post-mandato (≥2 años)	Independencia interpretativa	0-3	Mínimo operativo: 1

5.2. Dimensión II: Capacidad técnica (máx. 18 puntos)

	Indicador	Dimensión	Escala(0-3)	Nivel mínimo operativo
T.1	Equipo de ciencia de datos / ML con capacidad de auditoría algorítmica (mín. 3 especialistas)	Capacidad técnica interna	0-3	Mínimo operativo: 1 (al menos 1 especialista o acuerdo de asistencia técnica externa)
T.2	Equipo jurídico con formación específica en tecnología y derechos digitales	Capacidad técnica interna	0-3	Mínimo operativo: 2 (al menos 2 juristas con formación relevante)
T.3	Herramientas de análisis estadístico de sesgo y equidad algorítmica	Capacidad metodológica	0-3	Mínimo operativo: 1 (uso de herramientas de código abierto o cooperación con academia)
T.4	Infraestructura tecnológica propia para gestión de casos y análisis de datos	Capacidad técnica interna	0-3	Mínimo operativo: 2 (sistemas de gestión de casos, aunque sin infraestructura analítica propia)
T.5	Programa de formación continua del personal con presupuesto asignado	Desarrollo de capacidades	0-3	Mínimo operativo: 1 (participación en redes internacionales y formación ad hoc)
T.6	Función de monitoreo de tecnologías emergentes y alerta temprana	Prospectiva	0-3	Mínimo operativo: 1 (seguimiento informal o delegado en persona específica)

5.3. Dimensión III: Poderes efectivos (máx. 24 puntos)

	Indicador	Dimensión	Escala(0-3)	Nivel mínimo operativo
P.1	Poder de investigación de oficio sin reclamo previo	Supervisión	0-3	Mínimo operativo: 3 (obligatorio para supervisión efectiva de IA)
P.2	Poder de acceso a sistemas, datos de entrenamiento y logs de inferencia	Supervisión	0-3	Mínimo operativo: 1 (poder general de inspección aplicable a los tratamientos de datos personales en sistemas de IA)
P.3	Poder de requerir documentación técnica (arquitectura, métricas de rendimiento, DPIA)	Supervisión	0-3	Mínimo operativo: 2 (poder de requerir documentación de tratamiento, aplicable a los

	Indicador	Dimensión	Escala(0-3)	Nivel mínimo operativo
				tratamientos efectuados mediante sistemas de IA)
P.4	Poder cautelar de suspensión preventiva de sistemas	Supervisión	0-3	Mínimo operativo: 1 (medidas cautelares previstas en la ley de PDP, aplicables a tratamientos de datos personales en sistemas de IA)
P.5	Poder sancionatorio con multas proporcionales (preferentemente al volumen de negocio)	Enforcement	0-3	Mínimo operativo: 2 (sanciones con efecto disuasorio aunque no basadas en % de facturación)
P.6	Poder normativo vinculante (emitir disposiciones de alcance general)	Regulación	0-3	Mínimo operativo: 2 (poder de emitir instrucciones vinculantes en al menos algunas materias)
P.7	Poder de publicar resoluciones con efecto orientador	Enforcement	0-3	Mínimo operativo: 2 (publicación de resoluciones aunque sea en forma anonimizada)
P.8	Legitimación para recibir denuncias de organizaciones de sociedad civil	Supervisión	0-3	Mínimo operativo: 1 (canales de denuncia ciudadana activos)

5.4. Dimensión IV: Rendición de cuentas y legitimidad (máx. 18 puntos)

	Indicador	Dimensión	Escala(0-3)	Nivel mínimo operativo
L.1	Informe anual ante el Parlamento con comparecencia pública	Rendición de cuentas	0-3	Mínimo operativo: 2 (informe anual público, aunque sin comparecencia parlamentaria formal)
L.2	Publicación sistemática de resoluciones sancionatorias y criterios	Transparencia	0-3	Mínimo operativo: 2 (publicación en al menos los casos más relevantes)
L.3	Registro público de sistemas de IA registrados o notificados	Transparencia	0-3	Mínimo operativo: 0 (deseable pero escasamente disponible hoy en la región)
L.4	Consejo consultivo multisectorial con representación de sociedad civil	Participación	0-3	Mínimo operativo: 1 (mecanismo de consulta,

	Indicador	Dimensión	Escala(0-3)	Nivel mínimo operativo
				aunque no institucionalizado formalmente)
L.5	Canal de denuncias ciudadanas accesible y con tiempos de respuesta definidos	Participación	0-3	Mínimo operativo: 2 (canal activo con respuesta en plazo razonable)
L.6	Evaluación externa periódica del desempeño (revisión por pares o auditores independientes)	Rendición de cuentas	0-3	Mínimo operativo: 1 (participación en revisiones RIPD aunque sin evaluación formal de desempeño)

5.5. Dimensión V: Cooperación y actualización (máx. 12 puntos)

	Indicador	Dimensión	Escala(0-3)	Nivel mínimo operativo
C.1	Participación activa en espacios internacionales (RIPD, grupos de trabajo, adopción de instrumentos)	Cooperación regional	0-3	Mínimo operativo: 2 (membresías activas con participación regular)
C.2	Acuerdos bilaterales de asistencia técnica y mutual recognition	Cooperación bilateral	0-3	Mínimo operativo: 1 (al menos un acuerdo activo con autoridad de referencia)
C.3	Protocolos formales de coordinación con reguladores sectoriales nacionales	Coordinación interna	0-3	Mínimo operativo: 1 (coordinación ad hoc aunque sin protocolo formalizado)
C.4	Mecanismo de revisión periódica del mandato (mínimo quinquenal)	Actualización	0-3	Mínimo operativo: 1 (revisión prevista aunque sin plazo fijo)

5.6. Interpretación del puntaje

Puntaje total	Nivel de fortaleza	Implicaciones para la supervisión de IA
70-90	**Fortaleza alta**	La autoridad puede asumir de manera autónoma la supervisión de los tratamientos de datos personales en sistemas de IA. Fuera de ese ámbito, la supervisión de IA requiere mandato legal. El foco debe estar en actualización metodológica y especialización técnica en IA.
50-69	**Fortaleza media**	La autoridad puede supervisar los tratamientos de datos personales en sistemas de IA con poderes de PDP vigentes. La cooperación con autoridades de referencia es el acelerador más eficiente. Debe

Puntaje total	Nivel de fortaleza	Implicaciones para la supervisión de IA
		identificar las 3-5 brechas más críticas y diseñar un plan de cierre en 18 meses.
30-49	**Fortaleza parcial**	La autoridad tiene capacidad limitada para supervisar los tratamientos de datos personales en sistemas de IA. Requiere reforma normativa en al menos una dimensión (generalmente independencia o poderes). Debe priorizar: (a) articular demandas concretas al legislador; (b) aprovechar al máximo las herramientas disponibles; (c) buscar asistencia técnica regional.
<30	**Fortaleza crítica**	La independencia o la capacidad técnica están por debajo del umbral mínimo operativo. La supervisión efectiva de IA no es posible sin reformas estructurales. La autoridad debe desarrollar una hoja de ruta de reforma institucional.

6. Sistemas de auditoría algorítmica

La auditoría algorítmica es la función supervisora más específica y técnicamente exigente que impone la regulación de IA. Esta sección ofrece a las autoridades una guía operativa para diseñar o fortalecer sus sistemas de auditoría dentro de su mandato existente.

6.1. Tipos de auditoría algorítmica

Cuatro tipos de auditoría pueden articularse con los poderes de PDP vigentes, en tanto el sistema auditado trate datos personales:

- Auditoría de conformidad de PDP aplicada a IA (pre-despliegue): verifica que el sistema cumple con los principios de finalidad, minimización, exactitud y responsabilidad proactiva. Es el tipo más directamente ejercible con poderes de PDP existentes. La DPIA extendida es el instrumento principal.

- Auditoría de sesgo y equidad algorítmica: examina si el sistema produce resultados diferenciados por grupos demográficos. Requiere acceso a métricas de rendimiento desagregadas.

- Auditoría postdespliegue: verifica que el sistema mantiene su comportamiento conforme a los requisitos a lo largo del tiempo. Exige sistemas de logging y mecanismos de notificación a la autoridad.

- Auditoría de incidentes: investigación retroactiva de casos con resultados dañinos. Es el tipo más ejercido por las autoridades de PDP actuales a través de sus procedimientos de investigación.

6.2. Poderes de acceso necesarios y cómo ejercer los existentes

El poder de acceso de las autoridades de PDP, dentro del ámbito material de su legislación, ya cubre varios de los accesos necesarios para auditar los tratamientos de datos personales en sistemas de IA:

- Requerir el registro de actividades de tratamiento del sistema de IA: este poder existe en la mayoría de los marcos modernos de PDP. El contenido mínimo del registro lo fija la norma aplicable. La autoridad puede orientar mediante guías la inclusión de la descripción de los datos de entrenamiento, su origen y las características del modelo.

- Exigir la DPIA del sistema: donde la ley reconoce la DPIA, puede solicitarse para los sistemas de alto riesgo que traten datos personales. Una guía puede orientar la inclusión de métricas de equidad. Su exigibilidad sancionatoria requiere fundamento normativo.

- Inspeccionar la documentación técnica del sistema: el poder de inspección alcanza la documentación del modelo de IA en cuanto forma parte del sistema de tratamiento de datos personales.

- Recibir y analizar estadísticamente los reclamos sobre el mismo sistema: el análisis agregado de reclamos individuales puede revelar patrones de discriminación algorítmica.

6.3. Límites a la interpretación extensiva

Si bien los marcos vigentes permiten a las autoridades de PDP requerir la documentación del sistema de IA, evaluar sus DPIA e inspeccionar los registros de tratamiento en tanto el sistema trate datos personales, existe un núcleo de competencias críticas que excede el alcance de control tradicional. Aquellas medidas que implican una intervención directa sobre la dimensión técnica, dinámica y operativa del modelo de aprendizaje automático no pueden ser inferidas, sino que requieren una habilitación legal y expresa mediante una reforma legislativa.

Este bloque de facultades de control avanzado comprende:

- Auditoría dinámica de decisiones (Acceso a logs de inferencia desagregados): La potestad de exigir el registro técnico, pormenorizado e individualizado de cada procesamiento y salida del algoritmo en tiempo real, superando la noción tradicional de inspección sobre bases de datos estáticas.

- Fiscalización empírica (Adversarial Testing): La atribución para someter al modelo a pruebas de estrés y simulaciones controladas mediante la introducción de datos vectoriales específicos, con el fin de verificar activamente la presencia de sesgos, patrones discriminatorios o vulnerabilidades de reidentificación.

- Tutela cautelar tecnológica (Suspensión preventiva): La facultad de dictar medidas de mitigación inmediata que ordenen el cese temporal o el congelamiento operativo del sistema de IA ante la detección de un riesgo inminente de daño grave o de tratamientos ilícitos a gran escala, sin perjuicio de la sustanciación posterior del procedimiento sancionatorio.

6.4. Metodologías y estándares técnicos de referencia

Algunos de los estándares técnicos disponibles para las auditorías son:

- ISO/IEC 42001:2023: El primer estándar internacional certificable diseñado específicamente para el establecimiento, implementación y mejora continua de un Sistema de Gestión de IA (SGIA) dentro de las organizaciones.

- Métricas de equidad algorítmica: Criterios estadísticos cuantitativos (como la paridad demográfica, la igualdad de oportunidades y la calibración) cuya selección y aplicación no es universal, sino que debe justificarse estrictamente en función del contexto socio-jurídico del tratamiento, dado que ciertos criterios de equidad resultan matemáticamente excluyentes entre sí.

- Directrices de Ciberseguridad de ENISA: Guías técnicas e informes de panorama de amenazas desarrollados por la Agencia de la Unión Europea para la Ciberseguridad, orientados a proteger los modelos de aprendizaje automático frente a ataques de envenenamiento de datos.

- NIST AI Risk Management Framework (AI RMF 1.0, 2023): Uno de los marcos intersectoriales de referencia global más robustos para la gestión de riesgos a lo largo del ciclo de vida de los sistemas de IA.

- Herramientas de auditoría de código abierto: Toolkits técnicos orientados a la detección de sesgos, tales como Fairlearn (Microsoft), AI Fairness 360 (IBM) y What-If Tool (Google). Al estar disponibles bajo licencias libres, reducen las barreras económicas de adopción para las autoridades de control, si bien su despliegue operativo requiere capacidades técnicas especializadas en ciencia de datos.

La selección y uso de estos, y otros, métodos y estándares depende lo que dictamine y decida el equipo técnico.

6.5. Modelos de auditoría

Hay varias respuestas para la pregunta sobre quién debe auditar los sistemas de IA, y concentrar toda la carga en la autoridad reguladora o, en el extremo opuesto, delegarla enteramente en el propio operador, puede producir sistemas que o bien colapsan por falta de recursos o bien carecen de cualquier efecto disuasorio real.

Un modelo adecuado para la región en la fase actual podría ser el de auditoría por capas complementarias. En la base, la autoauditoría documentada opera como obligación general, ya que todo operador de sistemas de IA debe poder demostrar en cualquier momento que su sistema cumple con los estándares aplicables. Esta capa es una extensión directa del principio de responsabilidad proactiva que ya existe en los marcos de protección de datos vigentes. En una segunda capa, la auditoría por tercero certificado se reserva para los sistemas de mayor riesgo: una empresa o entidad independiente, acreditada ante la autoridad, verifica el cumplimiento antes del despliegue y a intervalos periódicos. Esta capa sí requiere construcción de un ecosistema de auditores habilitados, lo que implica definir estándares de certificación y desarrollar oferta de mercado. En la capa superior, la auditoría regulatoria directa queda reservada para las investigaciones de oficio y para los incidentes, ya que es la más costosa y la que más poderes de acceso exige, por lo que su uso selectivo es condición de sostenibilidad.

Algunos proyectos legislativos y modelos en la región han avanzado en el diseño de plataformas nacionales de auditoría algorítmica como órganos técnicos autónomos con capacidad de auditar datasets, identificar sesgos y emitir dictámenes de riesgo vinculantes. Aunque todavía en etapa de propuesta, estos diseños representan el desarrollo conceptual más elaborado disponible en la región y pueden adoptarse como referencia para la creación de unidades de auditoría dentro de las autoridades de protección de datos existentes.

7. Buenas prácticas identificadas en la región

URCDP Uruguay: fortalecimiento gradual y cooperación regional como palancas

El trayecto institucional de la URCDP de Uruguay ilustra un modelo de evolución incremental sumamente valioso para la región. La Unidad no fue erigida originalmente como una agencia especializada en entornos algorítmicos complejos, sino que expandió sus competencias de forma sucesiva mediante hitos normativos clave (Ley 18.331/2008, Ley 19.670/2018 y Decreto 64/020/2020). Su principal lección metodológica es que el fortalecimiento fiscalizador frente a las tecnologías emergentes es viable mediante el acoplamiento normativo por capas, sin la necesidad de aguardar reformas estructurales integrales.

ANPD Brasil: de la autarquía especial a la agencia reguladora

La transformación de la ANPD en una autarquía de naturaleza especial -dotada de autonomía funcional, técnica, decisoria, administrativa y de gestión financiera- se consolidó mediante la Ley Nº 14.460 de 2022 (que tuvo su origen en la Medida Provisoria Nº 1.124/2022). La Ley Nº 15.352/2026 profundizó ese diseño al transformar a la ANPD en agencia reguladora. Estos hitos demuestran que, para fiscalizar entornos complejos como la IA, la autoridad de control debe estar blindada al nivel normativo más alto disponible, garantizando por ley su propia autonomía presupuestaria, de personal y de gobernanza.

AAIP Argentina: el Programa de Transparencia en IA como innovación sin reforma legislativa

El Programa de Transparencia y Protección de Datos en el uso de la Inteligencia Artificial de la AAIP (creado mediante la Resolución Nº 70/2023) constituye un ejemplo regional de cómo una autoridad de PDP puede desplegar una agenda sistemática sobre el tratamiento de datos personales en sistemas de IA dentro de su mandato existente, sin esperar una reforma legislativa. Sus tres pilares estratégicos -Observatorio, Gobernanza y Fortalecimiento- y sus herramientas operativas (como la Guía para el Tratamiento de Datos Personales en Procesos de IA, aprobada por la Resolución Nº 161/2023, y las subsiguientes líneas de trabajo sectoriales para entornos financieros y poblaciones vulnerables como NNA) ofrecen un modelo metodológico y replicable para otras agencias que compartan un marco de competencias similar.

SIC Colombia: circulares sectoriales como soft law de bajo costo

Las directrices de la SIC, cuyo principal hito se materializó en la Circular Externa Nº 002 de 2024, constituyen un ejemplo de cómo una autoridad multifunción (que unifica la tutela de la competencia, el consumidor y la privacidad) puede emitir orientaciones e instrucciones específicas para entornos de IA, en ejercicio de las facultades que le atribuye su legislación, sin necesidad de activar el proceso legislativo. Este modelo de gobernanza basado en instrumentos doctrinarios y circulares de supervisión resulta especialmente valioso para agencias regulatorias que operan en contextos donde las reformas parlamentarias son lentas, complejas o políticamente difíciles, permitiendo una adaptación rápida a los riesgos de la IA generativa y los modelos de lenguaje mediante la aplicación de los principios vigentes de protección de datos.

CPLT Chile: transparencia algorítmica por la vía de la transparencia activa

El Consejo para la Transparencia de Chile dictó, mediante la Resolución Exenta Nº 372 de 2024, recomendaciones sobre transparencia algorítmica dirigidas a los sujetos obligados. El Consejo recomienda mantener a disposición permanente del público, en los sitios electrónicos donde se cumple con la transparencia activa y con actualización al menos mensual, los antecedentes de los sistemas de decisión automatizada o semiautomatizada que tengan efectos en los derechos fundamentales de las

personas o en su acceso a servicios, programas sociales, subsidios, fondos y otros beneficios. Las recomendaciones incluyen referencias específicas a la protección de datos personales.

El caso aporta dos lecciones. La primera es que la visibilidad sobre los sistemas de IA del sector público puede construirse con el régimen de transparencia activa ya vigente, sin crear un registro nuevo ni esperar una ley de IA. La segunda es de articulación institucional: la iniciativa proviene del órgano garante de la transparencia, no de la autoridad de protección de datos. Donde ambas funciones están separadas, la coordinación entre las dos es la condición para que la transparencia algorítmica y la supervisión del tratamiento de datos personales no avancen por carriles independientes.

SPDP Ecuador: norma vinculante sobre IA dentro del mandato de protección de datos

La Superintendencia de Protección de Datos Personales del Ecuador expidió, mediante la Resolución Nº SPDP-SPD-2026-0009-R, la Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial, reformada luego por la Resolución Nº SPDP-SPD-2026-0037-R, que precisa el alcance de las obligaciones aplicables a responsables y encargados. La norma exige gestión de riesgos, evaluación de impacto cuando corresponda y auditorías de los sistemas de IA, conforme a la LOPDP, su Reglamento General y la normativa secundaria.

El Salvador: una ley de IA que delimita la competencia de la autoridad de datos

El Salvador cuenta con una ley específica de inteligencia artificial que encomienda a la Agencia Nacional de Inteligencia Artificial (ANIA) la rectoría del fomento de la IA. Sus artículos 22 y 28 reconocen la supervisión de la Agencia de Ciberseguridad del Estado (ACE) respecto del tratamiento de datos personales mediante modelos de IA. El artículo 17 encomienda a la ANIA un Marco Integral de Evaluación de Riesgos que concilie la innovación tecnológica con la seguridad pública y el bienestar social, con requisitos obligatorios para los sistemas que traten datos confidenciales, reservados o personales y criterios específicos de seguridad definidos a partir de la valoración técnica correspondiente. El artículo 18 dispone que, cuando la IA se utilice con fines comerciales o para acceder a derechos o servicios, debe informarse al usuario si la decisión fue adoptada directamente por un sistema de IA o impulsada por este, proporcionarle una explicación comprensible y transparente del proceso seguido y habilitar mecanismos para impugnarla ante una persona natural competente para confirmarla, modificarla o revocarla.

El diseño separa dos funciones que suelen confundirse: el fomento de la IA y la supervisión del tratamiento de datos personales. La ley de IA no desplaza a la autoridad de datos ni le confiere un mandato general sobre los sistemas, sino que confirma su competencia dentro del ámbito que le es propio. Para los legisladores de la región es una referencia concreta de cómo articular ambas funciones sin superposición de mandatos.

México PNAA: el proyecto de diseño de auditoría algorítmica

A pesar de no haber alcanzado su aprobación definitiva, los proyectos de ley presentados ante el Congreso de la Unión en México (particularmente las iniciativas orientadas a la regulación de la IA y el establecimiento de marcos de desarrollo ético y soberano) contienen uno de los diseños métricos y procedimentales más elaborados de la región para la fiscalización algorítmica. Las propuestas contemplan la creación de unidades técnicas especializadas con competencias explícitas para auditar conjuntos de datos (datasets), identificar sesgos cognitivos o discriminatorios de origen y emitir dictámenes vinculantes de riesgo. Este andamiaje metodológico constituye una referencia idónea para la estructuración interna de nuevas divisiones de auditoría dentro de las autoridades de PDP.

Además de estos proyectos, está en curso un proceso de actualización de la Ley Federal de Protección de Datos Personales en Posesión de Particulares. Entre los elementos considerados figuran las categorías especiales de datos personales, el derecho a no ser objeto de decisiones basadas exclusivamente en tratamientos automatizados, el derecho a la limitación del tratamiento, la designación de un oficial de protección de datos personales, las evaluaciones de impacto, la notificación de vulneraciones de seguridad a la autoridad competente, la privacidad desde el diseño y por defecto y los espacios de experimentación regulatoria. La propuesta incorpora disposiciones sobre tecnologías emergentes, incluida la inteligencia artificial, en los supuestos que involucren tratamiento de datos personales.

8. Hoja de ruta operativa para autoridades de control

La hoja de ruta siguiente ofrece a las autoridades un camino estructurado de fortalecimiento en tres etapas, distinguiendo entre lo que puede hacerse con recursos y poderes actuales y lo que requiere intervención del legislador. Está diseñada para ser adaptable a distintos puntos de partida, tomando como referencia los niveles de fortaleza identificados en la herramienta de autoevaluación.

Etapa	Acciones que puede tomar la autoridad hoy	Acciones que requieren al legislador / ejecutivo
Etapa 1 - Cimientos	• Aplicar la herramienta de autoevaluación y publicar el resultado internamente. • Mapear los sistemas de IA de mayor impacto operando en la jurisdicción (promover el registro voluntario). • Designar un punto focal o unidad de IA dentro de la autoridad, aunque sea con recursos existentes. • Emitir una circular o guía inicial que establezca la posición de la autoridad sobre el tratamiento de datos en sistemas de IA. • Suscribir un acuerdo de asistencia técnica.	• Iniciar diálogo con el poder legislativo para identificar las tres brechas más críticas (típicamente: acceso a sistemas, poderes cautelares, sanciones proporcionales). • Solicitar asignación presupuestaria para 1-2 puestos técnicos especializados en IA.
Etapa 2 - Capacidades	• Desarrollar guías sectoriales para los sectores de mayor riesgo identificados en el mapeo (empezar con 1-2 sectores prioritarios).	• Avanzar en la aprobación de la reforma legislativa para poderes de acceso a sistemas. • Obtener el mandato legal explícito para

Etapa	Acciones que puede tomar la autoridad hoy	Acciones que requieren al legislador / ejecutivo
	• Incorporar la extensión algorítmica en la metodología de DPIA existente. • Capacitar al equipo existente en herramientas de auditoría de sesgo. • Iniciar 1-2 investigaciones de oficio sobre tratamientos de datos personales en sistemas de IA de alto impacto, usando poderes de PDP vigentes. • Participar activamente en grupos de trabajo sobre IA y compartir metodologías.	supervisión de IA. • Establecer el registro voluntario como obligatorio mediante decreto o resolución con base legal.
Etapa 3 - Consolidación	• Lanzar el programa de certificación de auditores algorítmicos de tercero. • Publicar un informe anual específico sobre el estado de la IA en la jurisdicción. • Desarrollar el registro público de sistemas de IA de alto riesgo. • Establecer el consejo consultivo multisectorial con mandato preceptivo.	• Completar el marco normativo: poderes cautelares, sanciones proporcionales, obligatoriedad de logging. • Garantizar autonomía presupuestaria mediante ley de presupuesto con asignación directa. • Iniciar proceso de adecuación UE si aún no está reconocida.

9. Recomendaciones

Las recomendaciones siguientes están organizadas en dos bloques, el primero incluye acciones que las autoridades de control pueden tomar de manera inmediata dentro de sus mandatos existentes. El segundo bloque incluye acciones que requieren intervención del poder legislativo o ejecutivo.

9.1. Para autoridades de control

Aplicar la herramienta de autoevaluación y diseñar un plan de fortalecimiento

Aplicar los 30 indicadores a la situación propia, identificar las 3-5 brechas más críticas, y diseñar un plan de cierre con cronograma y responsables. El plan debe ser público y comunicado al Parlamento en el próximo informe anual.

Emitir guías sectoriales para IA con base en los principios de PDP vigentes

Las guías sectoriales son el instrumento más eficiente disponible hoy. Comenzar con 1-2 sectores prioritarios (empleo, crédito o servicios públicos digitales según el contexto nacional). La RIPD debe coordinar el desarrollo de guías modelo que las autoridades adapten localmente.

Extender la metodología DPIA para cubrir impactos algorítmicos

Emitir una guía que oriente el contenido de toda DPIA sobre sistemas de IA de alto impacto: representatividad del dataset, métricas de equidad, descripción del mecanismo de supervisión humana y protocolo de monitoreo. Ese contenido solo puede fijarse con carácter obligatorio por resolución cuando la ley habilita a la autoridad a dictar normas vinculantes.

Iniciar investigaciones de oficio sobre sistemas de IA de alto impacto

Seleccionar 1-2 sistemas de IA de alto impacto que traten datos personales en la jurisdicción (preferentemente en sector público) y abrir investigación de oficio usando los poderes de PDP existentes. La publicación de los resultados, independientemente del desenlace, genera jurisprudencia administrativa de alto valor orientador.

Suscribir acuerdos de asistencia técnica con autoridades de referencia regional

Los acuerdos entre distintas autoridades pueden brindar asistencia técnica en auditoría algorítmica y metodologías de supervisión.

Desarrollar un programa de formación interno en auditoría de sesgos

Las herramientas de código abierto para auditoría de sesgos son gratuitas y accesibles. Una formación básica del equipo técnico existente habilitaría investigaciones que actualmente no son posibles.

Articular con precisión las demandas al legislador

El mensaje de una autoridad a su legislador debe ser específico, en qué caso concreto no pudo resolver, qué poder exacto faltó, y cuál sería el texto normativo que lo solucionaría. Esto convierte la experiencia supervisora en insumo legislativo directo.

9.2. Para legisladores - Reforma requerida

Garantizar la autonomía de la autoridad al nivel normativo más alto disponible

La autonomía debe estar reconocida en la Constitución o en una ley orgánica que requiera mayoría calificada para su modificación. El mecanismo de nombramiento debe incluir propuesta multisectorial y mandatos fijos.

Conferir mandato legal explícito para la supervisión de IA

Las autoridades de PDP pueden supervisar con sus poderes existentes los tratamientos de datos personales efectuados mediante sistemas de IA. Esa competencia no equivale a un mandato general de supervisión de IA. Un mandato explícito es la vía para extender la supervisión más allá de ese ámbito. También refuerza la base jurídica de sus actuaciones y facilita la asignación de recursos. El mandato puede incorporarse como modificación de la ley de PDP existente o como disposición específica en una

ley de IA. La Ley de Fomento a la Inteligencia Artificial de El Salvador sigue esta segunda vía: sus artículos 22 y 28 reconocen la supervisión de la ACE sobre el tratamiento de datos personales mediante modelos de IA, mientras la ANIA conserva la rectoría del fomento.

Otorgar poder de acceso a sistemas, datos de entrenamiento y logs de inferencia

Este poder debe reconocerse expresamente, con las salvaguardas de confidencialidad técnica necesarias para proteger secretos industriales legítimos. Sin él, la auditoría algorítmica regulatoria directa es imposible.

Habilitar poderes cautelares para suspensión preventiva de sistemas

La autoridad debe poder ordenar la suspensión preventiva de un sistema de IA de alto riesgo por un plazo máximo de 90 días cuando detecte indicios de daño grave. Esta medida debe ser revisable por vía judicial pero ejecutable de manera inmediata.

Actualizar los techos sancionatorios para que sean efectivamente disuasorios

Los techos sancionatorios de leyes de PDP de los años 2000 son insuficientes para grandes operadores tecnológicos. Una referencia puede ser el AI Act europeo (hasta el 7% del volumen de negocio global anual). Incluso una actualización modesta que vincule la sanción al tamaño del operador tiene un efecto disuasorio significativamente mayor.

Obligar a los sistemas de IA de alto riesgo a guardar un historial de sus decisiones

Los sistemas de IA que toman decisiones que afectan derechos -acceso a crédito, empleo, servicios públicos, beneficios sociales- deben conservar un registro detallado de esas decisiones durante un plazo mínimo establecido por ley. Ese registro debe permitir a la autoridad verificar, en cualquier momento, si el sistema está produciendo resultados desproporcionadamente perjudiciales para algún grupo de personas. Además, los operadores de estos sistemas deben inscribirlos ante la autoridad de control, de la misma manera en que hoy se inscriben las bases de datos personales.

Garantizar independencia presupuestaria mediante asignación directa en ley de presupuesto

El presupuesto debe estar consignado directamente en la ley de presupuesto nacional, con mecanismos que impidan su reducción unilateral. Como referencia mínima el presupuesto debe ser proporcional al número de sistemas de alto riesgo registrados y al volumen de reclamaciones atendidas.

Incorporar mecanismos formales de revisión periódica del marco regulatorio

La ley debe prever revisión obligatoria al menos cada cinco años, con participación ciudadana institucionalizada. Las habilitaciones reglamentarias a la autoridad para actualizar la clasificación de riesgos deben ser explícitas.

10. Referencias

Instrumentos normativos e institucionales

- Reglamento (UE) 2024/1689 - AI Act. Publicado 12/7/2024. Entrada en vigor 1/8/2024.
- Ley Nº 14.460/2022 (Brasil), con origen en la Medida Provisoria Nº 1.124/2022 - ANPD como autarquía de naturaleza especial.
- Ley Nº 15.352/2026 (Brasil) - transforma la ANPD en agencia reguladora.
- Ley 21.719 (Chile, 2024) - Agencia de Protección de Datos. Vigencia 1/12/2026. Boletín 18623-07 (2026), en tramitación, propone postergarla hasta diciembre de 2027.
- Consejo para la Transparencia (Chile, 2024). Resolución Exenta Nº 372, recomendaciones sobre transparencia algorítmica.
- Ley 25.326 (Argentina, 2000).
- Ley 29/2021, de protección de datos personales (Andorra).
- Ley Orgánica de Protección de Datos Personales (Ecuador, 2021).
- Resolución Nº SPDP-SPD-2026-0009-R (Ecuador) - Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial.
- Resolución Nº SPDP-SPD-2026-0037-R (Ecuador) - reforma de la Resolución Nº SPDP-SPD-2026-0009-R.
- Ley de Fomento a la Inteligencia Artificial (El Salvador).
- Ley 31814 (Perú, 2023) + DS 115-2025-PCM - SGTD como autoridad de IA.
- Reforma constitucional 'Simplificación Orgánica' (México, DOF 20/12/2024) - Extinción del INAI.

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (México), vigente desde marzo de 2025.
- Ley Federal de Protección de Datos Personales en Posesión de Particulares (México), vigente desde marzo de 2025.
- Estándares de Protección de Datos Personales para los Estados Iberoamericanos (RIPD, 2017 y 2026).
- Plan Estratégico 2026-2030 de la RIPD. XXII Encuentro, Cartagena de Indias, junio 2025.
- AAIP Argentina (2024). Guía para el Uso Responsable de IA.
- SIC Colombia (2024). Circulares Externas 002 y 003.
- NIST AI Risk Management Framework (2023).
- ISO/IEC 42001:2023 - AI Management Systems.
- Ley Básica sobre Inteligencia Artificial (República de Corea, Ley N° 20676, vigente 22/01/2026).

Bibliografía académica y doctrina

- Guilera, S. et al. (2024). Marcos regulatorios de la IA: tendencias emergentes en la agenda legislativa argentina. UTDT-CEPE-GIDE.
- Derechos Digitales (2025). 2024: el año en que la protección de datos nos recordó su lado político.
- Granero, H. R. (2025). Inteligencia artificial en el derecho: entre la innovación y la protección de derechos. Buenos Aires: Eldial.

Estudios comparados sobre autoridades de protección de datos en la región

Foro de la Sociedad Civil (FSC) – Red Iberoamericana de Protección de Datos (RIPD)

- ADC / FSC-RIPD (2023). Estudio comparativo de agencias de protección de datos personales. Tomo I: Perú, Paraguay y Colombia. Redacción: Luis García Balcarce. Validaciones: Hiperderecho, Fundación Karisma, TEDIC.

- ADC / FSC-RIPD (2023). Agencias de protección de datos personales: un estudio comparativo. Tomo II: Argentina y México. Redacción: Luis García Balcarce. Aval: INAI México.

- ADC / FSC-RIPD (2023). Diagnóstico del funcionamiento de agencias de protección de datos. Tomo III: Costa Rica y Panamá. Autoras: Ana Karen Cortés Víquez, Christian Hidalgo García (Cooperativa Sulá Batsú); IPANDETEC. Edición: ADC.

- ADC / FSC-RIPD (2023). Estudio comparativo. Volumen III: Brasil. FSC-RIPD.