



Desafíos y Recomendaciones en la
Gobernanza de Datos
**PARA EL DESARROLLO DE
LA INTELIGENCIA ARTIFICIAL
EN SALUD EN AMÉRICA
LATINA Y EL CARIBE**

CONTENIDO

EQUIPO DE TRABAJO	3
RESUMEN EJECUTIVO	4
GLOSARIO	7
01. INTRODUCCIÓN	8
02. GOBERNANZA DE DATOS EN SALUD: ¿POR QUÉ IMPORTA?	9
INICIATIVAS GLOBALES Y REGIONALES	12
¿QUÉ SON LOS PRINCIPIOS DE GOBERNANZA DE DATOS EN SALUD?	17
03. GOBERNANZA DE DATOS EN SALUD E IA EN AMÉRICA LATINA Y EL CARIBE	25
¿CUÁL ES EL ESCENARIO EN LA REGIÓN?	25
¿CUÁLES SON LOS PRINCIPALES DESAFÍOS?	30
¿QUÉ RECOMENDAMOS?	32
04. CONCLUSIONES	35
05. AGRADECIMIENTOS	36
06. BIBLIOGRAFÍA	37
07. ANEXO	40

EQUIPO DE TRABAJO

SOFÍA PIRSCH: Licenciada en Ciencia Política (UBA). Diplomada en Estudios Avanzados de Género, Cultura y poder (Universidad de San Martín). Candidata a Magister en Ciencia Política (Universidad Torcuato Di Tella) y en Efectividad Clínica (UBA). Becaria de Investigación CIIPS-IECS.

MARTÍN SABÁN: Médico pediatra (UBA). Miembro de la subcomisión de Tecnologías de la Información y Comunicación de la Sociedad Argentina de Pediatría. Candidato a Magister en Efectividad Clínica (UBA). Becario CIIPS-IECS.

DANIEL RIZZATO LEDE: Médico (Universidad Nacional de Cuyo). Especialista en Medicina Interna (HB-UBA) e Informática en Salud (IUHIBA), con experiencia en implementaciones de Salud Digital y en gestión pública sanitaria. Consultor en Salud Digital en CIIPS-IECS.

CINTIA CEJAS: Licenciada en Ciencias Políticas (UCA) y Magister en Ciencias Sociales y de la Salud (FLACSO-CEDES). Especialista en gestión de proyectos de salud. Coordinadora del Centro de Implementación e Innovación en Políticas de Salud (CIIPS-IECS) y del Centro de Inteligencia Artificial en Salud para Latinoamérica y el Caribe (CLIAS).

RESUMEN EJECUTIVO

El documento “**Desafíos y Recomendaciones en la Gobernanza de Datos para el desarrollo de la Inteligencia Artificial en Salud en América Latina y el Caribe**” busca analizar el estado de situación de la gobernanza de datos y del avance de la IA en el sector de la salud en la región, los principales desafíos presentes y cuáles son las herramientas para sortearlos, **utilizando como marco de análisis los Principios de Gobernanza de Datos en Salud.**

¿CÓMO UNA GOBERNANZA DE DATOS ADECUADA PUEDE CONTRIBUIR A DESARROLLOS DE IA EN SALUD RESPONSABLES, EQUITATIVOS, REPRESENTATIVOS Y QUE PRIORICEN A LAS PERSONAS Y LA PROTECCIÓN DE SUS DERECHOS?

- Asegurando la calidad de los datos y así proporcionando insumos de calidad para el desarrollo de algoritmos.
- Facilitando un acceso amplio y ético a conjuntos de datos, para que desarrolladores e investigadores puedan avanzar en soluciones innovadoras de IA.
- Garantizando la privacidad y confidencialidad de los datos, construyendo la confianza necesaria para que las personas compartan sus datos.
- Promoviendo la transparencia en el uso de datos en salud, lo que es fundamental para ganar aceptación y confianza pública.
- Favoreciendo la interoperabilidad de datos entre sistemas de salud para que la creación de modelos de IA cuente con una gama de información más amplia.
- Ofreciendo incentivos y estructuras para la colaboración entre instituciones, investigadores y empresas, fomentando la innovación conjunta en inteligencia artificial en salud.
- Facilitando la estandarización de datos, permitiendo que los modelos de inteligencia artificial sean aplicados de manera coherente en diferentes contextos y ubicaciones.
- Abordando la gestión de sesgos en los datos, promoviendo la equidad, la justicia y la representatividad en los resultados de los modelos de inteligencia artificial aplicados a la salud.
- Salvaguardando los derechos individuales y colectivos en el uso de datos de salud para entrenar modelos de inteligencia artificial, garantizando la protección de la privacidad y la autonomía.

En este sentido, **los desafíos presentes en ALC** pueden resumirse en:

- **Regulatorios:** los países de la región presentan marcos normativos inadecuados para la protección de los datos de las personas y las comunidades.
- **Calidad de los datos:** los repositorios disponibles en la región son escasos y los datos suelen presentar baja calidad y diversos sesgos, lo que supone riesgos de profundización de desigualdades existentes.

- **Infraestructura:** Los países de ALC presentan deficiencias respecto de la infraestructura para el desarrollo de soluciones responsables de IA, como el acceso inequitativo a internet o sistemas de información poco seguros.
- **Capacidad de los Estados:** La falta de agencias especializadas en uso de datos, así como la incapacidad de los Estados para garantizar de manera eficiente la protección y seguridad de los datos de las personas es un desafío para muchos países de la región.
- **Articulación de actores:** Los países de ALC tienen la oportunidad de avanzar hacia estrategias comunes no solo entre los Estados sino también con empresas, universidades y otros actores para definir parámetros comunes para el uso y el intercambio de datos.

En base a estos desafíos, **se presentan recomendaciones para los países de la región:**

REGULATORIAS

- Generar marcos regulatorios amplios, claros, actualizados y confiables sobre gobernanza de datos que garanticen tanto la protección de datos como la promoción de la innovación. Estos marcos deberían incluir cuestiones específicas para el abordaje y uso seguro de los datos sanitarios.
- Las normativas deben prever la protección de los datos frente a la agregación de éstos para armados de perfiles poblacionales.
- Incorporar la gobernanza de datos en salud en los diferentes niveles del sistema de salud: desde el gobierno, pero también desde hospitales, centros de atención, universidades y cualquier institución vinculada.

CALIDAD DE LOS DATOS

- Fomentar la recolección y utilización de datos locales, que se correspondan con el contexto de los países de la región y a los perfiles demográficos y epidemiológicos para generar soluciones de mejor calidad, más representativas de las poblaciones locales.
- Procurar la reducción y control de sesgos durante todo el desarrollo de los proyectos de IA.
- Incentivar la generación de bases de datos públicas actualizadas y con datos completos y de calidad.
- Capacitar a las personas encargadas de trabajar con datos en cualquiera las fases del ciclo del dato para garantizar que se preserve la calidad de los datos.
- Incorporar en las currículas educativas de los profesionales de la salud en formación elementos de uso y manejo de datos.

ÉTICAS

- Abordar las cuestiones éticas desde las etapas iniciales del diseño del proyecto hasta la implementación y el seguimiento.

- Participación de expertos en ética y otras disciplinas desde el comienzo de los proyectos para mitigar los sesgos.
- Procurar la anonimización de los datos sanitarios, el alojamiento de los datos en sitios seguros, así como su archivo temporal y compartimentado.
- Recolectar datos para responder una pregunta de investigación, es decir, con un fin específico.

INFRAESTRUCTURA

- Fomentar la inversión propia y extranjera para infraestructura digital.
- Diseñar planes integrales de ciberseguridad que incluyan expertos de diferentes disciplinas para conseguir tener una mirada integral, incluyendo al sector salud.

CAPACIDADES DE LOS ESTADOS

- Promover la existencia de agencias especializadas en uso y protección de datos, privacidad, acceso a la información, y que estas agencias cuenten con expertos en datos en salud.
- Incentivar la formación de una burocracia estatal especializada en el uso de datos y uso de datos en salud.
- Elaborar manuales, lineamientos o guías de buenas prácticas para que los desarrolladores de aplicaciones de IA en salud conozcan el recorrido gubernamental que deben seguir para desarrollar una solución de IA en salud.
- Promover el diseño e implementación de Estrategias Nacionales de Salud Digital para fomentar la innovación y articular la gobernanza de datos desde objetivos claros.
- En países federales o con mayores niveles de descentralización, se debe contemplar la adecuación de la gobernanza de datos a los niveles subnacionales.

ARTICULACIÓN DE ACTORES

- Promover la articulación entre los Estados nacionales y organismos regionales e internacionales para avanzar hacia objetivos comunes.
- Fomentar la participación de diferentes actores: desarrolladores, start ups, academia, ciudadanos y otros, para acompañar a los gobiernos en la creación de los ecosistemas.
- Estimular la participación y la educación digital en los ciudadanos para hacerlos para una mayor concientización sobre sus derechos, obligaciones y responsabilidades sobre el uso de sus datos.

Los Principios de Gobernanza de Datos en Salud se presentan como una valiosa herramienta para abordar de manera integral estos desafíos mencionados, al promover la generación de un ecosistema óptimo para la innovación en IA en salud, sin perder de vista el respeto a los derechos humanos, la seguridad de las personas y la promoción de la equidad en los sistemas sanitarios.

GLOSARIO

ALC: América Latina y El Caribe

BID: Banco Interamericano de Desarrollo

CEPAL: Comisión Económica para América Latina y el Caribe

CJI: Comité Jurídico Interamericano

CLIAS: Centro de Inteligencia Artificial y Salud para América Latina y el Caribe.

CNAI: Centro Nacional de Inteligencia Artificial de Brasil

CUS: Cobertura Universal de Salud

DDHH: Derechos Humanos

EBIA: Estrategia Brasileña de Inteligencia Artificial

GDPR: Reglamento General de Protección de Datos

HCE: Historia Clínica Electrónica

IA: Inteligencia Artificial

ICG: Índice de Ciberseguridad Global

I+D: Investigación y Desarrollo

MERCOSUR: Mercado Común del Sur

OCDE: Organización para la Cooperación y el Desarrollo

ODS: Objetivos de Desarrollo Sustentable

OEA: Organización de los Estados Americanos

OMS: Organización Mundial de la Salud

OPS: Organización Panamericana de la Salud

ONU: Organización de las Naciones Unidas

PB: Petabytes

RIPD: Red Iberoamericana de Protección de Datos

T&E: Transparencia y Explicabilidad

UE: Unión Europea

UNCTAD: Conferencia de las Naciones Unidas sobre Comercio y Desarrollo

UNESCO: Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura

UIT: Unión Internacional de Telecomunicaciones

01. INTRODUCCIÓN

El presente documento se propone ilustrar el estado y los desafíos que enfrenta la región de América Latina y el Caribe (ALC) sobre la gobernanza de los datos en salud para el desarrollo de soluciones de Inteligencia Artificial (IA) en este sector.

Los grandes avances tecnológicos que han tenido lugar desde las últimas décadas suponen un amplio horizonte de posibilidades y beneficios producto de la existencia de grandes caudales de datos personales, tanto sanitarios como de identificación, contacto, demográficos, financieros, educativos, entre otros. La IA ya ha demostrado no sólo su potencial para transformar los sistemas y servicios de salud, sino también su capacidad para mejorar la salud a través de diagnósticos más asertivos, personalización de los tratamientos y mejoras en el acceso a la salud a través de diversos desarrollos innovadores.

No obstante, la existencia de este recurso tan importante supone también la **necesidad de principios, políticas, regulaciones y prácticas** que guíen la gestión eficiente de los datos para garantizar que éstos tengan un tratamiento responsable, seguro, respetuoso de los derechos humanos, la privacidad, en pos de mejorar la salud de las poblaciones e individuos, evitando generar y profundizar brechas ya existentes, y previniendo la reproducción de sesgos de género,

lenguaje, características físicas y otras potenciales fuentes de discriminación. **A esto se le denomina “gobernanza de datos”.**

Este documento busca abordar la compleja intersección entre **la gobernanza de datos y la implementación de desarrollos de IA en salud en América Latina y el Caribe (ALC), considerando la existencia de los Principios de Gobernanza de Datos en Salud**, que brindan un marco conceptual para pensar soluciones a los desafíos presentes en la región.

Para esto se llevó adelante una búsqueda y revisión de literatura, se realizaron cinco entrevistas a siete expertos y un webinar con panelistas especializados en diferentes áreas vinculadas a la IA, la gobernanza de datos y la salud digital. Como resultado, se explora el escenario actual para conocer cuáles son las herramientas vigentes con las que cuentan los países para la gobernanza de datos y la protección de la información de las personas, así como también el nivel de desarrollo que presenta la IA en general y en salud en particular. Además, se identifican los principales desafíos y obstáculos que los países de la región enfrentan en estas áreas y, en función de eso, se proponen recomendaciones para mejorar la gobernanza de datos, promoviendo la innovación.

02. GOBERNANZA DE DATOS EN SALUD: ¿POR QUÉ IMPORTA?

La implementación masiva de tecnologías digitales está ocasionando transformaciones significativas en todas las industrias y sectores, incluido el sector de la salud. En este proceso de cambio, **los datos se consolidan como un activo fundamental para cualquier organización.**

Los grandes avances tecnológicos de las últimas décadas y el desarrollo de la Inteligencia Artificial (IA) en el ámbito de la salud han abierto un horizonte de beneficios y de potencialidades que ya han cambiado radicalmente la investigación y también la atención médica. La agilidad y precisión en el diagnóstico y tratamiento de enfermedades, así como la mayor eficiencia en la atención médica son sólo algunas de las ventajas que las innovadoras herramientas pueden brindar. La IA también ha aportado la capacidad de identificar patrones y tendencias en grandes conjuntos de datos, lo que facilita la detección temprana de enfermedades y la toma de decisiones basadas en evidencia, permite una atención médica personalizada adaptando tratamientos y cuidados de manera precisa a las necesidades individuales de cada paciente, y la generación de soluciones innovadoras a problemas complejos.

Los datos sanitarios son un insumo fundamental para estos desarrollos. La digitalización ha posibilitado un crecimiento exponencial en la producción y aplicación de datos relacionados con la salud. Se estima que un hospital puede generar hasta 50 petabytes (PB) por año (1 PB equivale a 500 mil millones de páginas de texto)¹. **Esta amplia disponibilidad de información oportuna conlleva notables ventajas para profesionales de la salud, responsables políticos y ciudadanos interesados en mejorar tanto la salud individual como la pública.**

De acuerdo con informe elaborado en 2021 por la Comisión Económica para América Latina y el Caribe (CEPAL)², **la valoración de los datos como un componente crítico para la toma de decisiones ha impulsado diversas iniciativas a nivel gubernamental, tanto a nivel nacional como regional e internacional.** Como resultado, se han desarrollado marcos conceptuales que abordan aspectos clave para una gobernanza efectiva de datos en términos estratégicos y técnicos. Estos marcos consideran elementos como la **calidad de los datos, la interoperabilidad, la infraestructura y la seguridad**, entre otros. En esta dirección, muchos gobiernos han adoptado estrategias nacionales de datos con el objetivo de fomentar políticas públicas coherentes y maximizar el potencial del uso de datos, aunque estos avances varían entre países y dependen de los contextos locales.

La gobernanza de datos también ha experimentado algunos avances en los gobiernos latinoamericanos en la última década, aunque aún enfrenta desafíos notables en términos de acceso, uso, protección de datos y diseño de políticas basadas en evidencia. Aunque algunos países se destacan en la apertura de datos, pocos han logrado establecer una cultura de datos y desarrollar un programa integral de gobernanza de datos. Por lo tanto, **es necesario fomentar una mayor conciencia sobre el potencial de los datos entre los tomadores de decisiones, los ciudadanos y la sociedad civil para integrarlos eficazmente en la agenda pública².**

La gestión de los datos en el ámbito de la salud presenta particularidades significativas que conllevan desafíos en su manejo y transformación en

información útil. **Uno de los desafíos principales radica en encontrar el delicado equilibrio entre garantizar la disponibilidad de los datos y mantener su seguridad, considerando la sensibilidad inherente de la información médica.** Una mayor disponibilidad y apertura de los datos personales y sanitarios de las personas puede facilitar y promover grandes mejoras en la atención y el acceso a la salud, pero esta información forma parte de la vida privada e íntima de las personas y su divulgación o su uso para fines diferentes de aquellos para los cuales fueron recolectados conlleva la posibilidad de **discriminación, estigmatización y violaciones a los derechos humanos.**

La divulgación no autorizada de datos sensibles puede derivar en discriminación laboral, ya que una persona podría no ser contratada en base a sus condiciones médicas, o también una persona podría ser víctima de chantaje o extorsión siendo amenazada con revelar su información de salud. Además, esto podría tener consecuencias de tipo psicológico, como ansiedad o depresión sobre la persona afectada.

Otro desafío presente en la generación y uso de los datos en salud se relaciona con su **fragmentación**. En muchos casos los datos sanitarios de las personas se recopilan en silos separados, lo que favorece la existencia de duplicaciones y múltiples versiones de la misma información. La **interoperabilidad** emerge como una solución crucial para establecer puentes entre estos silos, permitiendo compartir datos de manera eficiente, facilitar el acceso oportuno y garantizar su integridad.

La fragmentación de los datos sanitarios produce varios problemas: desde imposibilidad de contar

con una historia clínica integrada y que los profesionales de la salud no puedan tener una visión integral de la salud de los pacientes, hasta errores médicos, duplicación de diagnósticos y demoras en las entregas de resultados. Además, los datos fragmentados dificultan la innovación en IA, ya que ésta y otras tecnologías necesitan grandes cantidades de datos de calidad.

Además, la **agregación** de datos, que implica la necesidad de combinar y consolidar información de diversas fuentes, se convierte en el fundamento esencial para la toma de decisiones en todos los niveles de gestión del ámbito de la salud. La máxima expresión de esta agregación es la utilización de los datos para impulsar la inteligencia empresarial (business intelligence) y análisis (analytics), que permiten una toma de decisiones informada y estratégica. Cabe señalar, además, que en la actualidad el 80% de la información generada no se encuentra estructurada,³ y **una deficiente gobernanza de los datos sanitarios podría intensificar las disparidades, perpetuar sesgos y discriminación hacia grupos marginados y menoscabar los derechos humanos y la salud de las personas.**

El uso agregado de datos permite, por ejemplo, llevar adelante el análisis epidemiológico de enfermedades, al obtener información valiosa a nivel poblacional y al poder realizar análisis estadísticos para identificar tendencias y patrones. Contar con esta información permite que los tomadores de decisión puedan elaborar políticas públicas basadas en evidencia.

¿Cuáles son las distintas formas en que una deficiente gobernanza de datos en salud puede fomentar la discriminación hacia las personas?

- **Sesgos en recopilación de datos:** por ejemplo, si un sistema sólo recopila datos de hospitales ubicados en zonas urbanas, pero no incluye datos de comunidades rurales se crea un sesgo geográfico en los datos, ya que las condiciones de salud y los patrones de enfermedades pueden diferir entre ambas áreas.

- **Sesgos en algoritmos y modelos predictivos:** por ejemplo, si se entrena un algoritmo para predecir el riesgo de enfermedades cardíacas utilizando datos históricos sesgados hacia la población blanca, el modelo puede no ser preciso para predecir el riesgo en poblaciones de minorías étnicas, ya que no ha aprendido adecuadamente de su diversidad.

- **Falta de transparencia y rendición de cuentas:** por ejemplo, si una organización utiliza un algoritmo para asignar recursos médicos, pero no divulga cómo se toman esas decisiones ni proporciona un mecanismo claro para que los pacientes impugnen las decisiones, esto puede ocultar sesgos y dificultar la identificación y corrección de problemas.

- **Falta de representación en la toma de decisiones:** por ejemplo, si un comité de gobernanza de datos está compuesto principalmente por profesionales de la salud de una sola especialidad y no incluye representación de comunidades minoritarias, esto puede llevar a decisiones que no consideran completamente las necesidades y perspectivas de grupos diversos.

- **Desigualdades en el acceso y uso de la tecnología:** por ejemplo, si una aplicación de monitoreo de la salud se basa en dispositivos móviles, pero aquellos que no tienen acceso a smartphones o una conexión a Internet robusta no pueden utilizarla. Esto crea un sesgo en los datos recopilados, ya que excluye a aquellos que podrían enfrentar desigualdades en el acceso a la tecnología.

Estas particularidades ilustran la complejidad y la importancia de que el uso de los datos en salud se encuentre enmarcado dentro de parámetros de gobernanza que garanticen la seguridad de las personas y sus datos, promuevan el acceso equitativo a la salud y valores éticos y protejan los derechos humanos, en el contexto de una mayor aplicación de la inteligencia artificial en la salud a nivel mundial. En ALC, además, las disparidades dentro de los países en el acceso a la salud, a Internet y al desarrollo tecnológico suman complejidad al escenario.⁴

La gobernanza de datos implica, principalmente, el conjunto de principios, políticas y prácticas que buscan garantizar la gestión eficiente de los datos para tomar decisiones sobre éstos a lo largo de su ciclo de vida con el fin de optimizar la capacidad de un individuo, organización o gobierno para la gestión política, estratégica y operativa. **Específicamente en salud, refiere al proceso de gestión y toma de decisiones para guiar la generación, recopilación, almacenamiento y gestión de los datos de salud a través de políticas, prácticas, normas, puntos de referencia y reglamentos normativos, procesables y transversales.**⁵

Las nuevas tecnologías avanzan más rápido que la capacidad de los Estados para dar respuestas normativas y de políticas públicas pero esto, si bien resulta un gran desafío, **también supone oportunidades para el desarrollo de reglamentos, políticas y acuerdos a nivel nacional e internacional** que protejan a los habitantes, en especial a las poblaciones y comunidades vulnerables, a la vez que fomentan la transformación digital.

Una de las herramientas más usadas a nivel internacional son las denominadas “**soft laws**”, o **leyes blandas**. Estos instrumentos legales son normas no vinculantes, es decir que no imponen obligaciones legales específicas y no generan consecuencias legales directas en caso de incumplimiento. Suelen adoptar la forma de **declaraciones, resoluciones, códigos de conducta, principios y directrices, y sirven para brindar orientación y estándares de buenas prácticas en diversas áreas, ayudar a la formulación y desarrollo de políticas, mejorar la coordinación internacional entre los países, son más flexibles y adaptables a los contextos que las leyes vinculantes**. En contextos dinámicos y de gran velocidad en el avance de las tecnologías, estos instrumentos toman mayor relevancia y utilidad.

Para orientar a los países hacia una mejor **gobernanza de datos, la salud digital e IA en ALC y el mundo**, diferentes organismos internacionales han utilizado estos recursos. **A continuación, se presentan brevemente algunas de estas iniciativas regionales o globales.**

INICIATIVAS GLOBALES Y REGIONALES

Dentro de la comunidad internacional, uno de los principales recursos orientadores que han tenido los Estados miembros de la Organización de las Naciones Unidas (ONU) son los **Objetivos de Desarrollo Sostenible (ODS)**, que forman parte de la Agenda 2030 que la ONU estableció en el año 2015. Los ODS que definen 17 áreas sobre las cuales los países tienen oportunidad de avanzar en pos del desarrollo económico y diferentes necesidades sociales que contribuyan a la erradicación de la pobreza.⁶ En este sentido, **la gobernanza de datos en salud, las nuevas tecnologías, el avance de la IA y la importancia de reducir las desigualdades y brechas tecnológicas para favorecer la equidad tanto en el acceso a servicios de salud como también en el acceso a estas nuevas tecnologías encuentran eco en varios de ellos.**

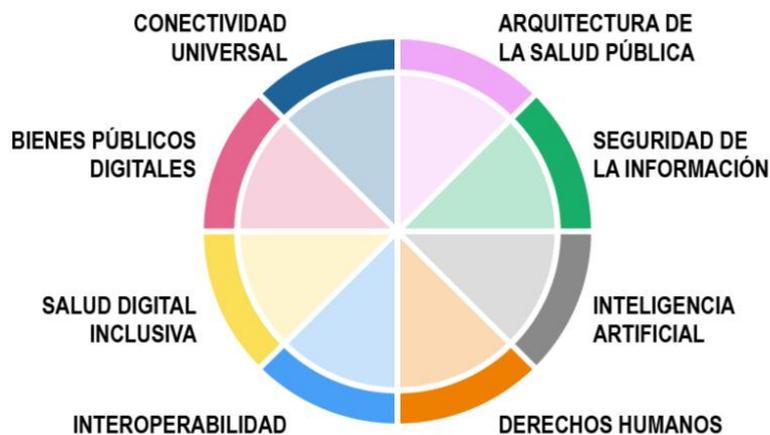
ODS 1: Fin de la pobreza	Incluye que todas las personas, especialmente los pobres y los más vulnerables, tengan los mismos derechos a acceder a recursos económicos, servicios básicos, propiedad de la tierra y otros bienes, herencia, recursos naturales, nuevas tecnologías y servicios económicos.
ODS 3: Salud y bienestar	Incluye entre sus metas lograr la Cobertura Universal de Salud (CUS) y la implementación de estrategias de Salud Digital.
ODS 5: Igualdad de género	Destaca la importancia del acceso equitativo a los avances tecnológicos para promover el empoderamiento de las mujeres.

<p>ODS 9: Industria, Innovación e Infraestructuras</p>	<p>Contempla entre sus metas apoyar el desarrollo de tecnologías, la investigación y la innovación nacionales en los países en desarrollo y aumentar el acceso a la tecnología de la información y las comunicaciones a Internet.</p>
<p>ODS 10: Reducción de las desigualdades</p>	<p>Enfatiza en la generación de normativa y políticas públicas de parte de los Estados para reducir las desigualdades interseccionales que atraviesan a las poblaciones en cuestiones económicas, sociales y de género, entre otros.</p>
<p>ODS 16: Paz, Justicia e Instituciones Sólidas</p>	<p>Establece la necesidad de crear instituciones eficaces y transparentes que rindan cuentas, de garantizar la adopción en todos los niveles de decisiones inclusivas, participativas y representativas, ampliar y fortalecer la participación de los países en desarrollo en las instituciones de gobernanza mundial y garantizar el acceso público a la información y proteger las libertades de acuerdo con las leyes nacionales y los acuerdos internacionales.</p>

Fuente: Objetivos de Desarrollo Sostenible, Organización de Naciones Unidas⁶

De esta manera, **los ODS buscan marcar el camino para que los diferentes Estados avancen en políticas y tomen decisiones orientadas a reducir las brechas y disparidades existentes en la población en el acceso a la salud, al desarrollo tecnológico y a las garantías institucionales en pos de un desarrollo no sólo sostenible sino también equitativo y que no deje a nadie atrás.**

Asimismo, como parte de su plan de acción 2019-2023 de Sistemas de Información para la Salud (IS4H), la Organización Panamericana de la Salud (OPS/PAHO) propuso **8 Principios para la Transformación Digital del Sector Salud**, que buscan ser un marco que oriente a los países de la región en los procesos de transformación digital y les permita avanzar en la toma de decisiones y la formulación de políticas públicas en esta temática, sin descuidar la búsqueda de la equidad en salud.⁷



Por su parte, **y respecto de los avances de la IA**, algunos organismos como la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO)⁸, la Organización para la Cooperación y Desarrollo (OCDE)⁹, la Organización

Mundial de la Salud (OMS)¹⁰ también elaboraron marcos, recomendaciones, principios o guías para orientar y promover el desarrollo de la IA centrada en el respeto a los derechos humanos, de manera confiable, segura y efectiva.

<p>UNESCO: Recomendación sobre la Ética de la Inteligencia Artificial⁸</p>	<p>4 valores fundamentales:</p> <ul style="list-style-type: none"> ○ Derechos Humanos y dignidad humana ○ Vivir en sociedades pacíficas ○ Garantizar la diversidad y la inclusión ○ Florecimiento del medio ambiente y los ecosistemas <p>10 principios básicos:</p> <ul style="list-style-type: none"> ○ Proporcionalidad e inocuidad ○ Seguridad y protección para prevenir posibles daños ○ Derecho a la intimidad y protección de datos ○ Gobernanza y colaboración de las partes interesadas ○ Responsabilidad y rendición de cuentas ○ Transparencia y explicabilidad (T&E) ○ Supervisión y decisión humanas ○ Sostenibilidad ○ Sensibilización y educación ○ Equidad y no discriminación
<p>OCDE: Principios para promover el uso de la IA en el marco de los DDHH y la democracia⁹</p>	<p>Principios orientados a promover el uso de la IA de manera innovadora y confiable, en el marco del respeto a los derechos humanos y la democracia:</p> <ul style="list-style-type: none"> ○ Crecimiento inclusivo ○ Desarrollo sustentable y bienestar ○ Valores centrados en el ser humano y la equidad ○ Transparencia y explicabilidad ○ Robustez ○ Seguridad y protección ○ Rendición de cuentas / accountability <p>Principios orientados a establecer recomendaciones a hacedores de políticas públicas</p> <ul style="list-style-type: none"> ○ Invertir en investigación y desarrollo (I+D) en IA ○ Fomentar un ecosistema digital para la IA

	<ul style="list-style-type: none"> ○ Crear un entorno político propicio para la IA ○ Desarrollar la capacidad humana y prepararse para la transformación del mercado laboral ○ Cooperación internacional para una IA confiable.
<p>OMS: Guía de consideraciones regulatorias para la IA en salud¹⁰</p>	<p>Seis áreas para la regulación de la IA</p> <ul style="list-style-type: none"> ○ Transparencia y documentación ○ Gestión de riesgos y claridad sobre el uso previsto de los datos ○ Calidad de datos ○ Validación externa de datos ○ Privacidad y protección de datos ○ Fomentar la colaboración entre los diferentes actores
<p>Khipu – Encuentro Latinoamericano de IA: Declaración de Montevideo sobre IA y su impacto en América Latina¹¹</p>	<p>Las tecnologías, y en especial la IA, deben:</p> <ul style="list-style-type: none"> ○ Beneficiar a las personas, y priorizando la mejora de la calidad de vida, las condiciones económicas, de salud y bienestar general ○ Cumplir con los Derechos Humanos, evitar la perpetuación de estereotipos o la exacerbación de la desigualdad ○ No causar daño a las personas y minimizar el impacto ambiental ○ Evaluar previamente y mitigar el riesgo desde su diseño ○ Respetar la diversidad cultural en el diseño y entrenamiento de modelos de IA para evitar la exclusión de las perspectivas latinoamericanas ○ Involucrar a las poblaciones ○ Fortalecer la soberanía de los países latinoamericanos en cuestiones estratégicas y regulatorias de la IA

Estos diferentes principios o estándares demuestran que existe un **interés compartido de parte de la comunidad internacional en impulsar la IA de acuerdo a ciertos preceptos básicos, como el respeto a los derechos humanos, la seguridad de las personas y sus datos, la transparencia y la rendición de cuentas, la cooperación y la no discriminación ni reproducción de desigualdades.**

Respecto de la **protección de los datos sanitarios y cualquier tipo de datos personales de los individuos y las comunidades**, esta necesidad fue abordada también por diferentes organizaciones transnacionales. Las iniciativas más sobresalientes son el **Convenio 108**

del Consejo de Europa, titulado **"Convención para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal"**, la **Reglamentación General de Protección de Datos (RGDP o GDPR)** de la Unión Europea¹², los **"Estándares de Protección de Datos de los Estados Iberoamericanos"** de la Red Iberoamericana de Protección de Datos (RIPD),¹³ y los **Principios Actualizados sobre la Privacidad y la Protección de Datos Personales** adoptados por el **Comité Jurídico Interamericano (CJI)** y aprobados por la **Asamblea General de la Organización de los Estados Americanos (OEA)**.

<p>Convenio 108 del Consejo de Europa: Convención para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal</p>	<ul style="list-style-type: none"> ○ Entiende los datos personales como cualquier información relacionada con una persona identificada o identificable ○ Garantiza la protección de los derechos y libertades fundamentales de las personas respecto de esos datos ○ Establece que los datos sean recopilados de manera justa y legal, y que sean adecuados y relevantes ○ Reconoce los derechos de los individuos sobre sus datos: acceso, rectificación, oposición. ○ Facilita transferencia transfronteriza ○ Establece requisitos para seguridad y confidencialidad ○ Fomenta la creación de autoridades de supervisión independientes ○ Requiere notificación de las violaciones de seguridad ○ Reconoce derecho a indemnización por uso o tratamiento ilícito de los datos.
<p>UE: Reglamentación General de Protección de Datos (RGDP o GDPR)</p>	<ul style="list-style-type: none"> ○ Establece el ámbito de aplicación extraterritorial ○ Principios para el procesamiento de datos: legalidad, equidad, transparencia, limitación de la finalidad y minimización de datos ○ Refuerza la necesidad de consentimiento informado ○ Reconoce los derechos de los individuos como titulares de datos: acceso, rectificación, supresión, portabilidad y oposición ○ Establece la obligatoriedad de notificación de violaciones de datos ○ Fomenta la designación de un delegado de protección de datos ○ Recomiendan evaluaciones de impacto de protección de datos ○ Regula las transferencias internacionales de datos ○ Establece sanciones y multas
<p>RIPD: Estándares de Protección de Datos de los Estados Iberoamericanos</p>	<p>Principios para la protección de datos:</p> <ul style="list-style-type: none"> ○ Legitimación ○ Licitud ○ Transparencia ○ Lealtad ○ Finalidad ○ Proporcionalidad ○ Calidad ○ Responsabilidad ○ Seguridad ○ Confidencialidad ○ Responsabilidad de los encargados de la gestión de los datos ○ Derechos de los titulares: acceso, rectificación, cancelación, oposición y portabilidad.

**OEA: Principios Actualizados
sobre la Privacidad y la
Protección de Datos
Personales**

Principios para el uso de datos de las personas

- Finalidades legítimas y lealtad
- Transparencia y consentimiento
- Pertinencia y necesidad
- Tratamiento y conservación limitados
- Confidencialidad
- Responsabilidad
- Seguridad
- Exactitud de los datos
- Derecho de los titulares al acceso, rectificación, cancelación, oposición y portabilidad
- Consideración de los datos personales sensibles
- Flujo transfronterizo de los datos.

Todas estas iniciativas comparten puntos en común sobre los parámetros que deben guiar la protección de los datos de las personas, estableciendo los derechos de los titulares de éstos, el flujo de datos entre los países, la necesidad de desarrollar medidas de seguridad y la importancia del tratamiento justo y responsable de estos datos.

Resulta claro, entonces, que **la necesidad de fortalecer la gobernanza de los datos de salud es un tema presente en la agenda global y de la región de ALC**. El gran avance de las tecnologías requiere de un conjunto de principios aceptados para la gestión de estos datos, que reflejen la diversidad regional y sectorial, con el propósito de corregir la desigual distribución de beneficios y perjuicios que actualmente resulta de la recopilación, análisis y utilización de estos datos, que además son considerados sensibles. **Un enfoque que permita fortalecer y promover la innovación sin dejar a nadie atrás es, entonces, una herramienta necesaria para los desafíos del presente y futuro.**

¿QUÉ SON LOS PRINCIPIOS DE GOBERNANZA DE DATOS EN SALUD?

En este escenario, la Coalición Transform Health junto con numerosos expertos del ámbito de la salud digital elaboraron los **Principios de Gobernanza de Datos en Salud**, con el objetivo de aportar una perspectiva de derechos humanos y equidad al uso de datos en salud y contribuir a la construcción de sistemas de salud resilientes y sostenibles que avancen hacia la Cobertura Universal de Salud (CUS).¹⁴

Estos Principios buscan, además, **contribuir a la creación de un marco global de gobernanza de los datos salud que pueda respaldar el uso de tecnologías y datos digitales en beneficio del bienestar colectivo**. Fueron diseñados y promovidos desde la sociedad civil a través de un proceso inclusivo y consultivo e incorporando amplia variedad de perspectivas y conocimientos procedentes de distintas regiones geográficas, sectores y partes interesadas

para orientar a gobiernos, empresas tecnológicas y otros actores involucrados en la recopilación y uso de datos de salud, así como para ser una herramienta esencial para las organizaciones que abogan por una gobernanza equitativa de los datos sanitarios basada en los derechos humanos. En este sentido, **los Principios se consideran un bien público,**

disponibles para ser incorporados en el trabajo político, el diseño de políticas y la defensa de los datos sanitarios.

Los Principios se encuentran organizados alrededor de tres ejes fundamentales: **proteger a las personas, promover el valor de la salud y priorizar la equidad.**

PROTEGER A LAS PERSONAS	PROMOVER EL VALOR DE LA SALUD	PRIORIZAR LA EQUIDAD
Proteger a las personas y a las comunidades	Mejorar los sistemas y servicios sanitarios	Promover los beneficios equitativos de los datos sanitarios
Abordar el riesgo individual y colectivo	Evaluar los beneficios de los datos sanitarios	Representar equitativamente a todos los grupos y poblaciones en los datos
Recopilar datos con fines definidos	Utilizar los datos para mejorar los servicios sanitarios de las personas y las comunidades	Tener en cuenta las necesidades específicas de los grupos marginados
Recopilar datos personales o sensibles sólo cuando sea necesario y con el consentimiento informado	Fomentar una cultura de información y acción basada en datos	Atenuar el sesgo de los datos
Utilizar mecanismos seguros de recopilación y almacenamiento de datos	Abordar la eficacia, la eficiencia y la resiliencia del sistema sanitario	Utilizar lenguaje accesible y colmar lagunas de conocimiento
Desidentificación y anonimización	Reforzar la propiedad comunitaria de los datos sanitarios	Establecer mecanismos de retroalimentación de datos inclusivos
Definir los usos abusivos de los datos sanitarios	Capacitar y empoderar al personal sanitario de primera línea	Promover un impacto y beneficio equitativos

DESAFÍOS Y RECOMENDACIONES EN LA GOBERNANZA DE DATOS
**PARA EL DESARROLLO DE LA INTELIGENCIA ARTIFICIAL EN SALUD
 EN AMÉRICA LATINA Y EL CARIBE**

Establecer salvaguardas contra la discriminación, la estigmatización, el acoso y los prejuicios.	Promover el intercambio de datos e interoperabilidad	Establecer los derechos y la propiedad de los datos
Presentar directrices específicas para los grupos y poblaciones marginados	Establecer normas y directrices para compartir datos	Aplicar la perspectiva de los derechos humanos a la gobernanza de los datos sanitarios
Crear confianza en los sistemas de datos	Comprobar el consentimiento informado antes de compartir datos	Definir claramente las funciones y responsabilidades de gobernanza
Respetar las mejores prácticas de protección de datos y privacidad	Promover la interoperabilidad de los sistemas de datos	Ampliar los derechos y la propiedad de los datos a los productos y servicios
Asegurar que el consentimiento sea informado y entendido en toda su complejidad	Definir estructuras de datos comunes a todos los sistemas sanitarios	Desarrollar fideicomisos y cooperativas de datos sanitarios
Obtener el consentimiento colectivo cuando sea necesario.	Establecer varios niveles de acceso a los datos	Emplear mecanismos de gobernanza participativa de los datos
Definir excepciones concretas al consentimiento informado	Utilizar definiciones comunes y normas globales	Contar con mecanismos de responsabilización más amplios.
Garantizar la calidad, disponibilidad y accesibilidad de los datos	Apoyar las asociaciones multisectoriales	
Reforzar la gobernanza de los datos sanitarios con pruebas	Facilitar la innovación mediante el uso de datos sanitarios	
Establecer procesos y sistemas transparentes y accesibles.	Aplicar la gobernanza de los datos sanitarios a las tecnologías emergentes	
Establecer mecanismos de retroalimentación y de responsabilización	Abordar el uso de datos no sanitarios en contextos sanitarios	

Garantizar la seguridad de los datos	Desarrollar una infraestructura de datos en salud pública	
Exigir fuertes medidas de seguridad técnica para el tratamiento de los datos	Emplear la innovación política	
Atenuar los riesgos relacionados con las amenazas a la seguridad		
Garantizar la transparencia sobre las violaciones de datos		
Contemplar los sistemas de datos federados		

Fuente: Transform Health¹⁴

El primer eje, “**Proteger a las personas**”, tiene como objetivo fundamental establecer que la gobernanza de datos de salud debe asegurar la salvaguardia de individuos, grupos y comunidades contra la posible amenaza de daños o violaciones en el uso de sus datos. Si bien la protección de personas generalmente se contempla en las leyes de protección de datos, los datos de salud, dada su delicadeza, exigen salvaguardias especializadas adicionales tanto en el marco legal como en las prácticas de manejo de datos. La ausencia de protección de datos de salud, ya sean individuales o agregados, podría exponer a riesgos a

individuos, grupos y comunidades. En la gobernanza de datos de salud se deben implementar medidas específicas de protección contra diversos tipos de perjuicios, como explotación, acoso, discriminación, vigilancia con fines comerciales y neocolonialismo basados en datos.

En este sentido, los principios incluidos en este eje se focalizan en la **protección de las personas y las comunidades, la necesidad de crear confianza en los sistemas de datos y garantizar la seguridad de los datos.**

¿EN QUÉ CASOS EL USO INDEBIDO DE LOS DATOS SANITARIOS PUEDE PONER EN RIESGO A LAS PERSONAS Y LAS COMUNIDADES Y POR QUÉ ES NECESARIO PROTEGERLAS?

Acceso no autorizado a los datos	Un empleado de un hospital que accede a los registros médicos de un paciente sin motivo legítimo o sin autorización.
---	--

Venta de información médica	Una clínica que vende la información de salud de sus pacientes a una empresa de marketing sin el conocimiento ni el consentimiento de los pacientes.
Acceso indebido a registros electrónicos	Un hacker que viola la seguridad de un sistema electrónico de registros médicos para acceder y modificar información.
Discriminación basada en los datos personales	Un empleador que utiliza información médica de candidatos para tomar decisiones de contratación, excluyendo a aquellos con condiciones de salud específicas o pertenecientes a alguna comunidad específica.

ALGUNOS EJEMPLOS SOBRE BUENAS PRÁCTICAS QUE RESALTAN LA IMPORTANCIA DE CREAR CONFIANZA EN LOS SISTEMAS DE DATOS

Transparencia en la recopilación y uso de los datos	Un proveedor de servicios de salud que comunica de manera clara y comprensible cómo se recopilan y utilizan los datos de los pacientes y les proporciona información detallada sobre esto.
Consentimiento informado claro y comprensible	Un hospital que implementa un proceso de obtención de consentimiento informado con el que explica de manera detallada los propósitos del tratamiento, la duración del consentimiento, y ofrece opciones claras para que los pacientes ejerzan control sobre su información.
Cumplimiento con normativas y estándares de privacidad de los datos	Una organización de atención médica que se adhiere estrictamente a normativas de privacidad, como la GDPR o normativas locales, y aumenta la confianza al garantizar que se aplican prácticas éticas y legales en el manejo de datos personales.

¿QUÉ MEDIDAS PUEDEN IMPLEMENTARSE PARA GARANTIZAR LA SEGURIDAD DE LOS DATOS?

Implementación de medidas robustas de seguridad y protección de datos	Una institución de salud puede invertir en medidas de seguridad de datos avanzadas, como cifrado, autenticación de dos factores y protocolos de acceso seguro.
--	--

<p>Respuesta efectiva a violaciones de datos</p>	<p>En caso de una violación de datos, una organización de salud debe responder de manera rápida y transparente: informar a los afectados, tomar medidas correctivas y ajustar sus prácticas para evitar futuras violaciones.</p>
<p>Educación sobre seguridad y privacidad</p>	<p>Los proveedores de salud pueden educar a los pacientes sobre la importancia de la privacidad y la seguridad de los datos a través de materiales informativos, capacitación y recursos para empoderar a los individuos en la comprensión de cómo se manejan y protegen sus datos</p>

El segundo eje, “**Promover el valor de la salud**”, pone su foco en que fomentar el valor de los datos de salud implica optimizar su gestión para mejorar la atención médica tanto a nivel individual como a nivel social. Además, dado que los enfoques basados en datos pueden dar lugar a nuevos servicios médicos innovadores, la gobernanza de los datos de salud debe

respaldar y estimular dichas innovaciones. En esta línea, los principios incluidos en este eje se focalizan en tres grandes principios generales: **mejorar los sistemas y servicios sanitarios, promover el intercambio de datos e interoperabilidad, y facilitar la innovación mediante el uso de datos sanitarios.**

¿CÓMO PUEDE LA GOBERNANZA DE DATOS CONTRIBUIR A MEJORAR LOS SISTEMAS Y SERVICIOS SANITARIOS Y CONTRIBUIR A LA CUS?

<p>Análisis de datos para prevenir enfermedades</p>	<p>Si se recopilan datos de diferentes fuentes, como registros médicos, encuestas de salud y factores socioeconómicos, se pueden analizar para identificar patrones y tendencias que puedan prever brotes de enfermedades en comunidades específicas, permitiendo intervenciones preventivas y estrategias de salud pública más eficaces.</p>
<p>Monitorización de desigualdades en la atención médica</p>	<p>Se pueden incorporar indicadores específicos para evaluar desigualdades en el acceso y la calidad de la atención médica. El seguimiento constante de estos indicadores permite identificar disparidades y abordar problemas sistemáticos que afectan a comunidades marginadas, promoviendo la equidad en la atención.</p>
<p>Participación de la comunidad en la toma de decisiones</p>	<p>La gobernanza puede involucrar a la comunidad en la toma de decisiones sobre políticas de salud. Esto asegura que las necesidades y perspectivas de diferentes grupos se consideren, contribuyendo a un enfoque más equitativo en la asignación de recursos y la planificación de servicios</p>

¿CÓMO PUEDE LA GOBERNANZA DE DATOS CONTRIBUIR A MEJORAR LOS SISTEMAS Y SERVICIOS SANITARIOS Y CONTRIBUIR A LA CUS?

Establecer estándares interoperables para compartir datos entre diferentes sistemas de salud y organizaciones mejora la colaboración, reduce errores de comunicación y facilita la transición de pacientes entre diferentes proveedores, mejorando la continuidad de la atención.

¿CÓMO PUEDE LA GESTIÓN DE DATOS SANITARIOS FACILITAR LA INNOVACIÓN?

Una buena gobernanza de datos permite el acceso a grandes conjuntos de datos para el desarrollo de modelos, de manera ética y segura. Esto facilita que los investigadores y desarrolladores de IA puedan utilizar datos variados, representativos de diferentes comunidades para entrenar modelos robustos y precisos. Por ejemplo, se puede elaborar un modelo predictivo para la detección temprana de enfermedades cardiovasculares y servir como apoyo para la toma de decisiones de políticas públicas en salud para poblaciones diversas.

Finalmente, el tercer eje, “**Priorizar la equidad**”, focaliza en el hecho de que el valor derivado del uso de datos debe distribuirse de manera justa para el beneficio tanto de individuos como de comunidades, ya que son ellos quienes contribuyen con sus datos, y

deben tener una participación equitativa en los beneficios sanitarios generados por sus datos. Este eje incluye dos grandes principios generales: **Promover los beneficios equitativos de los datos y Establecer los derechos y la propiedad de los datos.**

¿CÓMO PUEDEN PROMOVERSE LOS BENEFICIOS EQUITATIVOS DE LOS DATOS A PARTIR DE LA GOBERNANZA DE ÉSTOS?

<p>Acceso equitativo a tecnologías de salud</p>	<p>Pueden implementarse políticas que aseguren el acceso equitativo a tecnologías de salud, como telemedicina. Esto es especialmente crucial para comunidades rurales o marginadas que pueden tener dificultades para acceder a la atención médica tradicional.</p>
<p>Adaptabilidad cultural y lingüística</p>	<p>Mediante la promoción de sistemas de información de salud cultural y lingüísticamente sensibles, lo que implica la traducción de materiales y la adaptación de plataformas para que sean accesibles a personas de diferentes orígenes culturales y lingüísticos.</p>
<p>Inclusión de datos socioeconómicos</p>	<p>Integrando datos socioeconómicos en la gobernanza para comprender mejor los determinantes sociales de la salud, lo que permite una intervención más efectiva en problemas como la falta de</p>

	vivienda, el desempleo y otros factores que pueden afectar la salud de manera desproporcionada en ciertos grupos.
Educación y alfabetización en salud	Desarrollando programas de educación y alfabetización en salud que aborden las barreras de comprensión de la información de salud. Esto es crucial para garantizar que todos los individuos, independientemente de su nivel de educación, puedan beneficiarse plenamente de la información de salud disponible.

DIFERENTES MEDIDAS QUE PUEDEN REALIZARSE PARA ESTABLECER LOS DERECHOS DE PROPIEDAD DE LOS DATOS:

Mecanismos de gobernanza participativa de datos	Se pueden implementar mecanismos de toma de decisiones participativos que involucren a la comunidad en las decisiones relacionadas con la recopilación y el uso de datos de salud. Esto podría incluir comités de ética comunitaria o foros de participación ciudadana que permitan la voz activa de los individuos en la formulación de políticas de datos.
Definición clara de funciones y responsabilidades	Se pueden establecer políticas y normativas claras que definan las funciones y responsabilidades de cada entidad involucrada en la gestión de datos de salud. Esto puede incluir roles específicos para los proveedores de atención médica, las instituciones de investigación, las autoridades de salud y los propios individuos, asegurando una división transparente y ética de responsabilidades.
Desarrollo de fideicomisos o cooperativas de datos sanitarios	Pueden crearse fideicomisos o cooperativas de datos sanitarios que actúen como custodios independientes de la información. Estas entidades pueden ser gestionadas por representantes de las comunidades, profesionales de la salud y expertos en ética, cuya su función principal sea salvaguardar los intereses y derechos de los individuos propietarios de los datos.

03. GOBERNANZA DE DATOS EN SALUD E IA EN AMÉRICA LATINA Y EL CARIBE

¿CUÁL ES EL ESCENARIO EN LA REGIÓN?

La gobernanza de los datos sanitarios de las personas, entonces, es uno de los aspectos más importantes a tener en cuenta cuando se desarrollan soluciones de IA y de otras tecnologías innovadoras en este ámbito, **ya que la IA tiene el gran potencial de contribuir a mejorar la salud y el acceso a los servicios sanitarios, pero el tratamiento de los datos personales y datos sensibles de los pacientes requiere medidas, normas y políticas destinadas a brindarles protección y seguridad.**

En este contexto, la región de **ALC se enfrenta a grandes desafíos en torno a la implementación de políticas y medidas respecto de la gobernanza de los datos personales en salud, el desarrollo de estrategias de IA, así como de la seguridad y ciberseguridad de los datos.**

En el año 2020 el Banco Interamericano de Desarrollo (BID) llevó adelante un mapeo de la reglamentación sobre los datos de salud para el uso de Historias Clínicas Electrónicas (HCE), Telemedicina y Estrategias de Salud Digital en América Latina y el Caribe. De acuerdo con este estudio, y respecto de la protección de los datos de las personas y uso secundario de la información sanitaria, así como el rol de los pacientes en relación a sus datos sanitarios y el uso de estándares para uso de HCE e interoperabilidad, los 24 países de la región contemplados en el estudio presentan diferentes grados de desarrollo de normativas. Esta información se encuentra disponible en el Anexo.

Si bien la mayoría de los países cuenta con normativas y políticas públicas que abordan la protección de los datos personales, los derechos de los pacientes, las obligaciones de los sistemas de salud y el acceso a la información pública, **la gran parte de estas normas no aborda exhaustivamente los requerimientos necesarios que trae aparejado el desarrollo de nuevas tecnologías y los grandes caudales de datos y se encuentran desactualizadas.** Se destaca, además, que respecto a los estándares para el uso de HCE e interoperabilidad, el promedio regional de países que han elaborado e implementado normativa o políticas sobre esto es menor al 50%.

Por otra parte, en el año 2023 la Comisión Económica para América Latina y el Caribe (CEPAL), ha elaborado un documento acerca del **estado de los marcos normativos en cuanto a la seguridad cibernética**, que es uno de los aspectos fundamentales a considerar a la hora de pensar la gobernanza y la protección de los datos sanitarios en un contexto de grandes caudales de datos digitalizados.¹⁵

De acuerdo con este informe, **en la región se han registrado avances en el fortalecimiento de los marcos normativos relacionados con la protección de datos y la seguridad cibernética. Sin embargo, no todos los países de América Latina y el Caribe disponen de herramientas regulatorias en estos ámbitos.** Según el Rastreador Global de Legislación Cibernética de la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD), **únicamente 24 de los 33 países de la región cuentan con legislación específica sobre privacidad y protección**

de datos personales. En cuanto a la seguridad de los datos, el Índice de Ciberseguridad Global (ICG) de la Unión Internacional de Telecomunicaciones (UIT) revela **notables disparidades entre los países de la región.** Brasil encabeza la clasificación con 96,6 puntos sobre 100, seguido por México, Uruguay y la República Dominicana, todos con calificaciones superiores a 75. En contraste, algunos países de Centroamérica y el Caribe obtienen puntuaciones por debajo de 15 puntos.

En este sentido, una mayor alineación de los marcos normativos y regulatorios en la región en cuanto a protección de datos y ciberseguridad podría generar beneficios económicos y sociales significativos, desde el aumento de la confianza tanto de inversores nacionales como extranjeros, así como la estimulación de la innovación, la diversificación económica y facilita la escalabilidad. En este contexto, la interoperabilidad está directamente vinculada a las políticas públicas, ya que los países deben promover no solo la compatibilidad técnica y jurídica entre diferentes sistemas, sino también fortalecer la cooperación internacional para facilitar, por ejemplo, la transferencia segura de datos a través de fronteras.

¿Cómo puede la alineación regional de los marcos normativos contribuir a promover la innovación, y a la vez mejorar la protección de datos y la ciberseguridad?

La implementación del **Reglamento General de Protección de Datos (GDPR)** en la UE en 2018 sirvió como un ejemplo de alineación normativa. Esta regulación creó un estándar común para la protección de datos en toda la región, lo que no solo **fortaleció la privacidad de los ciudadanos europeos, sino que también simplificó el entorno regulatorio para las empresas al eliminar la necesidad de cumplir con**

regulaciones diferentes en cada país miembro. Esto condujo a un **aumento en la confianza de los consumidores y facilitó las operaciones comerciales transfronterizas.**

Por otro lado, empresas como Google, Facebook y otras que operan a nivel global deben cumplir con una variedad de regulaciones de privacidad y seguridad en diferentes países. Cuando existen estándares unificados, estas empresas pueden **optimizar sus procesos y recursos**, en lugar de tener que adaptarse a normativas diversas en cada país donde operan. Esto reduce costos operativos y les permite enfocarse más en la innovación y el desarrollo de productos.

En el sector salud, específicamente, esta necesidad de modificación de las estrategias de defensa cibernética por parte de los Estados se torna imperante, ya que es uno de los sectores que más ataques ha recibido, junto con educación e investigación y el sector gubernamental. A modo de ejemplo, caben señalar las experiencias recientes de **Argentina y Colombia, quienes sufrieron graves ataques cibernéticos a sus portales de sus Ministerios de Salud que pusieron en riesgo los datos sanitarios de millones de personas.**^{16,17}

Otro informe elaborado por la CEPAL en 2021 sobre el estado de madurez de la ciberseguridad en Argentina, Brasil, Chile, Colombia, Ecuador, México, Panamá, Perú, República Dominicana y Uruguay establece que, **a pesar de que existe un notable aumento en la concienciación sobre ciberseguridad y es una preocupación relevante en los países analizados, la actividad de actualización normativa y regulatoria es escasa o incluso nula.** Entre esos países analizados, únicamente Colombia exhibe avances sustanciales y concretos al introducir cinco nuevos

decretos nacionales, seguido por Chile y Ecuador quienes realizaron actualizaciones normativas significativas.¹⁸

Diferentes países han avanzado, aunque de manera desigual, en la **regulación de aspectos relacionados con el uso de los datos personales de las personas, los datos sanitarios, la salud digital y la IA**. Como se mencionó en la sección “Gobernanza de datos en salud: ¿por qué importa?”¹⁹, el desarrollo tecnológico produjo una mayor sensibilización respecto de la necesidad de protección de datos personales, las HCE y los derechos de los pacientes, lo que generó, aunque de manera heterogénea entre los países, actualizaciones o nuevas normativas y políticas públicas destinadas a salvaguardar la información de los pacientes y el uso secundario de sus datos; a orientar a los servicios y

sistemas de salud en seguridad informática, así como en la búsqueda de herramientas para el uso de datos que permita innovación, investigación, control de gestión, evaluación y planificación.

Según el Governant AI Readiness Index,²⁰ que se ha desarrollado para evaluar la preparación tecnológica, y a pesar de la inclusión de startups y la inversión en gobierno tecnológico y salud debido a la pandemia de COVID-19, **la preparación gubernamental para la IA entre los países de ALC es desigual, y el sector tecnológico todavía no logra ser competitivo en la región. De los doce países analizados, solo dos tienen una estrategia de IA, cinco están explorando su elaboración, y los demás no tienen una estrategia explícita de inteligencia artificial.**

	Estrategia digital	Estrategia de datos	Estrategia de IA	Infraestructura y conectividad
Argentina	Sí	Sí	Por explorar continuidad	Muy avanzado
Brasil	Sí	Sí	En curso	Muy avanzado
Chile	Sí	Sí	En curso	Líder
Colombia	Sí	Sí	Sí	Muy avanzado
Costa Rica	Sí	Sí	En curso	Muy avanzado
Ecuador	Sí	Sí	No	Semi avanzado
México	Sí	Sí	Por explorar continuidad	Avanzado
Paraguay	Sí	Sí	No	Semi avanzado
Perú	Sí	Sí	No	Avanzado
República Dominicana	Sí	Sí	No	Semi avanzado
Trinidad y Tobago	Sí	No	No	Avanzado
Uruguay	Sí	Sí	Sí	Líder

Fuente: Elaboración propia en base a “La inteligencia artificial al servicio del bien social en América Latina y el Caribe: Panorámica regional e instantáneas de doce países” BID - CMINDS²¹

De los países que han desarrollado una estrategia o plan de políticas a nivel nacional para el uso de la IA o que se encuentran en proceso de hacerlo, se destacan Colombia, Chile, Brasil y Uruguay. En estos casos, además, cabe señalar cuáles son los aspectos que contemplan en torno a la gobernanza de datos.

En el **Plan Nacional de Inteligencia Artificial de Colombia**²², se proponen estrategias específicas para la gobernanza de datos, como la creación de ambientes de prueba ("sandbox") para fomentar la innovación en sectores regulados como Fintech, Healthtech, Agritech y Govtech. También se planea establecer la infraestructura de datos, enfocándose en la explotación de datos públicos y del mercado y se buscará implementar medidas para la gestión responsable de la información, incluyendo la definición de lineamientos para Data Trusts o Data Commons, junto con la regulación necesaria. Este enfoque en la gobernanza de datos es clave para garantizar un desarrollo controlado de la IA, evaluando sus impactos en diversos mercados y contribuyendo al desarrollo sostenible e innovación en el país. Además, se ha creado una Task Force de IA con el objetivo de fortalecer el compromiso y la credibilidad en la construcción de políticas públicas en inteligencia artificial.

Por su parte, **la estrategia de IA en Chile**²³ se centra en la disponibilidad y calidad de los datos, promoviendo un ecosistema de datos abiertos y seguros que respeten los derechos de las personas. Destaca la importancia de la confianza, la representatividad precisa de la realidad, la calidad, la reducción de sesgos, la interoperabilidad y la seguridad de los datos, y se propone la creación de Laboratorios Naturales para desarrollar repositorios de datos de alta calidad. Además, busca actualizar la regulación sobre el uso de datos personales para garantizar la privacidad y prevenir la discriminación arbitraria, siguiendo estándares internacionales como los de GDPR. Para

alcanzar estos objetivos, se propone mantener regulaciones actualizadas, establecer una gobernanza de datos en el Estado, fomentar la colaboración público-privada, incentivar tecnologías de anonimización y seguridad computacional, promover la disponibilidad de datos científicos, y facilitar la creación de comunidades de usuarios.

A su vez, **la Estrategia Brasileña de Inteligencia Artificial (EBIA)**²⁴ prioriza la protección de datos personales, la prevención de discriminación y sesgo algorítmico, y busca un equilibrio para fomentar el desarrollo de la IA con parámetros legales y responsabilidad. Se alinea con la Ley General de Protección de Datos de Brasil y enfatiza en la transparencia y explicabilidad para abordar la discriminación. La EBIA también aboga por establecer parámetros legales para seguridad jurídica y se apoya en iniciativas como e-Digital, Startup Brasil y la propuesta de crear un Centro Nacional de Inteligencia Artificial para promover la colaboración y el tratamiento ético de la IA.

Finalmente, **la Estrategia de IA de Uruguay**²⁵ surge como herramienta para potenciar el gobierno electrónico y tiene como finalidad potenciar las capacidades humanas para mejorar la calidad de vida. Con un enfoque en el interés general, se busca garantizar la inclusión y equidad, reduciendo sesgos no deseados. Se destaca el respeto a los Derechos Humanos, la transparencia en el uso de IA en la Administración Pública, y enfatiza en abordar dilemas éticos humanamente. Además, dispone la importancia de la privacidad por diseño, y exige cumplir con principios básicos de seguridad de la información según la normativa vigente en Uruguay.

A nivel regional, además, existen iniciativas en esta línea, como **fAIr LAC, la Alianza por la Ética, Equidad y Transparencia en Inteligencia Artificial en América**

Latina y el Caribe, que tiene como objetivo principal promover un uso ético de la IA en la región. Para lograrlo, se ha diseñado una estrategia basada en **tres dimensiones**. La primera involucra la **creación de una red diversa de expertos en IA que asesoren el desarrollo de políticas y líneas de acción**. La segunda dimensión se centra en la **formación de capacidades**, buscando que los responsables de políticas, ciudadanos y empresas comprendan los desafíos y posibilidades de la IA. Por último, la tercera

dimensión promueve la **calidad y la mitigación de riesgos**, a través de guías, autorregulación, estándares de calidad y marcos regulatorios. Estas estrategias se buscan implementarse tanto a nivel regional como territorial, con hubs locales que actúen como referentes para promover una IA ética y equitativa en sus áreas geográficas. La retroalimentación y el aprendizaje entre la iniciativa regional y las centrales territoriales serán fundamentales para producir conocimientos y mejores prácticas en toda la región.²⁶

¿QUÉ ASPECTOS DE LA GOBERNANZA DE DATOS DEBEN CONSIDERARSE EN CADA ETAPA DEL CICLO DE VIDA DE LOS DATOS SANITARIOS EN EL DESARROLLO DE SOLUCIONES DE IA?

ETAPA DE GENERACIÓN Y CAPTURA DE DATOS SANITARIOS	ETAPA DE ALMACENAMIENTO DE DATOS SANITARIOS	FASE DE ACCESO Y COMPARTICIÓN DE DATOS	FASE DE ELIMINACIÓN DE DATOS
<p>La IA requiere datos de alta calidad, precisos y completos para su entrenamiento. Estos datos se obtienen de la práctica clínica: registros clínicos electrónicos, datos de laboratorio, exámenes complementarios como radiografías o resonancias magnéticas, datos epidemiológicos como los que provienen de los sistemas de vigilancia, censos, encuestas de salud y los registros de seguros médicos, administrativos, de farmacias, entre otros.</p> <p>La gobernanza de datos permite establecer los estándares sobre los cuales debe basarse la recopilación y el registro de datos íntegros y de calidad, a partir de fuentes tan diversas.</p>	<p>La IA necesita acceso eficiente a grandes conjuntos de datos, lo que requiere la gestión adecuada de bases de datos y sistemas de almacenamiento seguros y confiables.</p> <p>La gobernanza de datos debe contribuir a establecer políticas de seguridad y privacidad para proteger la información sensible y garantizar la confidencialidad y los derechos de las personas.</p>	<p>Se deben establecer protocolos para la interoperabilidad y la privacidad, permitiendo que los datos se compartan de manera segura y que los pacientes otorguen su consentimiento informado.</p>	<p>Se deben establecer procedimientos de eliminación segura y se debe regular la retención de los datos.</p>

La gobernanza de datos sanitarios desempeña así un papel central para el desarrollo de soluciones de IA en salud, ya que no solo se requiere una cantidad adecuada de datos, sino también **que estos datos sean de alta calidad, representativos de las diferentes comunidades que forman parte de una sociedad, y que estén disponibles de forma segura e interoperable.** Además, se evidencia una marcada necesidad en toda la región de intensificar los esfuerzos para respaldar a las instituciones tanto públicas como privadas mediante regulaciones y políticas actualizadas y pertinentes que favorezcan la innovación y protejan a las personas.

¿CUÁLES SON LOS PRINCIPALES DESAFÍOS?

Las secciones precedentes dejan abiertos interrogantes, pero también una certeza: los desafíos que presenta ALC en cuanto a gobernanza de datos y fomento de la innovación y el desarrollo en IA son numerosos.

Además de un análisis bibliográfico de fuentes secundarias, diversos expertos fueron entrevistados para la elaboración de este documento para **profundizar en los desafíos y necesidades en gobernanza de datos frente a los desarrollos de IA, las buenas prácticas vigentes, los pasos a seguir y cómo los Principios de Gobernanza de Datos en Salud pueden contribuir a afrontar estos desafíos.** También se realizó un webinar con expertos regionales en estas áreas, con quienes se conversó también sobre estas temáticas. **Se buscó contar con la opinión de personas pertenecientes a diversos ámbitos y países de la región: especialistas en apertura de datos, en investigación y desarrollo de soluciones de IA en salud, en derecho de la salud e IA y en salud digital.**

Este proceso de análisis de información e interacción con expertos permitió **consolidar los principales desafíos y necesidades identificados, que pueden agruparse en regulatorios, de calidad de los datos, de capacidades estatales, de infraestructura, y de articulación entre actores.**

REGULATORIOS

Uno de los principales desafíos que encuentra la región de ALC es que el **desarrollo normativo y regulatorio que sirve de marco para la innovación tecnológica en salud es deficiente, y la velocidad en la generación de los datos y la IA va más rápido que la estructura de los Estados para hacer frente a esto.** Como se analizó en secciones anteriores, actualmente las regulaciones sobre datos personales en la amplia mayoría de los países de la región lo hacen en términos generales y no incluyen una perspectiva específica sobre los datos en salud, lo que favorece un estado de fragilidad de estos datos. Esto se traduce, además en baja capacidad de fiscalización a través de estructuras de control y gobernanza de estas tecnologías, y en potenciales riesgos de discriminación especialmente en aquellas comunidades más marginadas.

Por este motivo es fundamental que los Estados avancen en la elaboración de marcos regulatorios claros, actualizados y confiables, que tengan en cuenta el contexto y las necesidades regionales y locales, y que promuevan la innovación y el desarrollo buscando el equilibrio entre el acceso a la información, junto con la protección y la privacidad de las personas.

CALIDAD DE LOS DATOS

Otro de los grandes desafíos que enfrenta la región de ALC para el desarrollo de soluciones de IA es la **baja calidad de los datos disponibles. Esto supone,**

además, **problemas para una correcta gobernanza de los datos utilizados.**

De acuerdo con la opinión de diferentes expertos, en ALC **los repositorios de datos son escasos y poco representativos de las poblaciones diversas que habitan la región.** En muchos casos, los desarrollos de IA se basan en algoritmos “importados” generados con perfiles en general provenientes de países de Europa o Norteamérica, que no reflejan el contexto y la diversidad presente en los países latinoamericanos. Además, **las bases públicas con las que cuentan los países de la región suelen estar desactualizadas,** con anotaciones o imágenes de baja calidad, lo que introduce nuevos sesgos y no garantiza que la información sea completa y veraz.

Otro de los desafíos relacionados con la calidad de los datos en la región es la **falta de capacitación de aquellas personas que se encargan de la recolección, etiquetado o cualquier instancia del uso de los datos.** Por ese motivo, **resulta fundamental que quienes trabajan con bases de datos,** incluidos los profesionales de la salud, reciban educación al respecto.

Estos desafíos también muestran una necesidad imperante: **es esencial que las herramientas de IA en salud incorporen desde sus etapas iniciales y a lo largo de todo su desarrollo e implementación, buenas prácticas y una perspectiva ética,** para garantizar que el uso de los datos en la IA beneficie a los seres humanos, promueva la salud y evite acciones perjudiciales, discriminación o injusticia²⁷.

INFRAESTRUCTURA

La región de ALC enfrenta además **desafíos relacionados a la infraestructura para el acceso a los datos.** La promoción de la innovación no puede

hacerse de manera responsable si no están dadas las condiciones en términos de infraestructura que garanticen **no sólo el acceso a internet, energía eléctrica o espacio en la nube (cosas que no siempre están garantizadas), sino también garantías sobre la seguridad de los datos.** En este sentido, **la ciberseguridad es uno de los puntos críticos a considerar.** Es necesario que se tomen medidas desde la gobernanza contra el cibercrimen, ya que el sector salud ha sido uno de los sectores más atacados.

Es importante señalar que estos aspectos, si bien son fundamentales, no son exclusivos para el sector salud. **La búsqueda de soluciones para estos problemas debe ser multidisciplinaria, integral, holística y debe incorporar experiencias exitosas de otros sectores que ya hayan avanzado en este camino.**

CAPACIDADES DE LOS ESTADOS

Otro de los desafíos centrales en la región son **las capacidades que tienen los Estados para efectivamente garantizar la protección de los derechos de las personas y a la vez promover la innovación en IA.**

Actualmente, los Estados de la región cuentan en gran medida con **bajas capacidades para la implementación y control de políticas de este tipo,** ya que se requieren burocracias y agencias especializadas en el uso de datos y en la **gran mayoría de los casos no se cuenta con los perfiles y/o los organismos gubernamentales necesarios.** En este sentido, resulta fundamental, por un lado, **promover la existencia de agencias especializadas en uso y protección de datos, privacidad y acceso a la información, y que estas agencias cuenten con expertos en datos en salud.**

Esto, además, se traduce en la falta de lineamientos claros sobre el camino que deben seguir los desarrolladores de aplicaciones y soluciones de IA en salud: a qué instituciones gubernamentales deben recurrir, cuáles son las agencias regulatorias involucradas y cuáles son los requerimientos que deben presentar. **La unificación de criterios, a través de lineamientos, manuales o guías de buenas prácticas que incluyan aspectos éticos, pueden marcar el camino para avanzar en la innovación a la vez que se garantice que los datos se encuentren seguros.**

Como se mencionó previamente, pocos países de América Latina cuentan con planes nacionales de salud digital e IA, y es necesaria la **promoción de estas estrategias, que incluyan financiamiento, educación, estimulación de ecosistemas e inversión.** Esto supone, además, la necesidad de que la discusión sobre la implementación de la IA en salud incluya la definición de las prioridades que tienen los sistemas de salud desde una mirada estratégica y ordenada. En este sentido es importante **considerar la estructura organizativa interna de los Estados.** Los países federales y los no federales poseen diferentes capacidades de acción por sus propias características de centralización o descentralización. En países federales, como Argentina, Brasil o México, esto también debe abordarse a nivel subnacional.

ARTICULACIÓN DE ACTORES

Una mejor gobernanza de datos en el contexto de la IA

requiere, además, la **articulación de los diferentes actores involucrados en los procesos.** Actualmente, y a pesar de las iniciativas regionales mencionadas en las secciones previas, **los países de ALC pueden avanzar hacia una mayor coordinación entre ellos a la hora de definir parámetros comunes para el uso y el intercambio de datos.** También a nivel local y regional debe **fomentarse la participación de los desarrolladores, las start ups, la academia y los gobiernos en la creación y el diseño de los ecosistemas.** Se trata, entonces, de que la **búsqueda de soluciones para los problemas nacionales cuente con la mayor cantidad de actores interpelados.**

Asimismo, es necesario **estimular la participación y la cultura digital en los ciudadanos** para hacerlos parte de las discusiones sobre el uso de datos, empoderarlos con información para una mayor concientización sobre sus derechos, obligaciones y responsabilidades sobre éstos. En este sentido, mayor educación digital y conciencia sobre el valor de los datos digitales resulta fundamental.

¿QUÉ RECOMENDAMOS?

De los desafíos presentados y **sobre la base de los Principios de Gobernanza de Datos en Salud** analizados pueden realizarse **recomendaciones para que los países de ALC avancen hacia la búsqueda de soluciones de IA que protejan a las personas, prioricen la equidad y promuevan la salud.**

<p>Regulatorias</p>	<ul style="list-style-type: none"> ○ Generar marcos regulatorios amplios, claros, actualizados y confiables sobre gobernanza de datos que garanticen tanto la protección de datos como la promoción de la innovación. Estos marcos deberían incluir cuestiones específicas para el abordaje y uso seguro de los datos sanitarios. ○ Las normativas deben prever la protección de los datos frente a la agregación de éstos para armados de perfiles poblacionales. ○ Incorporar la gobernanza de datos en salud en los diferentes niveles del sistema de salud: gobierno, pero también hospitales, centros de atención, universidades y cualquier entidad vinculada.
<p>Calidad de los datos</p>	<ul style="list-style-type: none"> ○ Fomentar la recolección y utilización de datos locales, que se correspondan con el contexto de los países de la región y a los perfiles demográficos y epidemiológicos para generar soluciones de mejor calidad, más representativas de las poblaciones locales. ○ Procurar la reducción y control de sesgos durante todo el desarrollo de los proyectos de IA ○ Incentivar la generación de bases de datos públicas actualizadas y con datos completos y de calidad ○ Capacitar a las personas encargadas de trabajar con datos en cualquiera las fases del ciclo del dato para garantizar que se preserve la calidad de los datos. ○ Incorporar en las currículas educativas de los profesionales de la salud en formación elementos de uso y manejo de datos.
<p>Éticas</p>	<ul style="list-style-type: none"> ○ Abordar las cuestiones éticas desde las etapas iniciales del diseño del proyecto hasta la implementación y el seguimiento. ○ Participación de expertos en ética y otras disciplinas desde el comienzo de los proyectos para mitigar los sesgos. ○ Procurar la anonimización de los datos sanitarios, el alojamiento de los datos en sitios seguros, así como su archivo temporal y compartimentado. ○ Recolectar datos para responder una pregunta de investigación, es decir, con un fin específico.
<p>Infraestructura</p>	<ul style="list-style-type: none"> ○ Fomentar la inversión propia y extranjera para infraestructura digital ○ Diseñar planes integrales de ciberseguridad que incluyan expertos de diferentes disciplinas para conseguir tener una mirada integral, incluyendo al sector salud.

Capacidades de los Estados	<ul style="list-style-type: none">○ Promover la existencia de agencias especializadas en uso y protección de datos, privacidad, acceso a la información, y que estas agencias cuenten con expertos en datos en salud.○ Incentivar la formación de una burocracia estatal especializada en el uso de datos y uso de datos en salud.○ Elaborar manuales, lineamientos o guías de buenas prácticas para que los desarrolladores de aplicaciones de IA en salud conozcan el recorrido gubernamental que deben seguir para desarrollar una solución de IA en salud.○ Promover el diseño e implementación de Estrategias Nacionales de Salud Digital para fomentar la innovación y articular la gobernanza de datos desde objetivos claros.○ En países federales o con mayores niveles de descentralización, se debe contemplar la adecuación de la gobernanza de datos a los niveles subnacionales.
Articulación de actores	<ul style="list-style-type: none">○ Promover la articulación entre los Estados nacionales y organismos regionales e internacionales para avanzar hacia objetivos comunes.○ Fomentar la participación de diferentes actores: desarrolladores, start ups, academia, ciudadanos y otros, para acompañar a los gobiernos en la creación de los ecosistemas.○ Estimular la participación y la educación digital en los ciudadanos para hacerlos para una mayor concientización sobre sus derechos, obligaciones y responsabilidades sobre el uso de sus datos.

04. CONCLUSIONES

El desarrollo de la IA y de otras tecnologías innovadoras presentan un enorme potencial para mejorar la salud de las personas en ALC. Pero este desarrollo no puede llevarse adelante sin una política de gobernanza de los datos sanitarios.

La región presenta numerosos desafíos para garantizar la protección de los datos de salud de las personas y la seguridad en todas las instancias del proceso de tratamiento de sus datos. La falta de marcos regulatorios adecuados y de estrategias claras y coordinadas para el desarrollo de la IA entre los países de la región, así como la baja calidad de los datos disponibles y un déficit en la concientización sobre la importancia del uso responsable de los datos, suponen riesgos pero también grandes oportunidades para que las respuestas a estos desafíos sean elaboradas de manera integral, coordinada y con base en la protección de las personas, sus derechos y la promoción de los derechos humanos.

Los avances tecnológicos se mueven más rápido que la capacidad de los Estados para dar respuestas inmediatas, y por ese motivo **las instituciones deben ser dinámicas y resilientes, generando marcos**

regulatorios amplios que permitan a todas las partes interesadas adaptarse de manera más eficaz a los cambios exponenciales y tomar decisiones informadas para garantizar que la IA beneficie a la sociedad en su conjunto, se proteja y se respeten los principios éticos, la privacidad y la equidad en la atención médica. En este sentido, la creación de bienes públicos digitales y la representación adecuada de las poblaciones son fundamentales para garantizar la promoción de la equidad y la protección de las personas, y la conectividad universal es crucial para evitar subrepresentaciones y soluciones sesgadas que profundicen brechas existentes, fomenten la discriminación y vulneren los derechos de las personas.

Los Principios de Gobernanza de Datos en Salud, por lo tanto, resultan una valiosa herramienta para abordar de manera integral los desafíos normativos, operativos y de política pública, de manera que se genere un ecosistema óptimo para la innovación en IA en salud, sin perder de vista el respeto a los derechos humanos, la seguridad de las personas y la promoción de la equidad en los sistemas sanitarios.

05. AGRADECIMIENTOS

Se agradece por haber contribuido con su conocimiento a la elaboración de este documento a Félix Rígoli (FIOCRUZ), Fernando Aith (Universidad de San Pablo), Mercedes de los Santos (Open Data Charter), Renato Berrino Malaccorto (Open Data Charter), Laura Alonso Alemany (Universidad Nacional de Córdoba), Daniel Otzoy (RECAINSA), Mauricio Farez (ENTELAI), Marcelo D'Agostino (OPS/PAHO), María Cristina Pombo (BID) y May Chomali (CENS).

06. BIBLIOGRAFÍA

1. Alegsa L. Definición de Petabyte. Alegsa.com.ar. Published 18 de junio de 2023. Accedido noviembre 30, 2023. <https://www.alegsa.com.ar/Dic/petabyte.php>
2. Cabello S. Análisis de los modelos de gobernanza de datos en el sector público: Una mirada desde Bogotá, Buenos Aires, Ciudad de México y São Paulo. documentos de Proyectos (LC/TS2023/71), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL). Published online 2023. <https://repositorio.cepal.org/server/api/core/bitstreams/9e5b987c-9168-4f88-9503-ca05c6d353ce/content>
3. Eastwood B. How to Navigate Structured and Unstructured Data as a Healthcare Organization. Publisher. Published 8 de mayo de 2023. Accedido noviembre 30, 2023. <https://healthtechmagazine.net/article/2023/05/structured-vs-unstructured-data-in-healthcare-perfcon>
4. García Zaballos A, Iglesias Rodriguez E, Puig Gabarró P. Informe anual del Índice de Desarrollo de la Banda Ancha: IDBA 2020: Brecha digital en América Latina y el Caribe. Inter-American Development Bank; 2021. doi:10.18235/0003337
5. Closing The Digital Gap (CTDG). Closing The Digital Gap (CTDG). Accedido noviembre 30, 2023. <https://closingthedigitalgap.org/>
6. United Nations. Sustainable Development Goals. un.org. Published 22 de agosto de 2018. Accedido noviembre 30, 2023. <https://www.un.org/sustainabledevelopment/es/sustainable-development-goals/>
7. Organización Panamericana de la Salud. Ocho principios rectores de la transformación digital del sector de la salud. Un llamado a la acción panamericana. Published online 2021. https://iris.paho.org/bitstream/handle/10665.2/53730/OPSEIHIS210004_spa.pdf?sequence=1&isAllowed=y
8. UNESCO. Ética de la inteligencia artificial. UNESCO. Published 13 de septiembre de 2023. Accedido noviembre 30, 2023. <https://www.unesco.org/es/artificial-intelligence/recommendation-ethics>
9. OECD. OECD AI Principles overview. OECD. Accedido noviembre 30, 2023. <https://oecd.ai/en/ai-principles>

10. World Health Organization. WHO outlines considerations for regulation of artificial intelligence for health. World Health Organization. Accedido noviembre 30, 2023.
<https://www.who.int/news/item/19-10-2023-who-outlines-considerations-for-regulation-of-artificial-intelligence-for-health>
11. Filmus D, Schapachnik F. Inteligencia Artificial: el debate principal es cómo se regula y democratiza. Argentina.gob.ar. Published 2 de agosto de 2023. Accedido noviembre 30, 2023.
<https://www.argentina.gob.ar/noticias/inteligencia-artificial-el-debate-principal-es-como-se-regula-y-democratiza>
12. PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO: relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Diario Oficial de la Unión Europea. <https://www.boe.es/doue/2016/119/L00001-00088.pdf>
13. RED IBEROAMERICANA DE PROTECCIÓN DE DATOS. ESTÁNDARES DE PROTECCIÓN DE DATOS PERSONALES PARA LOS ESTADOS IBEROAMERICANOS. Red Iberoamericana de Protección de Datos. Published online 20-JUNIO-2017.
https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf
14. Transform Health. Principios de Gobernanza de Datos de Salud. Health Data Principles. Accedido noviembre 30, 2023. <https://healthdatapinciples.org/sp/about>
15. Mariano Díaz R, Núñez Reyes G. Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe. Published online 23 de agosto de 2023. Accedido noviembre 30, 2023. <https://hdl.handle.net/11362/49086>
16. Brodersen J. Tras el hackeo al PAMI, ciberdelincuentes publican información robada: hay historias clínicas, estudios y datos personales. clarin.com. Published 19 de agosto de 2023. Accedido noviembre 30, 2023. https://www.clarin.com/tecnologia/hackeo-pami-ciberdelincuentes-publican-informacion-robada-historias-clinicas-estudios-datos-personales_0_oVEAPipTS0.html
17. Ownby J. Hackeo masivo en Colombia: “La información de millones de personas está en manos de delincuentes en este momento”. El País. Published 14 de septiembre de 2023. Accedido noviembre 30, 2023. <https://elpais.com/america-colombia/2023-09-14/hackeo-masivo-en-colombia-la-informacion-de-millones-de-personas-esta-en-manos-de-delincuentes-en-este-momento.html>

18. Díaz RM. Estado de la ciberseguridad en la logística de América Latina y el Caribe. Accedido noviembre 30, 2023. <https://repositorio.cepal.org/server/api/core/bitstreams/4b04fcfe-c0f3-4c97-af14-2c234857f433/content>
19. Carnicero J, Serra P. Gobernanza de La Salud Digital: El Arte de La Transformación de Los Sistemas de Salud. Inter-American Development Bank; 2020. doi:10.18235/0002661
20. Broadband Commission. Reimagining Global Health through Artificial Intelligence: The Roadmap to AI Maturity.
21. Gómez Mont C, Del Pozo CM, Martínez Pinto C, Martín del Campo Alcocer AV. La inteligencia artificial al servicio del bien social en América Latina y el Caribe: Panorámica regional e instantáneas de doce países. Inter-American Development Bank; 2020. doi:10.18235/0002393
22. Administrative Department of the Presidency of the Republic (DAPRE). Artificial Intelligence Task Force. Presidency of the Republic of Colombia. Accedido noviembre 30, 2023. <https://inteligenciaartificial.gov.co/en/>
23. Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, Gobierno de Chile. POLÍTICA NACIONAL DE INTELIGENCIA ARTIFICIAL.
24. Cordeiro M. Brasil publica estrategia de Inteligencia Artificial. Accedido noviembre 30, 2023. <https://dplnews.com/brasil-publica-su-estrategia-de-inteligencia-artificial/>
25. Estrategia de Inteligencia Artificial. Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. Accedido diciembre 5, 2023. <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-inteligencia-artificial>
26. Quiénes somos. fairlac.iadb.org. Accedido noviembre 30, 2023. <https://fairlac.iadb.org/quienes-somos>
27. Tecnico D. Inteligencia Artificial (IA) Responsable: Claves para aplicar los principios éticos en las soluciones de IA en el campo de la salud. Accedido noviembre 30, 2023. https://clias.iecs.org.ar/wp-content/uploads/2023/11/DT3_CLIAS.pdf
28. Bagolle A, Park M, Marti M. Dashboard - Regulatory Frameworks for Digital Health in Latin American and the Caribbean: Electronic Health Records: Progresses and Next Steps. Dashboard - Social Digital. Accedido noviembre 30, 2023. <https://socialdigital.iadb.org/en/sph/dashboard>

07. ANEXO

Reglamentaciones sobre uso de los datos en salud en América Latina y Caribe.

	Protección de datos personales y uso secundario de la información sanitaria				Rol de los pacientes en relación a sus datos sanitarios				Estándares para HCE e interoperabilidad	
	Protección de datos personales	Intercambio de información a nivel nacional	Seguridad en el almacenamiento de los datos sanitarios	Uso secundario de información sanitaria	Consentimiento para el uso de sus datos en salud	Identificación y autenticación de pacientes	Derechos de los pacientes a editar su información	Acceso de los pacientes a sus datos sanitarios	Interoperabilidad y estándares	Códigos y normas para la salud
Argentina	Ley 25326 de Protección de datos personales	Ley 26529 de Derechos del paciente Ley 25326 de Protección de datos personales	Ley 26529 de Derechos del paciente Ley 25326 de Protección de datos personales	Ley 25326 de Protección de datos personales	Ley 26529 de Derechos del paciente Ley 25326 de Protección de datos personales	Ley 26529 de Derechos del paciente	Ley 26529 de Derechos del paciente	Ley 26529 de Derechos del paciente	Resolución 680/2018 Resolución 115/2019	Resolución 680/2018
Bahamas	Acta de protección de datos (privacidad de la información personal)	Acta de protección de datos (privacidad de la información personal)	Acta de protección de datos (privacidad de la información personal)	Acta de protección de datos (privacidad de la información personal)	Acta de protección de datos (privacidad de la información personal)	Acta de protección de datos (privacidad de la información personal)	Acta de protección de datos (privacidad de la información personal)	Acta de protección de datos (privacidad de la información personal)	Sin datos	Sin datos
Barbados	Ley de Protección de Datos	Ley de Protección de Datos	Ley de Protección de Datos	Ley de Protección de Datos	Ley de Protección de Datos	Ley de Protección de Datos	Ley de Protección de Datos	Ley de Protección de Datos	Sin datos	Sin datos
Bélica	Plan Estratégico del Sector Salud 2014-2024 Ley de Libertad de información	Plan Estratégico del Sector Salud 2014-2024	Sin datos	Sin datos	Sin datos	Sin datos	Sin datos	Sin datos	Sin datos	Sin datos
Bolivia	Decreto Supremo 1793 que reglamenta Ley 164	Sin datos	Decreto Supremo 1793 que reglamenta Ley 164	Decreto Supremo 1793 que reglamenta Ley 164	Ley 164 para el Desarrollo de Tecnologías de Información y Comunicación	Sin datos	Ley 164 para el Desarrollo de Tecnologías de Información y Comunicación	Ley 164 para el Desarrollo de Tecnologías de Información y Comunicación	Sin datos	Sin datos
Brasil	Ley 13709	Directiva 2073 Ley 13709	Ley 13709 Ley 13787	Ley 13709	Ley 13709	Ley 13709	Ley 13709	Ley 13709	Directiva 2073	Directiva 2073
Chile	Ley 19628 Decreto con Fuerza de Ley 1	Ley 19628 Decreto con Fuerza de Ley 1	Ley 19799 Decreto Supremo 83 Decreto 41	Ley 19628	Ley 20584 Ley 19628	Decreto 41 Decreto 643	Ley 19628	Decreto 41	Decreto 643	Decreto 643
Colombia	Ley 1581 Ley 2015 Res. 839/17 Decreto 1377/13	Ley 2015	Ley 1995 Ley 1413 Ley 1581 Ley 2015	Ley 1581	Ley 1581 Decreto 1377/13	Regulación N°12 de 2013 del Ministerio de Salud	Ley 1581 Decreto 1377/1	Ley 1581 Decreto 1377/1	Ley 2015	Sin datos
Costa Rica	Ley 9162 Regulaciones de la Historia Clínica Digital Unificada	Ley 9162	Ley 9162 Regulaciones de la Historia Clínica Digital Unificada Ley 8968	Ley 8968	Sesión 7366-1999 Ley 8968	Ley 9162	Ley 8968	Ley 8968 Ley 8239	Regulación 39652-S-MICIT	Regulación 39652-S-MICIT
Ecuador	Regulación 00005216-A	Regulación 00005216-A	Regulación 00005216-A	Regulación 00005216-A	Constitución Nacional Regulación 00005216-A	Regulación 0009-2017	Sin datos	Regulación 0009-2017	Regulación 0009-2017 Regulación 00001190	Regulación 0009-2017 Regulación 00001190

DESAFÍOS Y RECOMENDACIONES EN LA GOBERNANZA DE DATOS PARA EL DESARROLLO DE LA INTELIGENCIA ARTIFICIAL EN SALUD EN AMÉRICA LATINA Y EL CARIBE

El Salvador	Resolución 941 Decreto307	Resolución 941	Resolución 941 Decreto 133	Decreto 307	Resolución 941	Resolución 941	Resolución 941	Resolución 941	Sin datos	Sin datos
Guatemala	Decreto 57-2008	Sin datos	Sin datos	Decreto 57-2008	Decreto 57-2008	Sin datos	Decreto 57-2008	Decreto 57-2008	Sin datos	Sin datos
Guyana	Acta 21 de acceso a la información	Acta 21 de acceso a la información	Sin datos	Sin datos	Acta 21 de acceso a la información	Sin datos	Acta 21 de acceso a la información	Acta 21 de acceso a la información	Sin datos	Sin datos
Haití	Sin datos	Sin datos	Sin datos	Sin datos	Sin datos	Sin datos	Sin datos	Sin datos	Sin datos	Sin datos
Honduras	Decreto170-2006	Sin datos	Sin datos	Regulación 65-91	Decreto 170-2006	Sin datos	Decreto 170-2006	Decreto 170-2006	Sin datos	Sin datos
Jamaica	Acta 2020 de protección de datos	Acta 2020 de protección de datos	Acta 2020 de protección de datos	Acta 2020 de protección de datos	Acta 2020 de protección de datos	Acta 2020 de protección de datos	Acta 2020 de protección de datos	Acta 2020 de protección de datos Acta de acceso a la información	Sin datos	Sin datos
México	Ley DOF 05-07-2010	NOM-024-SSA3-2010	NOM-024-SSA3-2010	NOM-024-SSA3-2010	DOF 11-01-2012	NOM-024-SSA3-2010	DOF 11-01-2012	DOF 11-01-2012	NOM-024-SSA3-2010	NOM-024-SSA3-2010 NOM-024-SSA3-2012
Nicaragua	Regulaciones de la Ley 787 Ley 423	Regulaciones de la Ley 787	Regulaciones de la Ley 787	Regulaciones de la Ley 787	Regulaciones de la Ley 787	Sin datos	Regulaciones de la Ley 787	Regulaciones de la Ley 787	Sin datos	Sin datos
Paraguay	Ley 1682	Sin datos	Sin datos	Ley 1682	Ley 1682	Sin datos	Sin datos	Ley 1682	Sin datos	Sin datos
Perú	Ley 29733	Ley 30024 Decreto Supremo 009-2017-SA	Ley 30024 Decreto Supremo 009-2017-SA	Ley 30024 Decreto Supremo 009-2017-SA	Ley 29414 Ley 26842	Decreto Supremo 024-2005-SA Decreto Supremo 009-2017-SA	Ley 30024	Ley 30024 Ley 29414 Ley 26842	Ley 30024 Decreto Supremo 009-2017-SA Resolución ministerial 1104-2018/MINSA	Resolución ministerial 469-2019/MINSA
República Dominicana	Ley 172-13	Ley 172-13	Ley 172-13	Ley 172-13	Ley 172-13	Ley 172-13	Ley 172-13	Ley 172-13	Sin datos	Sin datos
Suriname	Sin datos	Sin datos	Sin datos	Sin datos	Sin datos	Sin datos	Sin datos	Sin datos	Sin datos	Sin datos
Uruguay	Ley 1831 Decreto 242/017	Ley 19355 Decreto 242/017	Decreto 242/017	Decreto 242/017	Ley 18335 Ley 18331	Decreto 242/017	Decreto 242/017Ley 18331	Decreto 242/017	Decreto 242/017	Decreto 242/017
Venezuela	Acta de Telesalud Decreto 9051	Acta de Telesalud Decreto 9051	Acta de Telesalud	Decreto 9051	Decreto 9051	Sin datos	Decreto 9051	Sin datos	Acta de Telesalud Decreto 9051	Sin datos
Promedio regional LAC (%)	88.46%	72.92%	73.07%	84.61%	88.46%	61.53%	73.07%	84.61%	42.3%	30.76%

Fuente: elaboración propia a partir del MAPA BID²⁸