fAIr LAC
Jalisco

Recomendación de lineamientos regulatorios para datos públicos y de la industria para el entrenamiento de Inteligencia Artificial

Análisis de mecanismos para la gobernanza de datos para casos de uso de la iniciativa fAIr LAC Jalisco

BID | BID LAB | Tecnológico de Monterrey Escuela de Ingeniería y Ciencias | C MINDS | Jalisco

fAIr LAC

Mayo 2023

Autores: Carla Vázquez Wallach, Constanza Gómez Mont, Cristian Guerrero, José Roberto Mejía, Lucía Tróchez Ardila, C Minds

Agradecimientos por sus contribuciones a: Cristina Martinez Pinto y Juan Manuel Sandoval de la Hoya C Minds; Erica Almaráz, Mayra Fernández y Yunive Moreno, Gobierno de Jalisco; Enrique Cortés, Director del Hub de IA del Tec de Monterrey; Juan Roberto Hernández, Tatiana Lefno, Unidad Ejecutora fAIr LAC Jalisco, Gaspar González Briseño, Coordinador del caso de uso de retinopatía diabética en fAIr LAC Jalisco; Jorge Miramontes, Juan Alberto Amezquita y Luis Enrique Vázquez del Comité de Riesgos Éticos y Gobernanza de Datos de fAIr LAC Jalisco.

Contenidos

Introducción

fAIr LAC[1] es una alianza regional, liderada por el Banco Interamericano de Desarrollo (BID) en América Latina y el Caribe para incidir tanto en la política pública como en el ecosistema emprendedor en la promoción del uso responsable y ético de la inteligencia artificial (IA). Está conformada por una red diversa de profesionales y expertos, desde la academia, el gobierno, la sociedad civil, la industria y el sector emprendedor.

El hub local en Jalisco de la iniciativa fAIr LAC es liderado por el BID, el Tecnológico de Monterrey en Guadalajara, el Gobierno de Jalisco y C Minds. Este hub busca impulsar el desarrollo del ecosistema de inteligencia artificial en el estado y promover la adopción y el uso ético y responsable de la IA en la región a través de la articulación multisectorial.

En Jalisco, las actividades giran en torno a tres componentes complementarios:

1. IA para el bien social desde el sector público;
2. IA para el bien social desde el sector de emprendimiento;
3. Desarrollo del modelo fAIr LAC y de capacidades para funcionarios públicos, academia y otros actores clave.

Como parte principal del primer componente se encuentran actividades enfocadas en diseñar e implementar casos de uso para probar métodos y proyectos piloto para el aprovechamiento de la IA en la resolución de problemáticas sociales.

Dentro del mismo, se han identificado distintas necesidades de los casos de uso, incluyendo la definición de un modelo de gobernanza de datos involucrando a todas las organizaciones, con el objetivo de dar solución a uno o varios problemas a través de herramientas tecnológicas que dependen de datos (de cualquier naturaleza: personales, sensibles, geográficos, biométricos, etc.) y recursos humanos de índole público.

Para ello, el presente documento presenta un análisis y recomendaciones de lineamientos regulatorios que pueden implementarse para lograr gobernanza de datos en el contexto de una solución público-privada. Este documento va más allá de una tecnología o caso de uso específico y busca ser agnóstico a las particularidades de los casos de uso, sin dejar de lado las necesidades específicas de los mismos.

En una primera parte, se busca analizar y emitir recomendaciones en torno al despliegue de la gobernanza en aspectos operativos, contextualizando el estado del arte en temas de gobernanza y las condiciones particulares de la iniciativa en Jalisco. En la segunda parte se analiza y recomienda en torno a temas legales y regulatorios, tomando en cuenta el marco legal actual, así como las tendencias y mejores prácticas regionales e internacionales. Finalmente, en un documento independiente y complementario, se ofrecen lineamientos técnicos para la gobernanza de datos, en línea con las mejores prácticas enunciadas en el presente documento.

1. fAIr LAC (2021) Acerca de fAIr LAC: en: https://fairlac.iadb.org/

Contexto

En lo individual, los datos pueden representar poco valor económico, comercial o estratégico; sin embargo, cuando se procesan en conjunto de grandes cantidades, ya sea derivados de una sola base de datos o bien compuestos por diversas fuentes, pueden significar un potencial enorme para propósitos de política pública o para cuestiones comerciales.

Conforme se han ido sofisticando las tecnologías de procesamiento de datos, la gestión de los mismos ha permitido la implementación de mecanismos innovadores y automatizados con miras a obtener información más precisa, en menor tiempo y predictiva. Si bien en principio ello significa una transición natural a nuevas técnicas y métodos de explotación de la información, las instituciones enfrentan el reto de equilibrar los beneficios de la innovación y el respeto por las libertades y derechos de protección y privacidad de datos, entre otros derechos.

La comunidad internacional[2] ha concluido que los datos son los insumos de los sistemas automatizados por medio de sistemas de Inteligencia Artificial (IA), y por tanto el impacto de dichos sistemas en la sociedad no sólo depende del diseño bajo el cual han sido desarrollados, sino también su calidad. Por tanto, también deberían observarse ciertos lineamientos y/o principios sobre la gestión y administración de los datos, tales como la forma en que han sido recolectados (es decir que ésta haya sido lícita), transparentar su uso y propósito, que sean suficientemente representativos del segmento de la sociedad para el cual tendrán un efecto determinado, proporcionalidad con relación a su finalidad, seguridad, confidencialidad y su tratamiento conforme a su naturaleza. En este sentido, surge la necesidad de establecer marcos de responsabilidad para todos los actores que participan en el diseño, desarrollo e implementación de un sistema de inteligencia artificial[3], para disuadir ciertos comportamientos no deseados y prevenir riesgos.

Ante esta necesidad, el presente documento consolida recomendaciones sobre gobernanza de datos en dos perspectivas: (i) a partir de la identificación de buenas prácticas en el ciclo de vida de los datos en sistemas autónomos y, (ii) desde la colaboración multi-actor entre organizaciones.

2. Consejo de Europa (https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da), la Red Iberoamericana de Protección de Datos (https://www.redipd.org/sites/default/files/2020-02/guia-recomendaciones-generales-tratamiento-datos-ia.pdf)

3. UNCITRAL (https://undocs.org/es/A/CN.9/1012/Add.1), recoge los tipos de actores definidos por la OCDE en: a) desarrollador: persona responsable del diseño teórico de alto nivel del sistema de IA, así como de la programación, la capacitación y la verificación de dicho sistema, y de su interfaz e integración con el hardware externo y las aplicaciones y fuentes de datos externos antes de la implantación; b) proveedor de datos: persona que proporciona datos —o es responsable de que se proporcionen datos al sistema (es decir, los datos necesarios para respaldar la capacitación, la implantación o el funcionamiento); c) implantador: persona que implanta el sistema integrándolo en sus operaciones (por ejemplo, en los bienes y servicios que suministra), en particular configurando, administrando, manteniendo y respaldando el suministro de los datos y la infraestructura necesarios para el funcionamiento y la supervisión del sistema de IA y su interacción con los datos suministrados una vez implantado; d) operador: la persona que hace funcionar el sistema: i) en muchos casos, el operador es la persona que implanta el sistema; ii) en algunos casos, el operador puede ser el usuario final de los bienes o servicios con IA incorporada (por ejemplo, si el usuario final tiene algún grado de control sobre el funcionamiento de esos bienes o servicios); e) persona afectada: cualquier otra persona 10 afectada por el funcionamiento de un sistema de IA, incluso al interactuar con el sistema (por ejemplo, cuando proporciona datos al sistema) o por ser el usuario final de bienes o servicios con IA incorporada.

Para la perspectiva (i) inicial, se analizó el estado del arte de la gobernanza de datos contemplando normativas positivizadas, es decir, obligatorias en el marco jurídico nacional e internacional, así como normas no vinculantes, guías, directrices, lineamientos, opiniones generadas por la comunidad internacional (tanto del sector público, privado, academia y social) que específicamente han tratado el tema en los años 2018-2022. Como referencia se utilizó la base de datos no exhaustiva del Consejo de Europa[4] mediante la cual concentran más de 450 iniciativas relacionadas con IA.

En el caso de la perspectiva (ii), el objetivo fue dar solución a uno o varios problemas a través de herramientas tecnológicas que dependen de datos (de cualquier naturaleza: personales, sensibles, geográficos, biométricos, etc.); especialmente en casos de índole público o gubernamental. Por ello, se analizaron los posibles mecanismos que pueden implementarse para lograr una gobernanza de datos robusta en el contexto de una solución público-privada. Estos mecanismos van más allá de una tecnología o herramienta digital y cubren temas legales y organizacionales que en conjunto componen una gobernanza efectiva.

Mediante las perspectivas anteriores, este documento tiene como finalidad llevar a la reflexión respecto a las mejores prácticas de gobernanza en sistemas automatizados, considerando como base las discusiones que la comunidad internacional y nacional ha realizado. Es necesario tener en cuenta que esta materia se encuentra en constante evolución, por lo que la actualización de este documento debe de ser una tarea permanente.

Gobernanza de datos

En general, la gobernanza de datos refiere a los mecanismos y procesos que controlan cómo se utilizan, administran, acceden, procesan y almacenan, es decir, la forma en que se gestionan y administran los datos de una organización; con el objetivo principal que los datos conserven su integridad (incluyendo consistencia y confiabilidad) y que sean usados de forma adecuada[5].

Para ello, las empresas e instituciones que requieren de una implementación de gobernanza de datos interna, requieren de personal que cree estándares, políticas, reglas y procedimientos para regular el acceso y utilización de datos en toda la organización.

Ahora bien, la gobernanza de datos tradicional no es suficiente para cubrir escenarios de interés público en los que existen colaboraciones entre gobierno y otros actores (por ejemplo. iniciativa privada y academia), ya que los datos llegan a compartirse fuera del organismo que los obtuvo y/o almacena. Por ello, se ha creado el concepto de gobernanza cívica de datos[6], que cubre estos escenarios tradicionalmente no abarcados por la gobernanza de datos corporativa; poniendo especial énfasis en implementar mecanismos que reduzcan el riesgo de efectos negativos al compartir y utilizar datos generados por ciudades, países, gobiernos o la ciudadanía como grupo social. Usualmente, estos mecanismos incluyen al menos tres elementos clave:[7] reglas claras para el intercambio y uso de datos; diferentes roles y responsabilidades de órganos que los operen a partir de dichas reglas; así como las herramientas de vigilancia para fines de transparencia y rendición de cuentas.

4. https://www.coe.int/en/web/artificial-intelligence/national-initiatives, actualizada el 4 de marzo de 2021.
5. https://www.sap.com/latinamerica/insights/what-is-data-governance.html, actualizado al 23 de mayo de 2022.
6. Más información: https://www.sciencedirect.com/science/article/abs/pii/S0736585320301155
7. Fuente: OECD

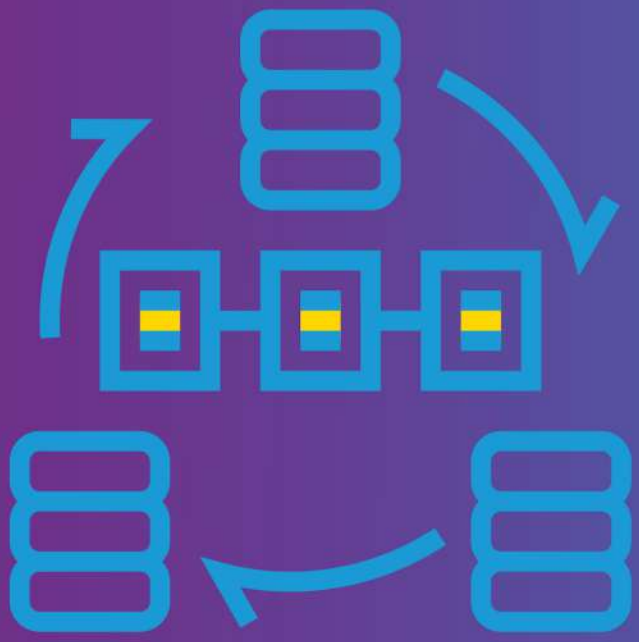
Gobernanza de datos en casos de uso en los que colaboran diversos sectores

A diferencia de datos obtenidos por una empresa para proveer u operar un servicio, los datos recolectados, por ejemplo en centros de salud, así como los provistos a través de dependencias de gobierno, son considerados de índole público[8]. Estos, son difíciles de gobernar al no tener un dueño único o claramente identificable y, en algunos casos, por tener una naturaleza atractiva para empresas que podrían monetizar su uso. En consecuencia, se requiere implementar mecanismos adecuados al interior de las instituciones para lograr colaboraciones público-privadas que cumplan no sólo con las regulaciones de protección de datos, sino también con un uso ético y responsable de éstos, apegado a los derechos humanos y libertades fundamentales y alineado a los mejores intereses de la sociedad.

Los datos de ciudadanos privados pueden verse vulnerados o estar sujetos a mal uso en cualquier punto del ciclo de vida de los mismos. Esta situación es evitable si la entidad gubernamental previamente define, en conjunto con los ciudadanos relacionados y/o afectados, las reglas de acceso y uso de esta información, y actúa de forma imparcial en cómo comparte esta información con terceros (no necesariamente haciéndola pública, pero sí dándole acceso a todos aquellos que lo soliciten y cumplan con los requisitos definidos para su acceso y uso).

8. Ejemplos: la actividad de movilidad de las personas dentro de una ciudad; información obtenida al proveer servicios públicos (salud, educación, seguridad, etc); datos demográficos sobre la población y sus organizaciones.

PARTE I: Recomendaciones operativas para la gobernanza de datos para casos en donde instituciones públicas y/o privadas colaboran en la provisión de datos para el entrenamiento de sistemas de IA



BID BID | LAB Tecnológico de Monterrey Escuela de Ingeniería y Ciencias C MINDS Jalisco

La selección de un modelo de gobernanza sobre otro depende enteramente del contexto en el cuál se implementará y las necesidades que se desean resolver. Por ello, el análisis siguiente se realizó con base en los casos de uso que se implementarán como parte de fAIr LAC Jalisco y de la realidad actual del estado de Jalisco y su gobierno.

Algunos elementos clave del contexto de Jalisco que se tomaron en cuenta para esta sección incluyen información provista por la Coordinación de Datos Abiertos de Jalisco, entre los que destacan: una mayor flexibilidad para realizar cambios a la forma en que se administran y abren los datos, debido a la falta de participación del actual gobierno federal; encontrarse en un momento de definición y planeación respecto a mejoras y restructuración en la forma que los datos del gobierno de Jalisco son almacenados y usados; contar con los recursos humanos y tecnológicos mínimos para realizar estos cambios y mejoras; así como tener apertura interna para implementar más y mejores mecanismos de gobernanza de datos.

En el Anexo III se explican algunos de los mecanismos multisectoriales existentes para la transferencia de datos entre instituciones, incluídos los sistemas tradicionales de análisis de datos; los intermediarios de datos de confianza o Trusted Data Intermediaries (TDI); los fideicomiso cívicos de datos o Civic Data Trusts (CDT) y X Road[9].

Con base en ello, se emiten dos recomendaciones que se describen en las secciones a continuación y pueden ser implementadas de forma conjunta.

Además, es importante mencionar que para lograr una gobernanza cívica completa será necesaria la implementación de cambios a nivel organizacional y humano dentro de las instituciones involucradas, los cuáles, independientemente de estas recomendaciones, deberán estar alineados a principios éticos del uso adecuado y responsable de IA y los datos que la soportan.

Esto quiere decir que el órgano de gobierno que tome el liderazgo de esta iniciativa, acompañado de fAIr LAC Jalisco y las instituciones que le componen, no sólo tendrá que llevar a cabo la integración tecnológica y operativa de estos mecanismos de gobernanza, sino también deberá realizar los ajustes necesarios a los procesos, procedimientos y estructuras de las unidades de gobierno correspondientes.

9. X-Road es una plataforma de código abierto creada por el gobierno de Estonia para la implementación de gobernanza electrónica que permite que, principalmente pero no exclusivamente, entidades de gobierno intercambien datos de forma transparente, controlada, ágil y automatizada (más información en el Anexo III)

Corto Plazo

Si se utiliza la tradicional matriz de impacto-esfuerzo (ver Fig. 4) para elegir entre estos métodos de gobernanza, encontraremos que aunque un Civic Data Trust sería la mejor opción para los ciudadanos, la cantidad de esfuerzo (construcción de software, cambios a la ley, recursos humanos, etc.) requerido es demasiado alta para justificar un uso inmediato que incluso detendría el avance de los proyectos de fAIr LAC Jalisco. Por ello, la mejor forma de dar el primer paso en temas de gobernanza cívica de datos es la implementación de X-Road como una práctica común y dominante en los sistemas del gobierno de Jalisco. A continuación algunas razones de esta recomendación:

1. X-Road requiere poco esfuerzo tecnológico para su implementación (en comparación con algo más complejo, como un TDI), al sólo requerir del despliegue de una capa de software (ya desarrollada y probada por terceros) encima de la infraestructura de gobierno existente.
2. El gobierno de Jalisco ya cuenta con órganos que pueden llevar a cabo el rol de operador central de la red X-Road, por ejemplo: la Dirección General de Tecnologías de la Información o su Coordinación de Datos Abiertos.
3. Jalisco empezará a contar con mecanismos de gobernanza y mayor protección de datos que, aunque básicos, son indispensables.
4. Esta plataforma es suficientemente flexible para permitir adecuaciones, mejoras y una evolución constante de los sistemas de gobierno, ya sea en temas de gobernanza de datos o desarrollo de software en general.
5. La implementación de X-Road permitirá al gobierno de Jalisco que cualquier colaboración con organizaciones externas con las cuales sea necesario compartir datos, se realice de forma automatizada, ordenada, trazable, no-repudiable y granular. Es decir, estas organizaciones podrán ser integradas a la red X-Road del gobierno de Jalisco por el operador central con condiciones claras y controles estrictos como consumidores de datos; y este rol puede ser revocado en cualquier momento, contando además con evidencia sustancial sobre qué datos fueron compartidos, cuándo y por qué con esta organización.

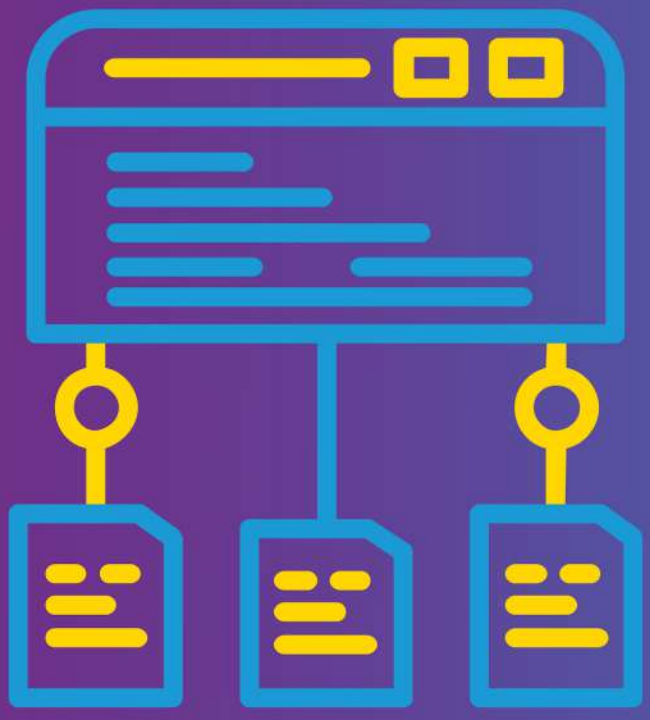
Figura 1. Matriz Impacto/Esfuerzo

Como se mencionó anteriormente, X-Road sólo cubre los elementos y herramientas básicas, por lo que se sugiere también la inclusión del factor humano para complementar con un diseño de gobernanza cívica de datos que integre el contexto ético, legal y cultural (de valores) dentro de las iniciativas de gobierno que dependan de datos y/o colaboración con terceros. Al incluir una capa humana (dentro de la cuál podría incluirse al comité de ética que fue formado para fAIr LAC Jalisco) a cargo de la vigilancia, definición de reglas/normas, la operación y la utilización correcta de estas herramientas de gobernanza, se podrá lograr una gobernanza de sistemas de IA basado en una visión ética.

Largo Plazo

En línea con la recomendación anterior, para lograr una gobernanza cívica de datos integral y enteramente alineada a los intereses de los ciudadanos que generan los datos, se recomienda la implementación de Civic Data Trusts (CDT) posterior a la adopción de una plataforma como X-Road. Al implementar un CDT, se asegura que los datos siempre están siendo utilizados en el mejor interés de sus propietarios y se comienza a crear confianza sobre proyectos basados en datos que previamente eran muy controversiales para siquiera tomarse en cuenta. La implementación de un CDT, por desgracia, implica un esfuerzo que trasciende los elementos meramente tecnológicos y requerirá de una iniciativa de ley o decreto que le dé forma a un órgano autónomo (resolviendo de forma ágil el problema presupuestal que enfrentan algunos CDTs) que pueda cumplir con todos los requerimientos legales; así como algunas leyes o regulaciones auxiliares que fomenten o hagan obligatorio el uso de CDTs para ciertas industrias u operaciones.

PARTE II: Recomendaciones y buenas prácticas en el ciclo de vida de los sistemas autónomos desde los lineamientos y marcos regulatorios existentes



BID BID | LAB Tecnológico de Monterrey Escuela de Ingeniería y Ciencias C MINDS Jalisco

Contexto nacional e internacional

La protección de datos en México se encuentra prevista en diferentes ordenamientos de diversas jerarquías, tanto a nivel constitucional, tratados internacionales, leyes secundarias y otras disposiciones de carácter administrativo.

En principio, la Constitución Política de los Estados Unidos Mexicanos establece que la información sobre la vida privada de una persona y el derecho a la protección de sus datos personales será protegida en los términos y con las excepciones que fijen las leyes[10], garantizando así las directrices y principios sobre los cuales se desarrollan sistemas de transparencia y acceso a la información pública.

De igual forma en el segundo párrafo del artículo 16 Constitucional se establece que: "Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros" disposición sobre la cual se construyen los sistemas de protección de datos personales.

En el ámbito internacional[11], el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, incluye el deber de los Estados Parte de abstenerse de injerencias incompatibles con dicho ordenamiento y de establecer un marco legislativo en el que se prohíban esos actos a las personas físicas o jurídicas, lo que incluye la recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos que podrían ser utilizados en los sistemas [12] de inteligencia artificial.

De manera similar, la Convención Americana de Derechos Humanos , en su artículo 11, párrafo 2, obliga a los Estados a la protección de la honra y dignidad, que comprende que nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación y la protección de la ley contra esas injerencias o esos ataques.

De particular importancia resulta el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal ("Convenio 108")[13] y su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos que fue promulgado por México en 2018. Dicho decreto entró en vigor el día primero de octubre de 2018, con lo cual el Convenio 108 y su Protocolo son vinculantes para México a partir de esa fecha.

10. Artículo 6, primer párrafo, apartado A, fracción II de la Constitución Política de los Estados Unidos Mexicanos.
11. Debemos recordar que en virtud de la reforma constitucional en materia de derechos humanos publicada en el Diario Oficial de la Federación el 10 de junio de 2011, los instrumentos internacionales son un referente obligatorio para garantizar los derechos humanos, y todas las autoridades, en el ámbito de sus competencias, tendrán la obligación de promover, respetar, proteger y garantizar el derecho humano, en este caso, de protección de datos personales de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad.
12. En 2 de marzo de 1981 México ratificó la Convención y el 16 de diciembre de 1998 reconoció como obligatoria de pleno derecho, la competencia contenciosa de la Corte Interamericana de Derechos Humanos, sobre los casos relativos a la interpretación o aplicación de la Convención Americana sobre Derechos Humanos https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos_firmas.htm#M%C3%A9xico.
13. El 26 de abril de 2018 la Cámara de Senadores de México aprobó la adhesión del país al Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo Adicional. A su vez, para cumplir con lo establecido en el artículo 89, fracción I de la Constitución Política de los Estados Unidos Mexicanos, el decreto promulgatorio del Convenio fue publicado en el Diario Oficial de la Federación estableciendo su inicio de vigencia a partir del primero de octubre de 2018.

El Convenio 108 y su Protocolo, tienen por objeto garantizar el derecho a la vida privada de cualquier persona física con relación al tratamiento automatizado de sus datos personales. Los principios y demás disposiciones contenidas en dichos instrumentos resultan aplicables tanto al tratamiento de datos personales por parte de entidades públicas como privadas.

El Consejo de Europa aceptó la adhesión de México al Convenio 108, en virtud de haber encontrado la congruencia normativa de protección establecida en el marco jurídico mexicano con respecto a los principios generales de la región. Es decir, los ordenamientos existentes a nivel federal: tanto la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), como la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) cumplen de manera general con los principios del Convenio 108 y de su Protocolo Adicional[14].

Es importante mencionar que de acuerdo con información difundida en medios de comunicación, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), informó que México ha iniciado gestiones para adherirse a la versión modernizada del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108+), así como la adecuación de la normativa nacional para lograr la armonización con el Reglamento General de Protección de Datos europeo[15].

De acuerdo con lo establecido en el Convenio 108, una de las prerrogativas a las cuales México se obligó, consiste en tomar medidas necesarias en la legislación para que sean efectivos los principios básicos para la protección de datos, así como la atención de ciertos lineamientos sobre los datos de carácter personal que sean objeto de tratamiento automatizado[16].

Otro referente relevante sobre el tratamiento de datos se encuentra en la Red Iberoamericana de Protección de Datos. Ésta surgió con motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos (EIPD) celebrado en La Antigua, Guatemala, del 1 al 6 de junio de 2003, con la asistencia de representantes de 14 países iberoamericanos, entre ellos México. Es un foro en donde participan distintos actores, tanto del sector público como del privado, a través del cual se desarrollan iniciativas y proyectos relacionados con la protección de datos personales en Iberoamérica[17].

En junio de 2017, en el marco del XVI Encuentro Iberoamericano de Santiago de Chile, se aprobaron los "Estándares de Protección de Datos Personales para los Estados Iberoamericanos", criterios orientadores que bien contribuyen a la expedición de regulaciones de protección de datos personales en aquellos países que aún

14. En el Dictamen de las Comisiones Unidas de Relaciones Exteriores, Europa; de Relaciones Exteriores; y de Anticorrupción y Participación Ciudadana, con proyecto de decreto por el que se aprueba la adhesión de México al Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y a su protocolo adicional relativo a las autoridades de control y a los flujos transfronterizos de datos personales se estableció en el numeral 4 de la sección I. Antecedentes Generales: El 16 de octubre, el Comité Consultivo aprobó por unanimidad la Opinión sobre la adhesión de México al instrumento internacional y concluyó que la legislación mexicana de protección de datos personales cumplía de manera general con los principios del Convenio 108 y de su Protocolo Adicional. En ese sentido, opinó que a la solicitud correspondiente se le debía dar una respuesta favorable. https://infosen.senado.gob.mx/sgsp/gaceta/63/3/2018-04-26-1/assets/documentos/Dic_REE_Consejo_Europa_proteccion_datos.pdf.
15. El Economista, Maritza Pérez, México inicia gestiones para suscribir el Convenio 108 de Europa sobre protección de datos a nivel internacional, publicado el 30 de enero de 2021, https://www.eleconomista.com.mx/internacionales/Mexico-inicia-gestiones-para-suscribir-el-Convenio-108-de-Europa-sobre-proteccion-de-datos-a-nivel-internacional-20210130-0020.html.
16. El Economista, Maritza Pérez, México inicia gestiones para suscribir el Convenio 108 de Europa sobre protección de datos a nivel internacional, publicado el 30 de enero de 2021, https://www.eleconomista.com.mx/internacionales/Mexico-inicia-gestiones-para-suscribir-el-Convenio-108-de-Europa-sobre-proteccion-de-datos-a-nivel-internacional-20210130-0020.html.
17. Sitio oficial de la Red Iberoamericana de Protección de Datos https://www.redipd.org/es.

no cuentan con estos ordenamientos, o en su caso, funjan como referente para la modernización y actualización de las legislaciones existentes. Particularmente en el uso de inteligencia artificial, la Red emitió en 2019 principios y recomendaciones para el tratamiento de datos personales, estableciendo un conjunto de directrices y orientaciones para que sean tomados en cuenta, desde el punto de vista de la privacidad por parte de los promotores de esta tecnología emergente.

Ahora bien, la legislación en México que regula específicamente la protección de datos personales y el acceso a la información se concentra en la LFPDPPP y la LGPDPPSO. La LFPDPPP, vigente desde el 6 de julio de 2010, tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. Su observancia es obligatoria para todos los particulares que lleven a cabo el tratamiento de datos personales, con excepción de las sociedades de información crediticia, que se encuentran reguladas por la ley especial. Para efectos de esta Ley, por datos personales se entiende cualquier información concerniente a una persona física identificada o identificable.

Por su parte, la LGPDPPSO, publicada el 26 de enero de 2017 y en vigor al día siguiente de su publicación, tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados. Para efectos de la ley, se consideran sujetos obligados en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos. La LGPDPPSO añade al concepto de datos personales, que se considerará que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Sin ánimo de profundizar en el detalle sobre el contenido de la normativa nacional e internacional dado que no es el propósito de este documento, es posible concluir que México ha logrado armonizar su legislación con la comunidad internacional en lo que se refiere a los principios generales que los sujetos obligados y/o responsables deben observar en el tratamiento de datos personales.

En la siguiente tabla se sintetizan los principios contemplados en los diferentes instrumentos de carácter normativo y orientador arriba mencionados:

Principios Convenio 108[18]	• Obtención y tratamiento justo y legal; • Finalidad determinada y legítima; • Adecuados, pertinentes y no excesivos • Exactos y, si fuera necesario, actualizados; • Se conservarán bajo una forma que permita la identificación de las personas durante un período de tiempo que no exceda del necesario para los fines para los cuales se hayan registrado.
Principios LGPDPPSO	• Licitud, • Finalidad, • Lealtad, • Consentimiento, • Calidad, • Proporcionalidad, • Información y • Responsabilidad en el tratamiento de datos personales
Principios LFPDPPP	• Licitud, • Consentimiento, • Información, • Calidad, • Finalidad, • Lealtad, • Proporcionalidad y • Responsabilidad
Principios Red Iberoamericana de Protección de Datos	• Legitimación • Licitud • Lealtad • Transparencia • Finalidad • Proporcionalidad • Calidad • Responsabilidad • Seguridad • Confidencialidad

18. En el Convenio 108 +, se agregaron nuevos principios, tales como transparencia (artículo 8), proporcionalidad (artículo 5), responsabilidad (artículo 10), impacto evaluaciones (artículo 10) y respeto de la privacidad desde el diseño (artículo 10). Adicionalmente se agregó el derecho a no estar sujeto a una decisión que afecte significativamente basada únicamente en un procesamiento automatizado de datos, sin que se tomen en consideración sus opiniones, y el derecho a obtener conocimiento del razonamiento subyacente al procesamiento de datos, donde se aplican los resultados del procesamiento (artículo 9). Estos nuevos derechos son de particular importancia en la elaboración de perfiles de personas y toma de decisiones automatizada.

Ciclo de vida de los sistemas automatizados

Según el Instituto Alan Turing, el ciclo de vida de los sistemas automatizados está integrado por las siguientes fases[19]:

En todo el ciclo del sistema automatizado, se espera que los actores involucrados: desarrolladores, proveedores de datos, implementadores, operadores y los usuarios finales, observen el estado de derecho y el respeto a los derechos humanos. En este sentido, distintos organismos internacionales han buscado en el ámbito de sus competencias la determinación de principios que guíen tanto a las empresas como a las instituciones de gobierno en el uso de sistemas automatizados u otras tecnologías como la inteligencia artificial[20].

Según los ejes que propone Luciano Floridi, profesor de filosofía y ética de la información de Oxford, para el estudio sobre la ética en los sistemas autónomos, el análisis de los sistemas automatizados se puede abordar bajo tres enfoques: (1) los datos, (2)[12] los algoritmos y (3) las prácticas. Conforme a lo anterior, las recomendaciones contenidas en este documento se concentran en las buenas prácticas de IA sobre los datos, es decir, a la gobernanza de los datos en todo el ciclo de vida del sistema automatizado, considerando tanto normativa vigente como aquella no vinculante pero sí referencial desarrollada por la comunidad internacional.

1. Diseño

En esta fase del ciclo de vida de un sistema de IA se recomienda materializar el cumplimiento de los principios primordialmente en las siguientes actividades:

1. Ejecución de una evaluación sobre el nivel de cumplimiento o congruencia con la normativa legal que regula la protección y privacidad de los datos, particularmente sobre el tratamiento que tendrán los datos en todo el procesamiento:
   a. Sobre este punto, la Red Iberoamericana de Protección de Datos sugiere incluir en dicha evaluación:
      i. Descripción detallada de las operaciones de tratamiento;
      ii. Evaluación de riesgos potenciales para los derechos y libertades de los titulares, o hacia ciertos grupos de la sociedad; y
      iii. Medidas para la mitigación y afrontamiento de los riesgos, incluyendo aquellas de seguridad.

19. Artificial intelligence, human rights, democracy, and the rule of law, realizado por The Alan Turing Institute para soportar el "Feasibility Study published by the Ad Hoc Committee on Artificial Intelligence published in December 2020 del Consejo de Europa", https://www.turing.ac.uk/sites/default/files/2021-03/cahai_feasibility_study_primer_final.pdf.
20. Véase Anexo 1. Matriz no exhaustiva sobre prácticas internacionales.

2. Análisis de la calidad de los datos:
   a. Determinar que los datos se han mantenido exactos, completos, correctos y actualizados a fin de que no se altere la veracidad de éstos[21].
   b. Asegurar que la base de datos que servirá para el entrenamiento y pruebas del sistema de IA, es suficientemente representativa del sector o grupo de personas a quien se dirigirá el uso del sistema de IA[22].
   c. Garantizar proporcionalidad, es decir, sólo podrán ser objeto de tratamiento los datos personales que resulten necesarios, adecuados y relevantes con relación a las finalidades para las que se hayan obtenido.
   d. El Instituto Alan Turing sugiere en esta etapa incluir ciertas preguntas clave:
      i. ¿Hay información faltante?
      ii. ¿Hay valores atípicos o no esperados?
      iii. ¿Se detectan desequilibrios en las categorías de los datos o en la correlación?
   e. La Red sugiere en esta actividad:
      i. Llevar un registro de procedencia de datos
      ii. Otorgar puntajes de veracidad a los conjuntos de datos que están utilizando para el aprendizaje de máquina durante su creación
      iii. Tener conjuntos de datos separados para entrenar, probar y validar el proceso de toma de decisiones.
3. Tratamiento de datos sensibles: cuando el sistema de IA involucre el procesamiento de datos sensibles deben incluirse actividades adicionales en esta etapa:
   a. En términos generales, tanto la LGPDPPSO como la LFPDPPP establecen que no podrán tratarse datos personales sensibles sin el consentimiento de los titulares[23] (salvo algunas excepciones[24]). Particularmente la LFPDPPP establece que no podrán crearse bases de datos que contengan datos personales sensibles[25], sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado[26].
      i. De acuerdo con el artículo 56 del Reglamento de la LFPDPP, sólo podrán crearse bases de datos que contengan datos personales sensibles cuando: (i) obedezca a un mandato legal; (ii) se justifique en términos del artículo 4 de la Ley, o (iii) el responsable lo requiera para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue.
   b. Cuando se tratan datos personales y sensibles se considera que dicho

21. Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario (artículos 23 de la LGPDPPSO y 36 del Reglamento de la LFPDPPP).
22. De acuerdo con reporte "REVIEW INTO BIAS IN ALGORITHMIC DECISION-MAKING publicado por el CENTRE FOR DATA ETHICS AND INNOVATION, en Reino Unido en 2020, la evidencia ha demostrado que ciertas personas están sobrerrepresentadas en los datos en poder de autoridades y esto puede conducir a sesgos en las predicciones e intervenciones, un problema relacionado ocurre cuando el número de personas dentro de un subgrupo es pequeño y estos datos son utilizados para hacer generalizaciones provocando desproporcionadamente altas tasas de error entre grupos minoritarios.
23. Artículo 7 de la LGPDPPSO y artículo 9 de la LFPDPPP.
24. Artículo 22 de la LGPDPPSO y artículo 10 de la LFPDPPP
25. Esta normativa es congruente con lo dispuesto en el artículo 6 del Convenio 108 en el que se establece que los datos de carácter personal que revelen el origen racial, las opiniones políticas, las creencias religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que la legislación interna prevea garantías apropiadas. Se entiende que dichas garantías serán adicionales a las medidas de seguridad para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.
26. Artículo 9 de la LFPDPPP.

tratamiento es intensivo[27] y en este caso se debe realizar una evaluación de impacto[28] sobre la protección de datos personales y presentarla ante el INAI o los Organismos garantes estatales, los cuales podrán emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales.

i. La evaluación de impacto tendrá por objeto:
   - Identificar y describir los riesgos altos, potenciales y probables que entrañan los tratamientos intensivos o relevantes de datos personales;
   - Describir las acciones concretas para la gestión de los riesgos;
   - Analizar y facilitar el cumplimiento de los principios, deberes, derechos y demás obligaciones previstas en la normativa respecto a tratamientos intensivos o relevantes de datos personales, y
   - Fomentar una cultura de protección de datos personales al interior de la organización del responsable.

ii. Particularmente, las disposiciones señalan que en la evaluación de impacto deberán describirse y representar cada una de las fases de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, específicamente el ciclo de vida de éstos a partir de su obtención, aprovechamiento, explotación, almacenamiento, conservación o cualquier otra operación realizada.

iii. Además de lo previsto en el párrafo anterior del presente artículo, el responsable deberá señalar:
   - Las fuentes internas y/o externas, así como los medios y procedimientos a través de los cuales se recabarán los datos personales, o bien, son recabados;
   - Las áreas, grupos o personas que llevarán a cabo operaciones específicas de tratamiento con los datos personales;
   - Los plazos de conservación o almacenamiento de los datos personales, y
   - Las técnicas a utilizar para garantizar el borrado seguro de los datos personales.

i. Particularmente en el tratamiento de datos biométricos se recomienda consultar la Guía para el Tratamiento de Datos Biométricos emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

iv. Particularmente en el tratamiento de datos biométricos se recomienda consultar la Guía para el Tratamiento de Datos Biométricos emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales[29].

27. Art. 75 de la LGPDPPSO.
28. Para conocer el detalle de la evaluación de impacto, se sugiere consultar el acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, publicado en el Diario Oficial de la Federación el 23 de enero de 2018.
29. Guía para el Tratamiento de Datos Biométricos, 2018, consultada el 30 de abril de 2021 en la siguiente liga: https://home.inai.org.mx/wpcontent/documentos/DocumentosSectorPublico/GuiaDatosBiometricos_Web_Links.pdf.

2. Desarrollo

En el Convenio 108, se define como "tratamiento automatizado", las operaciones efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: registro de datos, aplicación a esos datos de operaciones lógicas y/o aritméticas, su modificación, borrado, extracción o difusión y por "autoridad controladora del fichero" significa la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sea competente de conformidad con la legislación nacional para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán.

La LGPDPPSO incluye en la definición de "tratamiento" cualquier operación o conjunto de operaciones efectuadas mediante procedimientos automatizados aplicados a los datos personales[30]. Asimismo, la LFPDPPP considera el "tratamiento" como la obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. En este sentido, ambos ordenamientos demuestran no estar desvinculados totalmente de la regulación sobre sistemas automatizados. Todas las disposiciones relacionadas con el tratamiento, así como derechos de protección, deben entenderse también extendidos a los sistemas automatizados[31].

Durante todo el tratamiento de los datos se deben implementar ciertas medidas para evitar vulnerabilidades a los derechos de privacidad y protección de datos personales. En la modificación del Convenio 108, se integró un contexto más robusto sobre el procesamiento legítimo de los datos, estableciendo los siguientes elementos:

- El procesamiento debe ser proporcional al propósito perseguido y demostrar en todo momento un equilibrio entre los intereses involucrados, ya sean públicos o privados, así como las libertades y derechos que estén en juego;
- El procesamiento debe ejecutarse sobre la base de un consentimiento libre, específico, informado y no ambiguo del titular o cualquier otra disposición legal que así lo permita;
- El procesamiento debe ser legal, justo y transparente;
- Los datos deben ser recopilados para fines explícitos, específicos, legítimos y no procesados de una manera incompatible con dichos fines;
- El procesamiento posterior con fines de archivo en el interés público, fines de investigación científica o histórica o fines estadísticos es, deberá estar sujeto a las salvaguardias apropiadas, compatibles con esos propósitos;
- El procesamiento de los datos deberá ser adecuado, pertinente y no excesivo en relación con los fines, deberá ser adecuado y, cuando sea necesario, ser actualizado; y
- No debería conservarse el procesamiento que permita la identificación de los titulares más allá de lo estrictamente necesario para el cumplimiento de los fines para el cual se procesan esos datos.

Si bien en la normativa nacional no hay referencias específicas, salvo en casos muy particulares, sobre el tratamiento de datos a través de sistemas automatizados, en la siguiente Tabla se muestra la equivalencia normativa:

30. Artículo 3, fracción XXXIII de la LGPDPPSO.
31. Si bien no hace referencia expresa al uso de sistemas automatizados por IA ni a ningún tipo de tecnología o método técnico, el procesamiento automatizado de datos personales, para generar predicción o recomendación sobre alguien; se entiende como tratamiento de datos en términos de las leyes mencionadas. En el mismo sentido lo establece el criterio contenido en la tesis aislada I.10o.A.6 CS (10a.), al considerar que el deber del Estado de salvaguardar el derecho humano a la privacidad y protección de datos debe potencializarse ante las nuevas herramientas tecnológicas, debido a los riesgos que éstas representan por sus características especiales.

Derechos en el procesamiento de los datos contemplados en la normativa

Derecho a ser informado

Convenio 108 y su modificación

Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero

LFPDPPP

Los datos personales proporcionados serán tratados conforme a lo que acordaron las partes.

Si bien no contempla específicamente la obligación de informar a la persona afectada sobre la existencia de decisiones exclusivamente automatizadas, el artículo 12 del Reglamento de la Ley
establece como características del consentimiento, que éste debe ser:

- Libre: sin que medie error, mala fe, violencia o dolo, que puedan afectar la manifestación de voluntad del titular;
- Específica: referida a una o varias finalidades determinadas que justifiquen el tratamiento, y
- Informada: que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales y las consecuencias de otorgar su consentimiento.

LGPDPPSO

Establece las mismas prerrogativas que la LFPDPPP; sin embargo, al tratarse de entes públicos o personas que ejercen funciones o recursos públicos, limita el tratamiento de datos personales, además de la debida justificación, a finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.

La LGPDPPSO al reconocer el derecho del titular de oponerse al tratamiento automatizado de sus datos personales, es dable inferir que ello implica que le debe informar cuando esté frente a este tipo de procesamiento.

Derechos en el procesamiento de los datos contemplados en la normativa

Derecho al acceso, ratificación, corrección y borrado

Convenio 108 y su modificación

Obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que concierne a dicha persona, así como la comunicación de dichos datos en forma inteligible.

LFPDPPP

Deberán contemplarse en el aviso de privacidad los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley

LGPDPPSO

El responsable deberá establecer procedimientos sencillos que permitan el ejercicio de los derechos ARCO.

Derecho al olvido

LFPDPPP y LGPDPPSO

Tanto la LFPDPPP como la LGPDPPSO establecen que el tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá realizar esfuerzos razonables para limitar el periodo de tratamiento de los mismos a efecto de que sea el mínimo indispensable.

Derechos en el procesamiento de los datos contemplados en la normativa

Derecho de oposición

Convenio 108 y su modificación

Los titulares tienen el derecho de no ser objeto de una decisión que le afecte significativamente, únicamente basada en el procesamiento automatizado de datos sin haber sido tomado en cuenta.

LFPDPPP

Si bien no contempla una referencia específica, el titular o su representante legal en cualquier momento podrán solicitar al responsable, en cualquier momento, la oposición del tratamiento, respecto de los datos personales que le conciernen.

LGPDPPSO

En este caso la normativa si prevé un supuesto específico a la oposición del tratamiento mediante sistemas automatizados, pues reconoce al titular su derecho a exigir que se cese el tratamiento cuando:

- Aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular,
- Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

Ahora bien, dado el potencial riesgo que puede significar el uso de sistemas automatizados, la tendencia internacional ha sido establecer ciertos principios rectores sobre los cuales se visualiza la construcción de normativa a futuro, independientemente si se procesan datos personales o no.

La OCDE definió como principios: (i) Crecimiento inclusivo, desarrollo sostenible y bienestar; (ii) Valores centrados en el ser humano y equidad: (iii) Transparencia y explicabilidad: (iv) Robustez, seguridad y protección; y (v) Rendición de cuentas. La definición de estos principios y su conexión a la gobernanza de datos puede encontrarse en el Anexo I de este documento.

De manera similar, el Comité Ad Hoc en IA del Consejo de Europa estableció nueve principios: (i) Dignidad humana; (ii) Autonomía y libertades humanas; (iii) Prevención del daño; (iv) No discriminación, equidad de género, justicia y diversidad; (v) Transparencia y explicabilidad; (vi) Protección de datos y privacidad; (vii) Responsabilidad y rendición de cuentas; (viii) Democracia; y (ix) Estado de derecho.

A continuación, se detallan las obligaciones clave de los principios establecidos por el Comité Ad Hoc[32]:

32. Se toma como base el documento elaborado por el Instituto de Alan Turing, Artificial intelligence, human rights, democracy, and the rule of law, realizado por The Alan Turing Institute para soportar el "Feasibility Study published by the Ad Hoc Committee on Artificial Intelligence published in December 2020 del Consejo de Europa", https://www.turing.ac.uk/sites/default/files/2021-03/cahai_feasibility_study_primer_final.pdf

Principio	Obligaciones relacionadas
Dignidad Humana	• Aquellas tareas en las que pudiera existir el riesgo de violaciones a la dignidad humana al usar un sistema automatizado deberán reservarse esa tarea a un ser humano. • Informar a los usuarios de sistemas de IA que están interactuando con un sistema y no con un ser humano.
Autonomía y libertades humanas	• Cualquier procesamiento de datos personales a través de un sistema automatizado debe cumplir con la normativa aplicable. • Es necesario establecer mecanismos de supervisión diseñados en función del riesgo específico que pudiera provocar el sistema automatizado. • Los desarrolladores e implementadores deberán comunicar las opciones de reparación de manera oportuna.
Prevención del daño	• Los desarrolladores e implementadores deberán tomar las medidas necesarias para minimizar cualquier daño físico o mental a los individuos, la sociedad y el medio ambiente. • Se deberá asegurar la existencia de seguridad desde el diseño y por defecto, requerimiento y cumplimiento de robustez • Los sistemas automatizados deben desarrollarse y usarse de forma sustentable con pleno respeto a la protección de estándares del medio ambiente.
No discriminación, equidad de género, justicia y diversidad	• Los sistemas automatizados no podrán provocar resultados discriminatorios ilegales, estereotipos dañinos (género), desigualdad social acentuada, por lo que se deberá de usar el escrutinio más alto en la promoción del uso de los sistemas en áreas sensibles de política pública, incluyendo de forma enunciativa más no limitativa: justicia, seguridad pública, migración, asilos, salud, seguridad social y laboral. En la etapa de desarrollo será fundamental ejecutar pruebas piloto para ajustar o corregir cualquier sesgo o posibles impactos negativos en la esfera de los derechos fundamentales de los usuarios. • En los procesos de adquisición del sector público se incluirán requisitos de no discriminación y promoción de la equidad. Asegurando que dichos sistemas estén sujetos a auditorías independientes sobre posibles efectos discriminatorios antes de ser implementados.

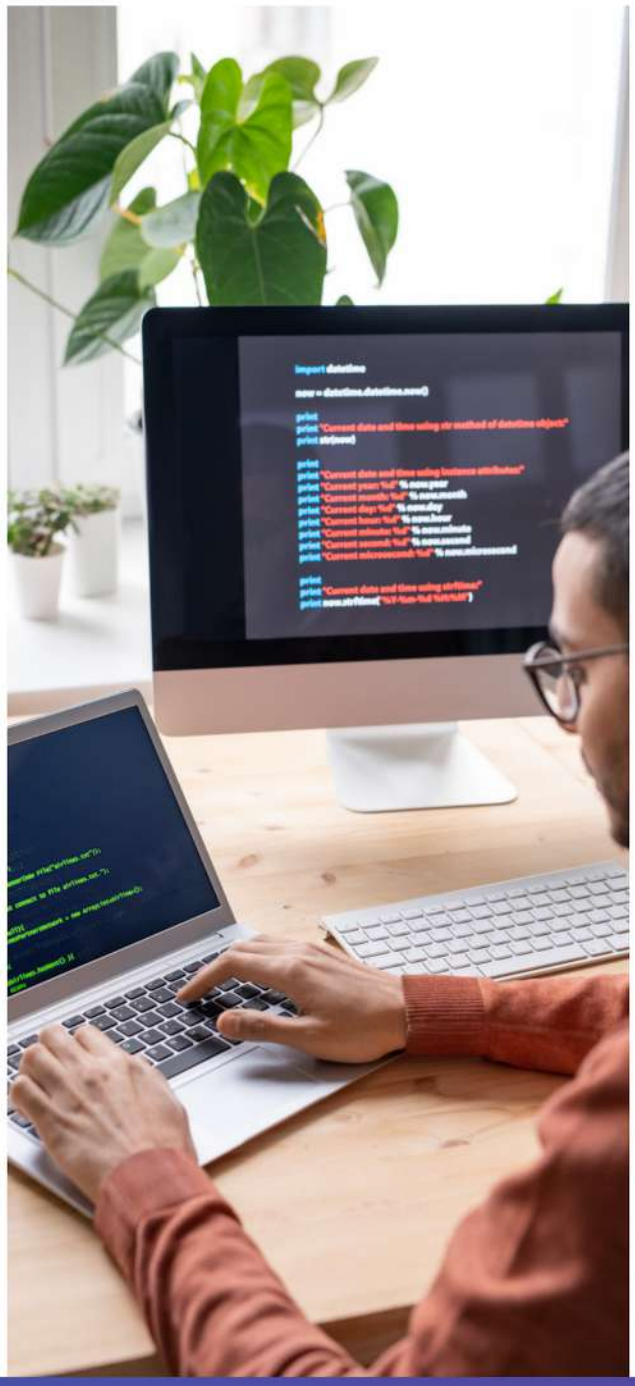
Principio	Obligaciones relacionadas
No discriminación, equidad de género, justicia y diversidad	• Se deberán imponer requisitos para contrarrestar eficazmente los posibles efectos discriminatorios de los sistemas autónomos desplegados tanto por el sector público como por el privado y proteger a las personas de las consecuencias negativas de los mismos. Estos requisitos serán proporcionales al riesgo involucrado. • Deberá promoverse la diversidad y la equidad de género en la fuerza laboral que desarrolla sistemas automatizados así como la retroalimentación periódica de los actores involucrados. Se debe fomentar la conciencia del riesgo de discriminación, los nuevos tipos de diferenciación y el sesgo en el contexto de sistemas automatizados.
Transparencia y explicabilidad	• Los usuarios deben estar claramente informados sobre su derecho a ser asistidos por un ser humano al usar un sistema automatizado que pueda impactar en sus derechos, particularmente en el contexto de servicios públicos. • Siempre que se ponga en riesgo los derechos humanos, la democracia o el estado de derecho, se impondrán requisitos de trazabilidad y de provisión de información. • Debería hacerse pública y accesible toda la información relevante sobre los sistemas automatizados (incluyendo su funcionamiento, optimización, lógica asociada, tipos de datos procesados) en la provisión de servicios públicos mientras se salvaguarde la seguridad o la propiedad intelectual.
Protección de datos y privacidad	• Salvaguardar los derechos de privacidad y protección de datos en todo el ciclo de vida del sistema automatizado que implemente el sector público o privado. • Deberán tomarse medidas efectivas para proteger a los individuos de medidas de vigilancia masiva (reconocimiento biométrico o cualquier otra tecnología de rastreo). • Al implementar un sistema automatizado se deberá evaluar y mitigar cualquier impacto negativo al derecho de privacidad y protección de datos. En particular deberá analizarse la proporcionalidad de la invasión de los sistemas en virtud de la legítima necesidad de su utilización. • Deberán establecerse salvaguardas apropiadas para el flujo transfronterizo de datos a fin de asegurar reglas sobre la protección de datos.

Principio	Obligaciones relacionadas
Responsabilidad y rendición de cuentas	• Asegurar medidas compensatorias eficientes y disponibles bajo la jurisdicción nacional, incluyendo responsabilidad civil y penal para aquellos que han sufrido perjuicios en sus derechos en virtud del uso de un sistema automatizado. • Deberá establecerse supervisión gubernamental para aquellos sistemas que pudieran generar un perjuicio en la esfera de los derechos humanos, democracia o estado de derecho. • Deberá identificarse, documentarse e informar sobre los potenciales impactos negativos de la operación de sistemas automatizados en la esfera de los derechos humanos, la democracia y el estado de derecho. • Deberán implementar medidas de mitigación adecuadas para asegurar la responsabilidad y rendición de cuentas por cualquier daño causado. • La autoridad gubernamental debería siempre poder auditar un sistema automatizado, incluso en el sector privado, para evaluar su nivel de cumplimiento conforme a la normativa y solicitar su rendición de cuentas.
Democracia	• Deberán tomarse medidas adecuadas para contrarrestar el uso inadecuado de sistemas automatizados para interferir en procesos electorales, políticas personalizadas focalizadas, sin la transparencia, responsabilidad y rendición de cuentas necesaria, para incidir en el comportamiento de los votantes o manipular su opinión. • Se adoptarán estrategias para combatir la desinformación, así como para identificar discursos de odio para asegurar la pluralidad justa de la información. • Deberá procurarse en los procesos de adquisición gubernamental el cumplimiento de salvaguardas relacionadas con estos principios. • Promover la educación en habilidades digitales en todos los segmentos de la sociedad.
Estado de derecho	• En los sectores de justicia y seguridad deberá asegurarse que los sistemas automatizados que se utilicen cumplan con los requisitos de legalidad y debido proceso. Debiendo asegurar la calidad y seguridad de las decisiones judiciales y los datos relacionados, así como la transparencia e imparcialidad.

Principio	Obligaciones relacionadas
Estado de derecho	• Deberán preverse medidas compensatorias para aquellos que sufran un perjuicio en virtud del uso de un sistema automatizado en el sector del estado de derecho. • Posibilitar información significativa sobre el uso de sistemas automatizados en el sector público, especialmente aquellos en el área de la justicia y seguridad. • El uso de sistemas automatizados no deberá interferir con la atribución de los juicios para emitir decisiones con independencia y que cualquier resolución judicial está sujeta a la supervisión humana.

Será en la fase de desarrollo e implementación del sistema automatizado donde se podrá obtener información relevante y crítica que permita a los desarrolladores e implementadores ajustar el grado de cumplimiento del sistema automatizado con los principios arriba mencionados, toda vez que se ve involucrado el proceso de limpieza de datos, selección, entrenamiento, prueba y validación del modelo, con sus respectivos sets de datos para conocer y definir comportamientos esperados.

Cuando se tenga validado el modelo, entonces podrá llevarse a cabo su evaluación, incluyendo la variedad de comportamientos, así como de los impactos. En este momento, se genera la información detallada acerca del flujo de operación del modelo para soportar los elementos de transparencia sobre los resultados del modelo.



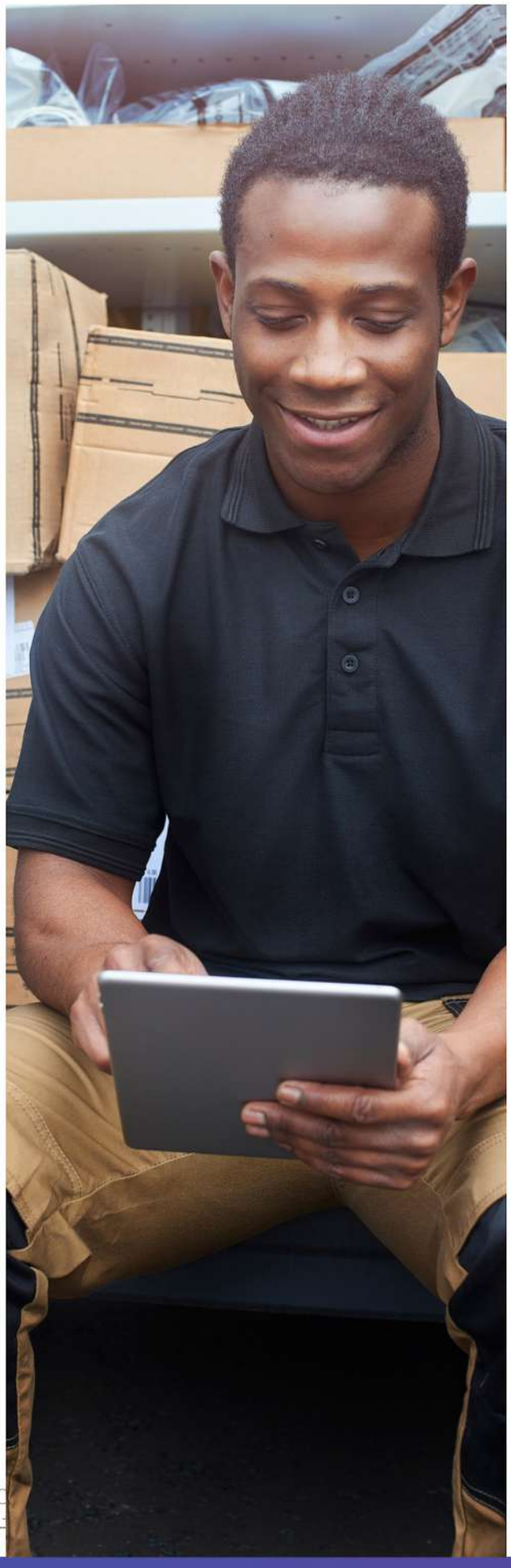
3. Implementación

Con la puesta en marcha del sistema de IA y la interacciónconcon los usuarios finales se recopilan nuevos datos, por lo tanto es recomendable realizar de manera iterativa actividades que permitan evaluar, supervisar y monitorear el comportamiento del sistema para asegurar que se siguen cumplimiento con los elementos previamente comprobados en las fases de diseño y desarrollo[33].

- Para atender y dar seguimiento al sistema de IA, es recomendable que la organización, ya sea pública o privada, forme una estructura con funciones y responsabilidades claras que garanticen el gobierno de los datos en todo el ciclo de vida del sistema automatizado.
- Realizar evaluaciones y manejo de riesgos (periódica).
- Realizar actividades de mantenimiento, monitoreo y revisión (periódica).
- Al transcurrir el tiempo, el sistema de IA podría perder efectividad, para ello será necesario regresar a las fases de diseño y desarrollo para modificar o eliminar procesos o incluso cambiar de modelos de entrenamiento.

Por otro lado, también será responsabilidad de los actores que participan en el diseño, desarrollo e implementación de un sistema de IA tener claridad sobre su responsabilidad frente a los usuarios. Para ello se listan las siguientes recomendaciones:

- Demostrar, de ser necesario, que han cumplido con todos los deberes relacionados con el tratamiento de los datos, incluyendo normas jurídicas como éticas sobre el respeto a derechos humanos, la sociedad y su bienestar.
- Mantener un equipo capacitado y actualizado sobre los estándares del sector en el que opera el sistema de IA, así como de la regulación que eventualmente surja para, de ser necesario, ajustar el modelo de entrenamiento elegido.



33. Red Iberoamericana de Protección de Datos, Tratamiento de Datos en Inteligencia Artificial, 20 https://www.redipd.org/sites/default/files/2020-tratamiento-datos-ia.pdf.

Conclusión

Tomando en consideración la normativa nacional e internacional, así como las consideraciones y buenas prácticas ofrecidas en la sección anterior de este documento, se emiten las siguientes recomendaciones generales:

- Si bien la normativa actual relacionada con la protección de datos personales y derecho a la privacidad no hace referencia explícita al término "inteligencia artificial", existen disposiciones legales y reglamentarias, tanto a nivel internacional como nacional, cuyo alcance repercute indudablemente en el diseño, desarrollo e implementación de sistemas automatizados mediante el cual se procesan datos y, por tanto, es necesario observarlos para que se considere como un sistema lícito.

  La LGPDPPSO incluye en la definición de "tratamiento" cualquier operación o conjunto de operaciones efectuadas mediante procedimientos automatizados aplicados a los datos personales[34]. Así mismo la LFPDPPP considera el "tratamiento" como la obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. En este sentido ambos ordenamientos demuestran no estar desvinculados totalmente de la regulación sobre sistemas automatizados, todas las disposiciones relacionadas con el tratamiento, así como derechos de protección deben entenderse también extendidos a los sistemas automatizados[35].

- Tanto los entes públicos como los privados que realicen el diseño y análisis de un sistema automatizado con el uso de IA debieran por lo menos:
  - Ejecutar una evaluación sobre el nivel de cumplimiento o congruencia con la normativa legal que regula la protección y privacidad de los datos, particularmente sobre el tratamiento que tendrán los datos en todo el procesamiento;
  - Llevar a cabo el análisis de la calidad de los datos, y en su caso,
  - Observar disposiciones adicionales para el tratamiento de datos sensibles.

- Un requisito indispensable para asegurar el éxito en la implementación de un sistema automatizado es la formación de una estructura con funciones y responsabilidades claras que garanticen el gobierno de los datos en todo el ciclo de vida del sistema.

- En virtud que no todos los sistemas automatizados tendrán las mismas implicaciones, efectos e impactos en la sociedad, la observancia de los principios que rigen el diseño, desarrollo e implementación de un sistema automatizado debe ejecutarse a la luz de los riesgos identificados tanto para la sociedad en su conjunto como de manera individual.

- Los sistemas automatizados implementados por entes públicos tienen un valor específico en cuanto a su repercusión con la sociedad. Dependiendo el sector en el que se vayan a utilizar, así como el nivel de autonomía que tendrían dichos sistemas para afectar la esfera jurídica de los particulares,

34. Artículo 3, fracción XXXIII de la LGPDPPSO.
35. Si bien no hace referencia expresa al uso de sistemas automatizados por IA ni a ningún tipo de tecnología o método técnico, el procesamiento automatizado de datos personales para generar predicción o recomendación sobre alguien, se entiende como tratamiento de datos en términos de las leyes mencionadas. En el mismo sentido lo establece el criterio contenido en la tesis aislada I.10o.A.6 CS (10a.), al considerar que el deber del Estado de salvaguardar el derecho humano a la privacidad y protección de datos debe potencializarse ante las nuevas herramientas tecnológicas, debido a los riesgos que éstas representan por sus características especiales.

resulta esencial garantizar la legalidad y seguridad jurídica de la relación supranacional con el gobernado y por tanto debieran preexistir las siguientes condiciones:
  - El marco legal habilite la toma de decisiones exclusivamente automatizadas que produzcan efectos significativos,
  - Actualizarse los supuestos para su actuación,
  - Encontrarse normada la información significativa sobre la lógica involucrada y la importancia y las consecuencias previstas para el individuo y
  - Dar a conocer al afectado estas circunstancias en el mismo acto.

- Los entes públicos deben responder a un principio de máxima transparencia en su relación con la ciudadanía, por tanto, cuando se utilicen sistemas automatizados para implementar políticas públicas o prestar servicios públicos se vuelve relevante la necesidad de explicitar la responsabilidad de los actores que convergen en el diseño, desarrollo e implementación de los sistemas automatizados. Esto con la finalidad de que el público en general cuente con los elementos necesarios para evaluar el desempeño de estos sistemas y sus efectos jurídicos.

- Hay ciertos principios que deberán regir el uso de sistemas automatizados, entre estos: (i) Dignidad humana; (ii) Autonomía y libertades humanas; (iii) Prevención del daño; (iv) No discriminación, equidad de género, justicia y diversidad; (v) Transparencia y explicabilidad; (vi) Protección de datos y privacidad; (vii) Responsabilidad y rendición de cuentas; (viii) Democracia; y (ix) Estado de derecho. De tal suerte que será recomendable que las empresas desarrollen políticas y procedimientos apropiados que les permita asumir su responsabilidad frente a aquellos que resulten afectados por comportamientos de sistemas automatizados.

- Existen diversos enfoques sobre la información que debería estar disponible para que los usuarios obtengan un entendimiento claro sobre el funcionamiento de la explicabilidad de sistemas automatizados. Por ello, se recomienda ofrecer información suficiente y clara para que cualquier persona que esté interactuando con sistemas automatizados conozca:
  - La trazabilidad de los datos[36],
  - Comportamientos esperados,
  - Conocimiento de las capacidades y limitaciones del sistema,
  - Conocimiento de que están interactuando con un sistema automatizado,
  - Los mecanismos de supervisión humana establecidos, y
  - Las personas responsables de la operación del sistema.

36. La trazabilidad de los datos se entiende como toda aquella información que ofrezca al usuario claridad sobre las fases o etapas por las que sus datos personales fueron procesados en el sistema de IA, desde su recolección hasta su eliminación.

Recursos

Fuente	Titulo
PricewaterhouseCoopers	The foundation for smart city success: Seven layers of data governance and management
OECD	Data governance in the public sector
OECD	Recommendation of the Council on Digital Government Strategies
Statistics Estonia	Development Plan of Statistics Estonia 2018–2022: Statistics Estonia as coordinator of state data governance
Stats New Zealand	An operational Data Governance Framework for New Zealand Government
USA's Federal Data Strategy	Data Governance Playbook
European Commission	Data governance and data policies
Murdoch University, Australia	Government data does not mean data governance: Lessons learned from a public sector application audit
Consejo de Europa	AD HOC COMMITTEE ON ARTIFICIAL INTELLIGENCE (CAHAI)
Consejo de Europa	Non-exhaustive data collection by the Secretariat
Red Iberoamericana de Protección de Datos	RECOMENDACIONES GENERALES PARA EL TRATAMIENTO DE DATOS EN LA INTELIGENCIA ARTIFICIAL
UNCITRAL	CUESTIONES JURÍDICAS RELACIONADAS CON LA ECONOMÍA DIGITAL: LA INTELIGENCIA ARTIFICIAL
The Alan Turing Institute y el Consejo de Europa	Artificial intelligence, human rights, democracy, and the rule of law.
Cámara de Diputados	• Constitución Política de los Estados Unidos Mexicanos • Ley Federal de Protección de Datos Personales en Posesión de los Particulares • Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados • Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Recursos

Fuente	Titulo
Diario Oficial de la Federación	Decreto Promulgatorio del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, hecho en Estrasburgo, Francia, el veintiocho de enero de mil novecientos ochenta y uno.

ANEXOS

Indice de anexos

BID BID | LAB Tecnológico de Monterrey Escuela de Ingeniería y Ciencias C MINDS Jalisco

Anexo I. Gobernanza de datos y los principios de la IA ética y responsable de la OCDE.

En mayo de 2019 fueron adoptados por los países miembros de la Organización para la Cooperación y el Desarrollo Económico (OCDE) los Principios de la OCDE sobre IA cuando aprobaron la Recomendación del Consejo de la OCDE sobre Inteligencia Artificial[1], un documento resultante del trabajo colaborativo de un comité formado por 50 miembros, y representando a 20 países. Si bien los principios promulgados se enfocan en la Inteligencia Artificial, también se menciona la importancia de la infraestructura digital que acompañará forzosamente, la adopción de esta tecnología. Es por esto que resulta pertinente, describir cómo la gobernanza de los datos está relacionada con la capacidad de los sistemas que utilizan IA de apegarse a los principios éticos de la IA.

En la recomendación la OCDE definió como principios: (i) Crecimiento inclusivo, desarrollo sostenible y bienestar; (ii) Valores centrados en el ser humano y equidad: (iii) Transparencia y explicabilidad: (iv) Robustez, seguridad y protección; y (v) Rendición de cuentas. Si bien los documentos emitidos por la organización no son legalmente vinculantes para los países miembros, son recursos que definen un estándar internacional y que ayuda a los gobiernos a generar legislaciones nacionales.

En adelante se busca definir brevemente cada uno de los principios y describir su relación con la gobernanza de datos para sistemas que utilizan IA. A lo largo del presente documento, específicamente en la Parte II, se detallarán recomendaciones para su implementación desde los lineamientos y marcos regulatorios existentes.

A. Crecimiento inclusivo, desarrollo sostenible y bienestar

Este primer principio dispone que los actores que desarrollan, implementan u operan sistemas de IA deben ser activamente responsables de su funcionamiento adecuado, para tener resultados que generen crecimiento inclusivo, desarrollo sostenible y bienestar.[2]

En este sentido, el trabajo que están desarrollando las instituciones e individuos que conformamos la iniciativa del hub local en Jalisco de la iniciativa fAIr LAC, deberá priorizar el bienestar de los habitantes del estado, teniendo en cuenta las características demográficas de los mismos y estableciendo mecanismos que garanticen la inclusión y sostenibilidad de las soluciones que surjan del desarrollo de los casos de uso.

---

[1] OECD Legal Instruments, Recommendation of the Council on Artificial Intelligence, publicado el 21de mayo de 2019, en https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

[2] Banco Interamericano de Desarrollo, Pombo, Cristina; Cabrol, Marcelo; González Alarcón, Natalia; Sánchez Ávalos, Roberto, fAIr LAC: Adopción ética y responsable de la inteligencia artificial en América Latina y el Caribe, enero del 2020, en http://dx.doi.org/10.18235/0002169

Para ello, en adición a lo que se desarrollará en la Parte II del documento, es recomendable que se considere la realización de evaluaciones de impacto periódicas de acuerdo a las características de cada caso de uso y los riesgos identificados, así como estudios de impacto ambiental de las soluciones desarrolladas, dado que la huella ecológica que supone su desarrollo, entrenamiento, despliegue y monitoreo es considerable.[3] Sin esta información será complejo sopesar los beneficios obtenidos por la solución en relación a sus impactos y posibles riesgos ecológicos.

B. Valores centrados en el ser humano y equidad

De acuerdo a éste principio los actores deben respetar el estado de derecho, los derechos humanos y los valores democráticos a lo largo de todo su ciclo de vida. Entre estos últimos sobresalen la libertad, la dignidad y la autonomía, la privacidad y la protección de los datos, la no discriminación y la igualdad, la diversidad, la equidad, la justicia social y los derechos laborales internacionalmente reconocidos. Para ello los actores deben implementar mecanismos y salvaguardias de protección de derechos. Estos deben ajustarse al contexto y ser consistentes con el estado del arte. [4]

Referente a este principio el desarrollo de las Partes II y III del documento profundizan en los contextos, estado del arte y los mecanismos existentes para la protección de las personas, y la garantía de la equidad de resultados al interactuar con sistemas que utilizan IA.

C. Transparencia y explicabilidad

En este principio se establece que los actores deberán comprometerse con la transparencia y la divulgación responsable de los sistemas relacionados. Deberán proporcionar información relevante que se ajuste al contexto y sea coherente con el estado del arte. Con lo anterior se busca: (i) fomentar una comprensión general de los sistemas de IA, (ii) procurar que las partes interesadas tomen plena conciencia de sus interacciones con los sistemas de IA, (iii) asegurarse de que los afectados por un sistema de IA entiendan el resultado, y (iv) permitir que las personas afectadas adversamente por un sistema de IA impugnen sus resultados basándose en información clara y fácil de entender sobre los factores y la lógica que sirvieron de base para la predicción, recomendación o decisión que se busca refutar.[5]

Referente a este principio el desarrollo de la Partes II del documento expone los mecanismos y obligaciones existentes, así como el estado del arte en temas regulatorios para sistemas autónomos, dentro de los que actualmente se contemplan aquellos que utilizan la IA.

---

[3]https://www.lavanguardia.com/tecnologia/innovacion/20190617/462863973194/inteligencia-artificial-impacto-ambiental.html

[4] Banco Interamericano de Desarrollo, Pombo, Cristina; Cabrol, Marcelo; González Alarcón, Natalia; Sánchez Ávalos, Roberto, fAIr LAC: Adopción ética y responsable de la inteligencia artificial en América Latina y el Caribe, enero del 2020, en http://dx.doi.org/10.18235/0002169

[5] Banco Interamericano de Desarrollo, Pombo, Cristina; Cabrol, Marcelo; González Alarcón, Natalia; Sánchez Ávalos, Roberto, fAIr LAC: Adopción ética y responsable de la inteligencia artificial en América Latina y el Caribe, enero del 2020, en http://dx.doi.org/10.18235/0002169

Adicionalmente es importante que las instituciones que conforman la iniciativa, continúen realizando una labor de socialización de la tecnología para garantizar una comprensión general de los sistemas en todos los sectores de la sociedad. Adicionalmente es importante que todos los involucrados puedan tener acceso a información que les permita comprender los fines para los que podrían ser utilizados sus datos, y los riesgos que conlleva para los individuos y las organizaciones parte.

D. Robustez, seguridad y protección

De acuerdo a este principio la robustez, la seguridad y la protección son elementos esenciales de todo sistema de IA por las siguientes razones: (i) Los sistemas de IA deben ser robustos, seguros y protegidos durante todo su ciclo para que, en condiciones de uso normal, uso previsible, uso incorrecto u otras condiciones adversas, funcionen adecuadamente y no supongan un riesgo irrazonable para la seguridad. (ii) Para ello, los actores de la IA deben garantizar la trazabilidad permanente, incluso en relación con los conjuntos de datos, procesos y decisiones tomadas durante el ciclo de vida del sistema de IA. Así será posible analizar correctamente, y en consonancia con el estado del arte, sus resultados y respuestas a las preguntas que se les formulen. (iV) En función de sus labores, del contexto y de su capacidad de actuación, los actores de la IA deben aplicar continuamente un enfoque sistemático de gestión de riesgos en cada fase del ciclo de vida del sistema para abordarlos de la mejor manera, incluyendo los relativos a la privacidad, seguridad digital y sesgos.[6]

Para la gobernanza de datos es especialmente importante el desarrollo de lineamientos técnicos de uso transversal que establezca un estándar de trabajo para todos los casos de uso, para ello se recomienda el uso de recursos publicados dentro del documento "*Uso responsable de IA para política pública: manual de formulación de proyectos"*[7] y el documento *"Uso responsable de la IA para las políticas públicas: manual de ciencia de datos".*[8]

E. Rendición de cuentas

Finalmente, el quinto principio establece que los actores deben ser responsables del buen funcionamiento de los sistemas de IA y del respeto por los principios antes mencionados, en función de sus deberes, del contexto y del estado del arte.[9]

Para fines de la iniciativa es necesario que los usuarios tengan claridad de dónde, cómo y en qué tiempo sus datos serán usados, además de asegurarse que existe una comprensión de quién es

---

[6] Ibid.

[7] Banco Interamericano de Desarrollo, Denis, Gabriela; Hermosilla, María; Aracena, Claudio; Sánchez Ávalos, Roberto; González Alarcón, Natalia; Pombo, Cristina, Uso responsable de IA para política pública: manual de formulación de proyectos, septiembre del 2021, en http://dx.doi.org/10.18235/0003631

[8] Banco Interamericano de Desarrollo, Sánchez Ávalos, Roberto; González, Felipe; Ortiz, Teresa, Uso responsable de la IA para las políticas públicas: manual de ciencia de datos, octubre del 2021, en http://dx.doi.org/10.18235/0002876

[9] Banco Interamericano de Desarrollo, Pombo, Cristina; Cabrol, Marcelo; González Alarcón, Natalia; Sánchez Ávalos, Roberto, fAIr LAC: Adopción ética y responsable de la inteligencia artificial en América Latina y el Caribe, enero del 2020, en http://dx.doi.org/10.18235/0002169

responsable de su buen funcionamiento, quien ejecutaría las respuestas en caso de riesgo y qué mecanismos están a su alcance tanto para la vigilancia del buen uso de sus datos y como para el buen funcionamiento de los sistemas.

Anexo II. Matriz no-exhaustiva regulatoria Gobernanza de Datos – referencia internacional

Instrumento	Disposiciones relevantes
DATA ETHICS DECISION AID (DEDA): A DIALOGICAL FRAMEWORK FOR ETHICAL INQUIRY OF AI AND DATA PROJECTS IN THE NETHERLANDS (2021, University of Utrecht, University of Duisburg, Países Bajos) https://link.springer.com/article/10.1007/s10676-020-09577-5	Este documento contempla la discusión sobre el *Data Ethics Decision Aid* (DEDA), un marco referencial para revisar proyectos de datos de gobierno que consideran el impacto social, los valores involucrados y las responsabilidades del gobierno en la gestión pública basada en datos. DEDA es un proceso efectivo para moderar la deliberación del caso y promover el desarrollo de prácticas de los datos responsables. Adicionalmente, al documentar el proceso de deliberación, DEDA incluye la rendición de cuentas. En primer lugar, este artículo arroja luz sobre la necesidad de una deliberación ética de casos de datos. En segundo lugar, describe los prototipos, el diseño final del marco y su evaluación. Después de una comparación con otros marcos y una discusión de los hallazgos, el documento concluye argumentando que el marco DEDA es un proceso útil para la evaluación ética de proyectos de datos para la gestión pública y una herramienta eficaz para crear conciencia sobre cuestiones éticas en las prácticas de datos.
OPEN LETTER: CIVIL SOCIETY CALL FOR THE INTRODUCTION OF RED LINES IN THE UPCOMING EUROPEAN COMMISSION PROPOSAL ON ARTIFICIAL INTELLIGENCE (2021, European Digital Rights (EDRi), Belgica) https://edri.org/wp-content/uploads/2021/01/EDRi-open-letter-AI-red-lines.pdf	Este grupo miembro de la comunidad civil envió comunicado a la Comisión Europea para solicitar que la propuesta regulatoria sobre IA estableciera limitaciones claras en cuanto a lo que puede considerarse como usos lícitos de la IA, particularmente menciona los siguientes problemas: ● Permitir la vigilancia y vigilancia de biométricos recolectados en espacios públicos; ● La exacerbación de la discriminación estructural, la exclusión y los daños colectivos; ● La restricción y el acceso discriminatorio a servicios vitales como la atención médica y social seguridad; ● La vigilancia de los trabajadores y la vulneración de los derechos fundamentales de los trabajadores; ● El impedimento del acceso equitativo a la justicia y los derechos procesales; ● El uso de sistemas que hacen inferencias y predicciones sobre nuestras características más sensibles, comportamientos y pensamientos; y, ● La manipulación o el control del comportamiento humano y las amenazas asociadas a la dignidad humana, organización y democracia colectiva.

FEASIBILITY STUDY ON A LEGAL FRAMEWORK ON AI DESIGN, DEVELOPMENT AND APPLICATION BASED ON COE STANDARDS (2021, Council of Europe) https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da	En este documento se resalta la necesidad de contar con una definición sobre IA, de tal manera que se aborde el tema de manera tecnológicamente neutral (es decir independientemente de la tecnología subyacente) Además, se debe buscar un equilibrio entre una definición que puede ser demasiado precisa desde un punto de vista técnico y, por lo tanto, podría ser obsoleta en el corto plazo, y una definición que es demasiado vaga y por lo tanto deja un amplio margen de interpretación, potencialmente resultando en una aplicación no uniforme del marco legal. Es posible que sea necesario perfeccionar la definición a la luz de la forma y el alcance de un posible instrumento jurídico, para identificar qué tipo de comportamiento humano se pone en la mira para el procesamiento a través de algoritmos. Reflexión sobre regulación sobre datos El Convenio 108, establece estándares globales sobre el derecho a la privacidad y protección de datos de las personas, independientemente de las evoluciones tecnológicas. En particular, requiere que el procesamiento de categorías especiales de datos (datos sensibles) sólo se permita cuando las salvaguardias apropiadas están consagradas en la ley, complementando las de la Convención, y crea un derecho para que todos sepan que sus datos personales son tratados y con qué finalidad, con derecho de rectificación. El convenio fue modificado y se agregaron nuevos principios, tales como transparencia (artículo 8), proporcionalidad (artículo 5), responsabilidad (artículo 10), impacto evaluaciones (artículo 10) y respeto de la privacidad desde el diseño (artículo 10). Adicionalmente se agregó el derecho a no estar sujeto a una decisión que afecte significativamente basada únicamente en un procesamiento automatizado de datos sin que se tomen en consideración sus opiniones, y el derecho a obtener conocimiento del razonamiento subyacente al procesamiento de datos, donde se aplican los resultados del procesamiento (artículo 9). Estos nuevos derechos son de particular importancia en relación con la elaboración de perfiles de personas y toma de decisiones automatizada. Si bien el Convenio no aplica específicamente a las aplicaciones de la IA, el marco jurídico creado en torno al Convenio sigue siendo plenamente aplicable a la tecnología de IA tan pronto como los datos procesados entren dentro del ámbito de la Convención. Un instrumento legal del Consejo de Europa sobre aplicaciones de IA por tanto, tendría que tener plenamente en cuenta este acervo para complementarlo (es decir, centrarse en las lagunas pendientes de

	protección), por ejemplo, al incluir en su alcance operaciones de procesamiento que no solo involucran datos, ampliando su alcance a la prevención de daños a otros derechos humanos, e incluir daño a la colectividad y no solo a nivel individual. El Consejo de Europa trabaja en otros campos de aplicación de IA, tales como: - Cibercrimen: se encuentra en preparación un nuevo protocolo de modificación a la Convención de Budapest. - Sistemas algorítmicos: En 2020 adoptaron la Recomendación sobre el impacto de sistemas algorítmicos en los Derechos Humanos. Actualmente preparan recomendaciones sobre las dimensiones de los derechos humanos en el tratamiento automatizado de los datos y la rendición de cuentas, así como los impactos de la tecnología y el derecho de expresión. - Impartición de justicia: En 2018, aprobaron el Capítulo Etico Europeo para el uso de IA en el ámbito judicial basado en 5 principios: no discriminación, calidad y seguridad, transparencia, imparcialidad y equidad. Actualmente se revisa la posibilidad de solicitar una certificación para productos que se utilizarán para sistemas de impartición de justicia. - Buen gobierno y elecciones: se está preparando un estudio sobre el impacto en la transformación digital, incluyendo IA en la democracia y gobernanza. El estudio se refiere al impacto de IA en las elecciones, participación ciudadana y supervisión democrática. - Equidad de género y no discriminación: se emitió una recomendación para que se integrará una perspectiva de genero en todas las políticas, programas e investigación relacionada con IA para evitar riesgos potenciales sobre estereotipos de genero y por otro lado examinar como IA pudiera ayudar a eliminar esos sesgos. - Educación y cultura: actualmente se está explorando las implicaciones en IA y otras tecnologías emergentes para la educación en general y más específico sobre su uso en la educación. - Derechos Humanos: En 2019, se emitió la Recomendación con 10 medidas para proteger los derechos humanos para las autoridades en las siguientes áreas: evaluación del impacto en los derechos humanos; consultas públicas; estándares sobre derechos humanos en el sector privado; información y transparencia; evaluación independiente; no discriminación e igualdad; protección de datos y privacidad; libertad de expresión, libertad de reunión y asociación, y el derecho al trabajo; vías de reparación del daño; y promover el conocimiento y la comprensión de la IA.

	La Comisión Europea anunció la elaboración de una propuesta legislativa para atender los retos para garantizar una IA fiable, más información aquí. Por otro lado, se han desarrollado Guías Éticas de empresas, academia, sector público, denominados como *soft law*. Las cuales son útiles para ejercer influencia en las decisiones de política pública sobre IA. Este tipo de instrumentos debe percibirse como auxiliar en el ejercicio del poder público sobre todo cuando existan diferentes actores involucrados y pudieran presentarse efectos negativos en los derechos humanos o la democracia, es decir, no pueden sustituir las atribuciones de gobernanza del Estado.
AI IMPACT ASSESSMENT: A POLICY PROTOTYPING EXPERIMENT (2021, OPEN LOOP, Multisectorial) https://d32j3j47emgb6f.cloudfront.net/wp-content/uploads/2021/01/AI_Impact_Assessment_A_Policy_Prototyping_Experiment.pdf	Facebook se asoció con 10 empresas europeas de inteligencia artificial para crear un marco ADIA (prototipo de política) que esas empresas podrían probar aplicándolo a sus propias aplicaciones de IA. El prototipo de política se estructuró en dos partes: la ley prototipo (redactada como texto legal) y la guía de prototipos (redactada como un toolkit).
OVERVIEW OF NATIONAL AI-STRATEGIES (2021, AISOMA, Alemania) https://www.aisoma.de/wp-content/uploads/2021/01/Overview-of-National-AI-Strategies.pdf	El documento contempla las políticas sobre Inteligencia Artificial desarrolladas en 53 naciones, identificando su avance en la implementación así como su enfoque en la transformación gubernamental.
GOVERNMENT BY ALGORITHM: ARTIFICIAL INTELLIGENCE IN FEDERAL ADMINISTRATIVE AGENCIES (2020, STANFORD LAW SCHOOL, USA) https://law.stanford.edu/education/only-at-sls/law-policy-lab/practicums-2018-2019/administering-by-algorithm-artificial-int	El estudio señala que los rápidos desarrollos en IA tienen el potencial de reducir el costo de las funciones centrales del sector público, mejorar la calidad de las decisiones y liberar el poder de los datos administrativos, haciendo así el desempeño del gobierno más eficiente y efectivo. Al mismo tiempo se enfrentarán retos, tales como: el diseño adecuado de algoritmos e interfaces de usuario, el alcance respectivo de la toma de decisiones humana y mecánica.

elligence-in-the-regulatory-state/acus-report-for-administering-by-algorithm-artificial-intelligence-in-the-regulatory-state/	Se concluye que la academia está enfocada en cómo regula el uso de IA, y ha dedicado poco análisis a la forma en que el gobierno adquiere esas herramientas y cómo las supervisa. Actualmente ya se han puesto en marcha herramientas que están mejorando las operaciones de las instituciones de las agencias de gobierno, en tareas como: - Cumplimiento de normativas sobre eficiencia de mercado, seguridad, salud, protección ambiental. - Adjudicación de beneficios y privilegios desde deshabilitación de beneficios a derechos de PI. - Monitorear riesgos sobre salud y seguridad pública. - Extraer información de forma masiva sobre quejas de consumidores y patrones del clima. - Comunicación con el público sobre sus derechos y obligaciones, dueños de negocios, asilos, contribuyentes y beneficencia. Se ha identificado que no todos los sistemas explican de manera concreta cómo se llegó a determinada decisión. Sin embargo, esta explicación debería estar asociada al tipo de decisión, pues tratándose de tareas de investigación, no sería conveniente difundir al mismo detalle en el que se haría cuando se está entregando un beneficio o retirando alguno. Para lograr una rendición de cuentas significativa, concreta y favorecer conocimiento técnicamente informado dentro y entre contextos, debe evitarse la prohibición o la fe ciega en la innovación. Un despliegue pobre gubernamental de herramientas IA puede provocar pocos beneficios, aumentar la brecha entre la tecnología privada y pública, aumentar la opacidad en la toma de decisiones públicas y aumentar las preocupaciones sobre acciones arbitrarias del gobierno. Focaliza la recomendación en buscar mecanismos para fomentar el uso de herramientas adecuadas de IA para los procesos de gobierno respectivos, poniendo énfasis en la forma de adquisición de estas herramientas y generar mecanismos de rendición de cuentas al respecto.
FEASIBILITY STUDY ON THE ESTABLISHMENT OF A CERTIFICATION MECHANISM FOR ARTIFICIAL INTELLIGENCE TOOLS AND SERVICES (2020, Council of Europe (CEPEJ)	El estudio concluye que algunos campos del derecho son más sensibles que otros, debido a la diversidad de los supuestos en donde pudiera presentarse una decisión judicial sobre las libertades personales. Criminología y derecho penal son los campos donde se prevé que el uso de inteligencia artificial deba realizarse con la mayor precaución y cuidado. La certificación de inteligencia artificial conexionista se puede realizar a diferentes niveles: en el modelo de aprendizaje (supervisado o no,

https://rm.coe.int/feasability-study-en-cepej-2020-15/1680a0adf4	validez científica del protocolo y los sesgos de aprendizaje), a nivel de los datos utilizado (validez del elemento de datos, protección de la base de datos y exclusión de ciertos datos sensibles) y en el nivel de los resultados (impacto adverso en los derechos y libertades fundamentales).
REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos) (2020, Comisión Europea) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020SC0296&from=ES	Objetivo: ampliar la disponibilidad de datos con miras a su utilización, mediante el aumento de la confianza en los intermediarios de datos y el refuerzo de los mecanismos para el intercambio de datos en el conjunto de la UE. Regula: ● La cesión de datos del sector público para su reutilización, en los casos en que esos datos estén sujetos a derechos de terceros (datos que puedan estar sujetos a la legislación sobre protección de datos o sobre propiedad intelectual, o que puedan contener secretos comerciales u otra información sensible a efectos comerciales). ● El intercambio de datos entre empresas a cambio de algún tipo de remuneración. ● La cesión de datos personales con ayuda de un «intermediario de datos personales», cuya labor consistirá en ayudar a los particulares a ejercer los derechos que les confiere el Reglamento General de Protección de Datos (RGPD). ● La cesión de datos con fines altruistas.
ASSESSMENT LIST FOR TRUSTWORTHY ARTIFICIAL INTELLIGENCE (ALTAI) FOR SELF-ASSESSMENT (2020, EUROPEAN COMMISSION (AI HLEG) https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment	A través de la Lista de evaluación para la IA confiable (ALTAI), se traducen los principios de la IA en una lista de verificación accesible y dinámica que guía a los desarrolladores e implementadores de IA en la implementación de dichos principios en la práctica. ALTAI ayuda a garantizar que los usuarios se beneficien de la IA sin estar expuestos a riesgos innecesarios al indicar un conjunto de pasos concretos para la autoevaluación.
LIABILITY FOR ARTIFICIAL INTELLIGENCE AND OTHER EMERGING DIGITAL TECHNOLOGIES	Por lo general, cuando existe una afectación de los derechos y por lo tanto una posible compensación, esta se exige conforme a los regímenes de responsabilidad bajo derecho privado, en particular

(2020, European Commission (Expert group on liability and new technologies) https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199	derecho de responsabilidad civil, posiblemente en combinación con seguros. Solo la responsabilidad objetiva de los productores por productos defectuosos, que constituye una pequeña parte de este tipo de responsabilidad, está armonizado a nivel de la UE por la Directiva sobre responsabilidad por productos, mientras que todos los demás regímenes - salvo algunas excepciones en sectores específicos o bajo legislación especial - están regulados por los propios Estados miembros. Hasta ahora se ha concluido que con la normativa existente, existe una protección básica para las víctimas que han sufrido daños causados por la operación de las nuevas tecnologías. Sin embargo, las características específicas de estas tecnologías, incluyendo su complejidad, autoaprendizaje durante la operación, predictibilidad y vulnerabilidad a ciberataques hace más difícil ofrecer a las víctimas compensación en todos los casos donde parece estar justificado. Por lo tanto, deben realizarse ciertos ajustes a los regímenes de responsabilidad y en función de ello establece los siguientes criterios: - En función del daño que pudiera provocar debería establecerse una responsabilidad por su funcionamiento. - Debería determinarse quién es el responsable en función del control que tiene sobre la operación del mismo (desarrollador, implementador o usuario) - En aquellos casos donde pudieran no existir riesgo de daño, aún debiera cumplir con los deberes de seleccionar, operar, monitorear y mantener adecuadamente la tecnología en uso y, en su defecto, debe ser responsable del incumplimiento de dichos deberes si tiene la culpa. - Una persona que utiliza una tecnología que tiene un cierto grado de autonomía no debe ser menos responsable del daño resultante que si dicho daño hubiera sido causado por un auxiliar humano - Los fabricantes de productos o contenido digital que incorporan tecnología digital emergente deben ser responsable de los daños causados por defectos en sus productos, incluso si el defecto fue causado por cambios realizados en el producto bajo el control del productor después de haber sido colocado en el mercado. - Para situaciones que exponen a terceros a un mayor riesgo de daño, el seguro de responsabilidad obligatorio podría brindar a las víctimas un mejor acceso a la compensación. - Cuando una tecnología en particular contempla dificultades para probar la existencia de un elemento de responsabilidad más allá de lo que se puede esperar razonablemente, las víctimas deben tener derecho a que se les facilite la prueba.

	- Las tecnologías digitales emergentes deben integrar registros, según las circunstancias, y la falta de registro, o de proporcionar un acceso razonable a los datos registrados, debe dar lugar a una inversión de la carga de la prueba para no perjudicar a la víctima. - La destrucción de los datos de la víctima debe considerarse un daño, indemnizable en condiciones específicas. - No es necesario dotar a los dispositivos o sistemas autónomos de personalidad jurídica, ya que el daño siempre debe ser atribuible a personas u organismos existentes.
WHITE PAPER ON AI STANDARDIZATION (2020, CHINA ELECTRONICS STANDARDIZATION INSTITUTE, CHINA) https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-excerpts-chinas-white-paper-artificial-intelligence-standardization/	Los reguladores deben considerar cuestiones éticas y garantizar que las tecnologías de IA y sus aplicaciones cumplan con los requisitos éticos para lograr realmente la seguridad pública. Es necesario garantizar que los objetivos de diseño de la IA sean coherentes con los intereses, la ética y la moral de la mayoría de los seres humanos. Es necesario considerar cuestiones de responsabilidad y fallas en el proceso de desarrollo e implementación de la IA. Estableciendo contenido específico de derechos y obligaciones para los desarrolladores de tecnología de inteligencia artificial, fabricantes de productos o proveedores de servicios y usuarios finales, se logrará el objetivo de implementar requisitos de garantía de seguridad. China considera necesario establecer un estándar de la industria de IA y diseñar y mejorar estándares técnicos como fundamentos comunes, interoperabilidad, seguridad y privacidad, y aplicaciones industriales, y al mismo tiempo, construir sistemas de evaluación de productos de IA.
ETHICAL FRAMEWORK FOR ARTIFICIAL INTELLIGENCE IN COLOMBIA (2020, Presidential advisory for economic affairs and digital transformation, Colombia) https://mycloud.coe.int/s/FFEMLg884J6W3na	Modelos de gobernanza para asegurar la ética de la inteligencia artificial 1. Adaptar estructuras de gobernanza internas y medidas para incorporar valores, riesgos y responsabilidades relacionadas con la toma algorítmica de decisiones 2. Determinar el nivel de involucramiento humano en la toma de decisiones 3. Gestión de operaciones: considerando elementos de desarrollo, selección y mantenimiento de modelos de IA Estrategias para comunicarse e interactuar con los stakeholders de una organización y el manejo de las relaciones con ellos.

REVIEW INTO BIAS IN ALGORITHMIC DECISION-MAKING (2020, CENTRE FOR DATA ETHICS AND INNOVATION, UK) https://www.gov.uk/government/publications/cdei-publishes-review-into-bias-in-algorithmic-decision-making?utm_source=POLITICO.EU&utm_campaign=4a2811137a-EMAIL_CAMPAIGN_2020_12_02_09_59&utm_medium=email&utm_term=0_10959edeb5-4a2811137a-190482161	Este estudio considera el impacto del uso de herramientas algorítmicas y los sesgos en la toma de decisiones, los pasos que se requieren para gestionar los riesgos y las oportunidades que un mejor uso de los datos ofrece para mejorar la justicia. El punto de partida obvio es garantizar que los algoritmos sean confiables y para ello identificaron un número de pasos concretos para que la industria, los reguladores y el gobierno puedan respaldar la innovación ética en una amplia variedad de casos de uso. No es un manual de orientación, pero considera orientación, apoyo, regulación e incentivos que se necesitan para generar condiciones adecuadas para la innovación justa. Las organizaciones tienen un nivel de entendimiento sobre lo que consideran debida diligencia y justicia, el reto es trasladar este entendimiento al mundo del algoritmo y aplicar un estándar coherente de justicia ya sea en decisiones hechas por humanos, algoritmos o la combinación de estos. Los sectores estudiados fueron: reclutamiento, servicios financieros, gobierno local, vigilancia policial. Gobierno local: La evidencia ha demostrado que ciertas personas puede que estén sobrerrepresentados en los datos en poder de autoridades y esto puede conducir a sesgos en las predicciones e intervenciones. Un problema relacionado ocurre cuando el El número de personas dentro de un subgrupo es pequeño. Las generalizaciones pueden resultar en tasas altas de error entre grupos minoritarios. Detectaron que la infraestructura de datos y la calidad de los datos fueron barreras significativas para el desarrollo e implementación de herramientas basadas en datos de manera efectiva y responsable. Es necesario invertir en esta área antes de desarrollar más sistemas avanzados. Recomendación: debe desarrollarse una guía nacional para ayudar a las autoridades locales para que legalmente adquieran o desarrollen herramientas algorítmicas éticas para la toma de decisiones en áreas donde se toman decisiones importantes sobre las personas, incluyendo los aspectos para monitorear el cumplimiento de esa guía. Se tiene una creencia incorrecta que la ley de protección de datos impide la recopilación o el uso de datos protegidos. La recolección de datos sigue siendo un desafío y se necesita pensar en el potencial por ejemplo de terceros intermediarios de confianza.
RECOMMENDATION CM/REC(2020)1 OF THE	Se deben adoptar modelos de gobernanza flexibles que garanticen una reparación rápida y eficaz y posibilidades de reparación cuando ocurran

COMMITTEE OF MINISTERS TO MEMBER STATES ON THE HUMAN RIGHTS IMPACTS OF ALGORITHMIC SYSTEMS (2020, Committee of Ministers to member States) https://rm.coe.int/0900001680 9e1154	los incidentes, asegurando que la responsabilidad y la rendición de cuentas para la protección de los derechos humanos se distribuyan de manera efectiva y clara en todas las etapas del proceso, desde la etapa de propuesta hasta la identificación de tareas, selección de datos, recopilación y análisis, modelado y diseño de sistemas, hasta la implementación continua, revisión y supervisión por las autoridades.
MODEL ARTIFICIAL INTELLIGENCE GOVERNANCE FRAMEWORK SECOND EDITION (2020, PERSONAL DATA PROTECTION COMMISION, SINGAPORE) https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf	Los intermediarios tienen la obligación de cumplir con la normativa relacionada con la protección de datos Un intermediario de datos debe tomar medidas razonables de seguridad para proteger datos personales de accesos no autorizados, acceso, uso, revelación o cualquier riesgo similar, incluso cuando esté procesando datos personales en nombre de otra organización. El tipo de medidas dependerá de varios factores tales como: - La naturaleza del dato - La forma en que ha sido recolectado, y - El posible impacto en caso de que los datos queden en manos equivocadas Por ejemplo, datos financieros o médicos pueden requerir medidas de seguridad más robustas en comparación con información sobre la experiencia profesional o educación de una persona. Las organizaciones deberían diseñar sus medidas de seguridad en función de la naturaleza de los datos que poseen y tratan y el posible daño que podría causar en caso de presentarse una brecha de seguridad. Adicionalmente deberían contar con un plan de incidentes así como políticas y procedimientos robustos para asegurar niveles de seguridad apropiados derivados de la sensibilidad de los datos. Todos los intermediarios están obligados a comprometerse con la Retención Limitada de acuerdo con sus disposiciones normativas de protección de datos personales de Singapur. Esto significa que deberán dejar de retener documentos que contiene datos personales o remover los mecanismos a través de los cuales se pudiera asociar los datos personales a personas específicas cuando ya se haya cumplido el propósito para lo cual el dato fue recolectado y por tanto ya no es necesario conservarlo por disposiciones legales o cuestiones de negocio.

	Los intermediarios deberán revisar los datos de manera regular para determinar si aún es necesario mantener el dato. Las organizaciones en todo caso siguen siendo responsables para responder por los datos personales que están siendo procesados por intermediarios. En todo caso, deberán establecer en los respectivos contratos, provisiones claras sobre las responsabilidades de los intermediarios, así como sus obligaciones para asegurar el cumplimiento de las disposiciones normativas sobre la protección de datos. Los intermediarios que procesan datos a nombre de otra organización, deben asegurar que cumplen con la seguridad y la obligación de retención limitada con respecto a los datos que manejan a nombre de sus clientes. Así como cualquier requisito de protección de datos establecido en el contrato. Deberán desarrollar una cultura organizacional mediante la cual se adopten medidas razonables para proteger datos personales de terceros, así como remover, o anonimizar después de que ya no sea necesario seguir conservando el dato. Un intermediario de datos es totalmente responsable bajo la normativa de protección de datos personales aún y cuando no esté procesando datos en nombre de otra organización. Por lo tanto, le aplican las disposiciones sobre la recolección de datos personales, así como sobre su tratamiento
RECOMENDACIONES GENERALES PARA EL TRATAMIENTO DE DATOS EN LA INTELIGENCIA ARTIFICIAL (2019, RED IBEROAMERICANA DE PROTECCIÓN DE DATOS) https://www.redipd.org/sites/default/files/2020-02/guia-recomendaciones-generales-tratamiento-datos-ia.pdf	Aprobó los Principios y recomendaciones para el tratamiento de datos personales en la inteligencia artificial, donde se establecieron un conjunto de criterios y orientaciones para que sean tomados en cuenta, desde el punto de vista de la privacidad, por parte de los promotores de esta nueva tecnología. La Red consideró que cuando un software, producto o dispositivo de IA integra en alguna de sus funcionalidades datos personales, es relevante que los desarrolladores de estas soluciones tecnológicas observen el marco legal nacional, así como los principios y derechos establecidos en instrumentos internacionales. De acuerdo con las reflexiones realizadas por la Red, el marco legal no se opone al tratamiento de datos personales con IA, toda vez que dicho marco legal ya protege los intereses de los titulares de los datos personales exigiendo garantías para evitar cualquier abuso que pueda generar una amenaza o vulneración de los derechos que asisten a los titulares de los datos. Por ello, desarrolló una serie de recomendaciones para aquellos actores que desarrollan productos de IA para que desde el diseño y su posterior construcción se tengan en cuenta las exigencias de las regulaciones sobre el tratamiento de datos personales, haciendo

	especial énfasis que únicamente serán aplicables a ese tipo de información (datos personales) y no a cualquier información en general: - Cumplir con las normas locales sobre tratamiento de datos personales; - Efectuar estudios de impacto de privacidad; - Incorporar la privacidad, la ética y la seguridad desde el diseño y por defecto; - Materializar el principio de responsabilidad demostrada; - Diseñar esquemas apropiados de gobernanza sobre tratamiento de datos personales en las organizaciones que desarrollen productos de IA; - Respetar los derechos de los titulares de los datos e implementar mecanismos efectivos para el ejercicio de los mismos; - Asegurar la calidad de los datos; - Utilizar herramientas de anonimización; e - Incrementar la confianza y la transparencia con los titulares de los datos personales.
DATA TRUSTS: LEGAL AND GOVERNANCE CONSIDERATIONS (2019, UNIVERSITY OF LONDON) https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf	Intermediarios de Datos Este estudio señala que la ley de fideicomisos no es una estructura legal adecuada para los fideicomisos de datos. Pero el concepto fundamental subyacente, es que existen administradores de los datos que deben ser responsables de la supervisión adecuada de su intercambio y uso. Esta función se puede lograr a través de diferentes estructuras legales, como por ejemplo una estructura corporativa y una estructura contractual estableciendo obligaciones a los administradores de datos. En el futuro pudiera existir un ente público que pudiera vigilar las actividades de estos intermediarios de datos, pero en el presente no se visualiza un ente que pudiera ejecutar dichas acciones.
AI AND BIG DATA: A BLUEPRINT FOR A HUMAN RIGHTS, SOCIAL AND ETHICAL IMPACT ASSESSMENT (2018, Italy, Polytechnic University of Turin) https://doi.org/10.1016/j.clsr.2018.05.017	Modelos de Evaluación de Riesgos Se basa en un Modelo de evaluación centrado en los derechos humanos. Este modelo de autoevaluación pretende superar las limitaciones de los modelos de evaluación existentes, que están demasiado centrados en el procesamiento de datos o tienen una extensión y granularidad que los hacen demasiado complicados para evaluar las consecuencias de un uso determinado de los datos. En términos de arquitectura, la HRESIA tiene dos elementos principales: un cuestionario de autoevaluación y un comité de expertos ad hoc. Como anteproyecto, esta contribución se centra principalmente en la naturaleza del modelo propuesto, su arquitectura y sus desafíos.

	El Modelo se centra en sectores y no en tecnologías, se enfoca en los derechos y valores involucrados.
EUROPEAN ETHICAL CHARTER ON THE USE OF ARTIFICIAL INTELLIGENCE IN JUDICIAL SYSTEMS AND THEIR ENVIRONMENT (2018, Council of Europe (CEPEJ) https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c	Destaca la redefinición de la noción de Datos Abiertos, no es lo mismo tener acceso a la información que acceso a los datos (en la forma de bases de datos) que pueden ser descargados y procesados computacionalmente. Por lo tanto, los datos abiertos solo implican la difusión de datos "brutos" en bases de datos informáticas estructuradas. Estos datos, agregados en conjunto o en parte a otras bases estructuradas, constituyen lo que se llama *Big Data*. Cuando se habla de protección de datos, no solo involucra volumen, velocidad y variedad del procesamiento de datos sino también el análisis de los datos mediante software que permite extraer conocimiento nuevo y predictivo para la toma de decisiones. Datos Abiertos no debe confundirse con los métodos con los que se procesa, lo que comúnmente se denomina ciencia de datos. Usar IA para la justicia predictiva, buscados sofisticados y precisos así como robots legales son todos algoritmos aplicados que se alimentan de los datos pero no tienen nada que ver con la política de Datos Abiertos por si misma. Existe una dificultad real para medir el impacto de Datos Abiertos en la eficiencia y calidad de la justicia. Actualmente la iniciativa para reusar los datos es esencialmente privada, para departamentos legales y probablemente no sean los mejores medios para identificar resultados positivos. Aún no hay consenso sobre lo que debería publicarse, por ejemplo, Francis pública todo salvo aquellos que por ley en función de la privacidad de las personas involucradas. Y en ciertos casos se publican una vez que se haya hecho un análisis de riesgo sobre la re-identificación de las personas involucradas en algunas decisiones judiciales o administrativas.

Anexo III: Mecanismos multisectoriales existentes para la transferencia de datos entre instituciones.

Si bien la gobernanza cívica de datos multisectorial es de suma importancia para avanzar en el uso óptimo de la IA para el bien social, se encuentra en una etapa muy temprana y la mayoría de las propuestas de solución aún requieren de mayor adopción para formar un estándar de común acuerdo. Por ello, algunas de las definiciones encontradas en literatura de diversas instituciones líderes en el tema aquí presentadas podrían volverse obsoletas o considerarse imprecisas en un futuro cercano.

A) Sistemas tradicionales de análisis de datos

En este documento se ha dejado fuera el análisis de algunos métodos y sistemas de agregación de información debido a que su naturaleza es agnóstica a los mecanismos de gobernanza de las organizaciones y proveen poco valor agregado a una colaboración multi-actor que busque compartir datos de forma confiable, responsable y en cumplimiento a la regulación de tratamiento de datos.

La mayoría de estos métodos y sistemas de agregación de información han sido diseñados para la iniciativa privada con la intención de resolver sus necesidades en temas de compartición, análisis y procesamiento de datos como actividad interna y privada. A su vez, cuando se habla de gobernanza de datos, se construyen procesos y estructuras jerárquicas encima de estos sistemas para supervisar y asegurar su correcta operación. Las tecnologías que se han dejado fuera de este análisis debido a no contar con mecanismos de gobernanza dentro de su implementación base se describen en el siguiente listado:

- *Data Lake*
  Repositorio centralizado que permite almacenar todo tipo de información (estructurada o no estructurada) en su formato actual (sin un formato estándar) en cualquier escala. Esta infraestructura está diseñada para el análisis de grandes cantidades de datos sin requerir de un diseño previo de la estructura de datos, es decir más ágilmente.
- *Data Pool*
  Repositorio de datos compartido que permite el intercambio de datos en un formato estandarizado en una arquitectura que conecta múltiples bases de datos de forma centralizada y mantiene a múltiples actores sincronizados con actualizaciones de información. Utilizado comúnmente en ambientes corporativos para la automatización de reportes entre sistemas independientes.
- *Data Warehouse*
  Un *data warehouse* es un sistema que agrega y combina información de diferentes fuentes en un almacén de datos único y centralizado; consistente para respaldar el análisis empresarial, la minería de datos, IA y *Machine Learning*. El *data warehouse* permite

a una organización o empresa ejecutar análisis potentes en grandes volúmenes (e.g, petabytes) de datos históricos de formas que una base de datos estándar no puede.

- *Data Commons*
  Repositorio de datos enfocado en integrar bases de datos de acceso público con una estructura común para facilitar el uso para universidades y centros de investigación.
- *Data Sandbox*
  Ambiente escalable que permite a científicos de datos contar con infraestructura tecnológica para experimentar con los datos de una organización de forma segura y separada de un ambiente productivo. Usualmente está integrado por un servidor con software que permite el acceso a copias de bases de datos (en algunos casos anonimizadas o pseudo-anonimizadas) y recursos computacionales suficientes para desarrollar modelos y algoritmos con base en ellas.

A continuación se muestra una tabla que analiza cada uno de los sistemas previamente descritos y su relación con los elementos básicos de un mecanismo de gobernanza; justificando el razonamiento de dejarlos fuera de este análisis.

Tecnología	¿Reglas de uso de datos?	¿Responsabilidades?	¿Vigilancia de uso?
Data Lake	No	No	No
Data Pool	Sólo estructura	No	No
Data Warehouse	No	No	No
Data Commons	No	No	Sí, opcional
Data Sandbox	No	No	No

B) Intermediarios de datos de confianza (*Trusted Data Intermediaries/TDI*)

El primer mecanismo analizado consiste en una implementación es su mayoría tecnológica que propone la integración de nuevos componentes de software de un intermediario que administra los datos dentro de los dispositivos de los usuarios y permite a terceros la ejecución de *software* para el uso de esos mismos datos, sin el envío explícito de esa información a las bases de datos del tercero[10]. Este modelo, denominado *Trusted Data Intermediaries* (TDI) es útil para ser compatible con la forma en que la mayoría de los productos digitales obtienen datos de los usuarios, sin embargo, se requieren cambios importantes al software no sólo de los dispositivos de los usuarios (probablemente a nivel sistema operativo), sino también en todos los productos digitales que pretendan proveer compatibilidad con este modelo, ya que estos tendrán que

[10] Fuente: iapp.org/news/a/the-trusted-intermediary-model-supporting-both-privacy-and-internet-services/

construir *software* que se ejecute en dentro del *software* del intermediario para evitar que los datos lleguen a sus bases de datos[11]. Algunas de las ventajas de este modelo son las siguientes:

- Para los usuarios:
    - Sus datos sólo se comparten con el o los intermediarios que elija.
    - Sólo administran sus datos y sus configuraciones de privacidad con una o unas cuantas entidades. Reduciendo considerablemente la inversión de tiempo en temas de consenso y conciencia de uso de datos por terceros.
    - Manejo más granular y ágil sobre el uso de sus datos, incluyendo formas para retirar el uso a terceros de forma confiable y fácil.
    - Potencial creación de nuevos productos o servicios digitales que se construyan sobre este modelo. Por ejemplo, servicios altamente intrusivos en la privacidad que actualmente no serían viables debido a la desconfianza del público en actores públicos y privados.
    - Abre la posibilidad a nuevos modelos de ingresos compartidos entre el intermediario y el usuario a partir de las ganancias de uso de los datos por terceros.
- Para el tercero proveedor de productos o servicios digitales:
    - Menor carga legal respecto al uso de datos personales, esto al reducir el esfuerzo necesario para el cumplimiento de leyes y regulación en el tratamiento de datos personales, así como el riesgo a multas o demandas por estas problemáticas.
    - Reducción de costos tecnológicos respecto a los mecanismos e infraestructura necesarios para administrar datos correctamente.

En contraste, entre algunas de las áreas de oportunidad para este modelo se encuentran:

- Para los usuarios:
    - Posiblemente tendrá que absorber los costos de operación del intermediario de una forma u otra. Agregando, adicionalmente, la complejidad de seleccionar un intermediario dentro de sus posibilidades y preferencias.
    - El software de sus dispositivos se hará más complejo y propenso a fallos.

[11] Otra posible implementación es el uso de un sistema configurable provisto por el intermediario que, sin la necesidad de la ejecución de código personalizado, permita al tercero la utilización de los datos de forma privada. Por ejemplo, el tercero configura cómo desea usar los datos del usuario para mostrar publicidad y el usuario decide qué datos se usan, cómo y en qué casos.

- No todos los productos y servicios que utilice podrán migrar a un modelo así debido a su alta dependencia en el uso interno de datos de sus usuarios.

- Para el tercero:
  - Mayor complejidad técnica y limitaciones sobre las funcionalidades de su producto o servicio digital. La complejidad del código que puede ejecutar o las funcionalidades que puede configurar dependen en su totalidad de la sofisticación de la plataforma del intermediario.
  - La inversión necesaria para lograr compatibilidad con un modelo así sólo es justificable cuando la regulación obliga a la organización a migrar o el demográfico de usuarios que atiende lo valora o necesita suficiente para integrarlo como diferenciador dentro de su producto / servicio.

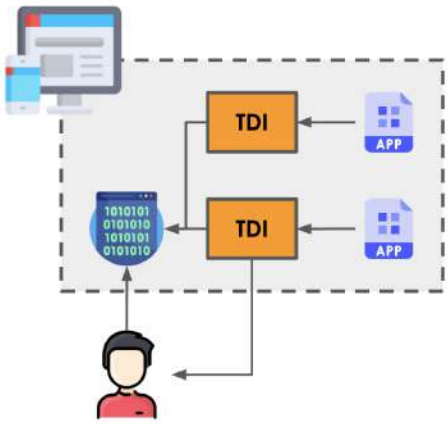


Figura 1. Diagrama de funcionamiento de un TDI dentro de un dispositivo

Desde el punto de vista legal, este modelo requerirá de repensar las estructuras legales sobre las cuales podría montarse un sistema así, ya que la relación entre el intermediario y los usuarios no está suficientemente definida y variará a partir de la legislación local. Adicionalmente, al no existir expectativas legales respecto a cómo deben funcionar las relaciones entre los actores, existe la posibilidad de que aparezcan conflictos de interés y acuerdos entre intermediarios y terceros que no estén en el mejor interés de los usuarios y su privacidad.

Por último, este modelo no cubre escenarios en los cuales los datos pueden tener múltiples dueños o forman parte de un sistema que no permite generar consentimiento individualizado. Por ejemplo, datos de peatones en una ciudad, aquellos generados por instituciones de gobierno sobre sus ciudadanos o los que se consideran de interés público.

C) Fideicomiso cívico de datos (*Civic Data Trust*)

Esta estructura tecnológica y legal[12] permite que usuarios entregan sus datos a una organización encargada de resguardarlos (*Trustee*), controlar el acceso y uso de terceros y velar por los intereses de sus dueños; una vez que el usuario final desea utilizar un producto o servicio tecnológico que requiere acceso a sus datos, este proceso se realiza con el *Trustee* como intermediario y vigilante del correcto uso y acceso a la información. Algunas de las piezas clave de un *Data Trust* (en adelante DT) incluyen[13]:

1. Contar con una estructura legal, incluyendo una constitución o incorporación como entidad, que incluya definiciones de derechos y obligaciones que tiene sobre los datos que se le encomiendan.
2. Tener un propósito u objetivo claro, de forma que sus usuarios puedan entender cómo se protegerán y usarán sus datos.
3. Contar con procesos de toma de decisión definidos y transparentes.
4. Tener un modelo de sostenibilidad financiera para su operación. Y, en el caso que se genere un beneficio económico de los datos, transparentar cómo se reparten o utilizan esos fondos. Esto es de especial importancia para que el DT cuente con los recursos necesarios para la protección de los datos desde el frente tecnológico y legal.

Este modelo permite un mayor control de la información provista por usuarios finales y contar con un tercero que activamente se asegura de que están siendo usados conforme a los contratos, términos, acuerdos y políticas acordadas previamente. Además, el usuario final encomienda al *Trustee* la persecución legal de actores que han hecho mal uso de la información provista. Asimismo, el *Trustee*, siendo un representante de todos sus usuarios, puede negociar los términos y contratos de uso de forma representativa y colectiva, velando por los mejores intereses de sus usuarios de forma fiduciaria y sin la capacidad de monetizar o crear un modelo de negocios a partir de los datos o los derechos de los datos en su posesión, a menos que así se defina como propósito en la constitución legal.

[12] Fuente: https://theodi.org/article/defining-a-data-trust
[13] Fuente: https://hello.elementai.com/rs/024-OAQ-547/images/Data_Trusts_EN_201914.pdf

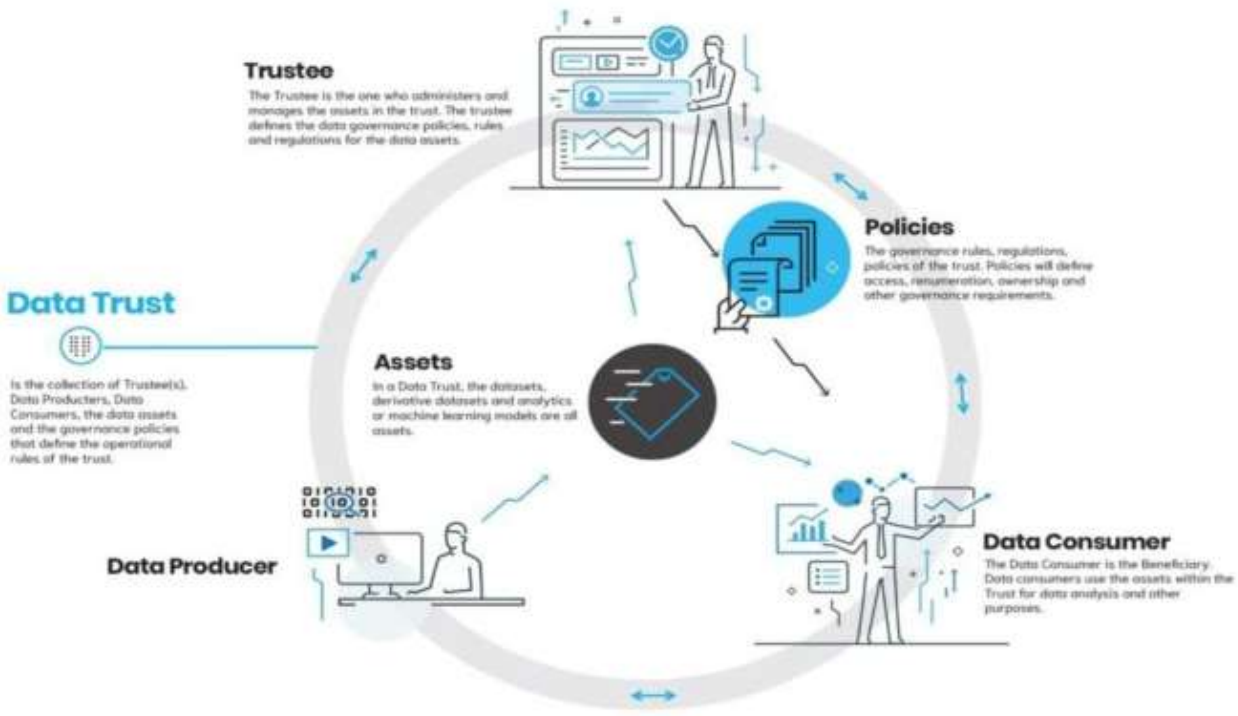


Figura 2. Ilustración explicativa de los elementos de un *Data Trust*

De esta forma, el DT es, sobre todo, una entidad con personalidad legal (ya sea en forma de una empresa, una organización sin fines de lucro, una entidad de gobierno u otro) que va más allá de una implementación o herramienta tecnológica. Si bien el componente tecnológico es importante, su estructura legal es lo que permite generar confianza y responsabilidades de los datos que los usuarios le encomiendan. Asimismo, existen dos componentes legales indispensables para el correcto funcionamiento de un DT:

1. Verificación de propiedad de los datos: el DT debe poder corroborar que el usuario tiene el derecho y poder legal para ceder los datos al DT y, en consecuencia, permitir su uso por un tercero.
2. Administración de terceros: al ser el DT el intermediario entre los propietarios de los datos y los beneficiarios de su uso, este deberá confirmar la identidad, las potenciales acciones y objetivos de los beneficiarios; con la intención de asegurar que el DT puede cumplir con sus obligaciones legales.

Concerniente a la tecnología, este mecanismo de gobernanza debe de contar con infraestructura y procesos suficientemente robustos para asegurar la seguridad y protección de los datos, así como los mecanismos necesarios para asegurar que los usuarios puedan ejercer sus derechos (e.g. borrado y migración de datos) y las herramientas de monitoreo de actividad de los terceros que utilizan los datos. Adicionalmente, un DT puede contar con mecanismos más complejos para la custodia y protección de datos, por ejemplo:

- Creación de plataformas de software que eviten la compartición de datos a terceros, de manera similar a un *Trusted Data Intermediary* (TDI). Es decir, el software que usa los datos de los propietarios se ejecutaría en infraestructura del DT, no del tercero.

- Un consejo multidisciplinario de encomendados que vigile la correcta operación del *Data Trust* y evalúe el impacto de iniciativas de terceros potencialmente invasivas, controversiales o éticamente cuestionables. Para ello, se pueden construir mecanismos de revisión del software (código) que accederá a los datos o auditorías técnicas con la intención de corroborar los objetivos y alcances del proyecto. Esto es especialmente efectivo en combinación con el mecanismo anterior.

- Para los casos especiales en los que los datos no son propiedad de individuos o colectivos fácilmente identificables (e.g. ciudades, países), se pueden crear DTs especializados en ejes temáticos enfocados al bien común, por ejemplo: salud, urbanismo, geografía, movilidad.

- Adicionalmente, como parte de los mecanismos de financiamiento de los DTs, se pueden crear modelos de Compartición de Ingresos enfocados a crear valor alrededor de los datos de sus propietarios. Para ello, se establecen reglas y principios sobre cómo pueden ser utilizados por terceros y el DT administra y negocia su compartición, incluyendo términos comerciales que pueden ser pagos o licencias de uso. Los ingresos generados, a su vez, pueden ser repartidos entre los propietarios de los datos y el DT.

Las ventajas de la implementación de este mecanismo heredan, en principio, las de un TDI con la adición de las siguientes:

- Empodera a los propietarios de datos de forma representativa, creando nuevos organismos que velan por sus intereses, la protección y correcto uso de sus datos. Esto invierte la estructura de poder respecto a los productos digitales y la economía de datos.
- Se abre la puerta para un enorme potencial de innovación a partir de análisis de datos que actualmente no son viables debido a la falta de confianza que existe actualmente en los consumidores de datos. Una vez que el público en general logre comprender los beneficios de estos mecanismos de gobernanza, aumentará la disposición a poner datos sensibles en *Data Trusts* que permitan crear nuevos productos y servicios para el beneficio de la sociedad. Por ejemplo: historias clínicas e investigación de nuevos fármacos y tratamientos; datos de movilidad urbana y optimizaciones en transporte.
- Creación de un nuevo ecosistema de protección de datos con un diseño centrado en usuarios, ya que cada persona tiene una preferencia distinta sobre sus datos personales, cómo le gustaría que se usaran, lo que le genera sospecha o desconfianza y las causas o objetivos que valora. Por ello, al invertir la estructura de poder de los datos, el usuario puede elegir al *Data Trust* que mejor se alinee con sus convicciones e ideales, de forma que el mercado pueda desarrollar soluciones a la medida de cada demográfico.

Por otro lado, de igual manera que cualquier mecanismo en una etapa temprana, aún tiene algunos retos y áreas de oportunidad por resolver; principalmente los relacionados a la obtención de financiamiento y su introducción al ecosistema. A continuación algunos fundamentos para ello:

- Un *Data Trust* requiere de un gran número de personas, o un conjunto de datos de gran interés, para alcanzar suficiente poder de negociación con organizaciones que consumen datos y convencerlas de realizar cambios a su tecnología, modelo de negocios y/u operación. Algunos posibles métodos de mitigación de esta problemática incluyen:
    - La introducción de nueva regulación que obligue a los consumidores de datos a interactuar con los usuarios a través de un *Data Trust*.
    - Crear DTs de índole público con datos de ciudades o países enteros que previamente no estaban disponibles y que generan interés en la iniciativa privada.
- La obtención de recursos es un gran obstáculo para la implementación de este mecanismo, especialmente si no se cuenta con apoyo de fondos públicos o privados. De manera similar al punto anterior, esto es resoluble mediante la introducción de regulación, subsidios o incluso la integración del DT como un nuevo organismo dentro del gobierno, aunque esto posiblemente requiera cambios a la ley.

- Por último, el convencimiento de valor al público en general es un reto importante que se deberá resolver para obtener la confianza de los usuarios respecto a las organizaciones que administran sus datos. Para ello, serán necesarias campañas de educación y concientización desde múltiples sectores (gobierno, sociedad civil, entre otros) sobre la problemática y cómo los DT pueden crear una solución a los temas más complejos de la actual economía de los datos.

Fideicomisos de datos (*Data Trusts*): Consideraciones legales y éticas

Lista las problemáticas que pudieran presentarse en la operación de los intermediarios de datos:

1. Protección y privacidad de datos: a menos que el intercambio de datos a través de un intermediario de datos se haya establecido como una finalidad de uso al momento en que se recolectó el consentimiento del titular de los datos, el intercambio requerirá una justificación legal. Será necesario contar con el consentimiento del titular, pero eso puede dificultar.

   En ciertos casos de interés legítimo o por virtud de un mandato de autoridad puede que sea una alternativa para justificar el intercambio de datos pero esto no siempre está presente.

   La anonimización o seudonimización tampoco resuelven del todo el problema, pues el intermediario debe implementar procesos para proteger la privacidad de los datos y respetar sus derechos asociados.

2. La confidencialidad en el ámbito comercial también necesita ser protegido, pues los titulares pueden ejercer una reclamación si la confidencialidad de sus datos se vio afectada.

3. Derechos de PI: el intermediario necesita asegurar las licencias y autorizaciones necesarias para proteger los derechos de los titulares y asegurar su cumplimiento.

4. Los proveedores de datos necesitan asegurar que el cumplimiento de las obligaciones contractuales con terceras partes sigue estando vigente aún y cuando comparten la información a través de un intermediario.

Reglas para los usuarios de datos

Las reglas sobre los intermediarios de datos deben ser legalmente vinculantes para los usuarios de datos, y debe garantizar que los derechos e intereses de los proveedores de datos, los intermediarios y los titulares son respetados, lo cual deberá quedar reflejado en el contrato respectivo. Sin embargo, hay ciertos tipos de datos que cuentan con una protección especial, que por su sensibilidad pueden estar sujetos a restricciones ya sea en virtud de las leyes de protección de datos o por seguridad nacional.

Los sectores de salud y servicios financieros debieran tener una regulación especial y el uso de datos de o por el sector público debería tener una atención particular. Por otro lado las reglas que se establecerán en los contratos, debieran contemplar también niveles de servicio y aspectos técnicos respecto de los participantes en un modelo de intermediario de datos.

Mecanismos de cumplimiento

Para el caso de violaciones a los términos contractuales, las partes tendrían a su disposición ejercer los mecanismos tradicionales de acceso a la justicia. Sin embargo, en el estudio se recomienda pactar mecanismos alternativos de solución de controversias. Lo anterior sin perjuicio que ciertas violaciones podrán ser atendidas por los órganos de gobierno correspondientes, como por ejemplo aquellos encargados de la protección y privacidad de datos.

También se recomienda incluir mecanismos de auditoría, interna o externa, que le permita identificar brechas o potenciales brechas e implementar mejoras y recomendaciones.

Gobernanza

Los intermediarios de datos deben intentar equilibrar la amplia gama de derechos e intereses tanto de los participantes como de las partes interesadas en general, y generar confianza entre ellos sobre el correcto desarrollo de sus actividades. Requiere de un mecanismo de gobernanza que se centre en las finalidades y objetivos primordiales del intermediario de datos.

Esto es, que debe proporcionar:

- Una representación adecuada de las partes interesadas que lo han elegido para la gestión de los datos;
- Un mecanismo para acordar cambios en el propósito y funcionamiento del intermediario de datos;
- Supervisión y garantía de que las reglas y los métodos se cumplen y son eficaces.

El objetivo primordial de la estructura de gobierno es lograr la confianza.

Concluir relación con el intermediario

En caso de que el intermediario de datos cumpla con su propósito o los proveedores de los datos y sus titulares ya no deseen usar un intermediario de datos, éste deberá dejar de existir. Lo que implica diseñar un procedimiento a priori para que los diferentes usuarios conozcan lo que sucederá en esta circunstancia antes de crear una relación con el intermediario de los datos y antes de proporcionar los datos o recibirlos. ¿Qué pasará con mis datos que ya fueron compartidos?

Reformas legales

El estudio no sugiere la creación de normativa para facilitar el uso de los datos a través de un intermediario de datos. E incluso establece que reformar la normativa relativa a los fideicomisos podría ser un camino largo y difícil. Considera que la mayoría de los temas legales que surgen en la operación de los intermediarios de datos puede resolverse a través de contratos y derecho societario.

Sin embargo, si se involucra el tratamiento de datos personales, surge la disyuntiva de hasta qué punto, las leyes sobre la materia, permiten una justificación de no consentimiento para permitir el intercambio de datos y esto representa un obstáculo real para algunos intermediarios de datos.

La incertidumbre sobre este aspecto podría reducirse a través de la emisión de guías emitidas por las autoridades reguladoras en la materia, respecto de la interpretación que deba hacerse sobre estos aspectos tratándose de un intermediario de datos, lo cual generaría confianza en el intercambio de datos que se ejecute conforme a dicha guía ya que no se estaría violando las leyes de protección de datos.

D) *X-Road*

X-Road es una plataforma de código abierto creada por el gobierno de Estonia para la implementación de gobernanza electrónica que permite que, principalmente pero no exclusivamente, entidades de gobierno intercambien datos de forma transparente, controlada, ágil y automatizada. Esto se logra a través de dos elementos:

1. Un operador central, usualmente una organización con infraestructura tecnológica y autoridad para definir las regulaciones, reglas y prácticas operativas de la red, que administra el acceso a la red para los consumidores y productores de servicios y en general dar soporte al sistema.
    a. Este rol también define las autoridades de confianza para las comunicaciones dentro de la red para la certificación de identidad (*Certification Authority*, o CA) y de *timestamping.*
    b. Los roles de productores de servicio refieren aquellas organizaciones o servidores dentro de la red que proveen datos a otros actores dentro de la red. Por otro lado, los consumidores son aquellas organizaciones que toman datos de los productores. Una organización puede contar con ambos roles.
2. Una capa de software que se agrega a los sistemas existentes de los consumidores y productores de servicios de forma que puedan intercambiar datos y acceder a las funcionalidades y características de *X-Road*. Esto significa que *X-Road* es agnóstico a la tecnología o infraestructura sobre la cual se implementa; por tanto, las organizaciones no requieren hacer cambios estructurales demasiado agresivos para crear o integrarse a una red *X-Road*.

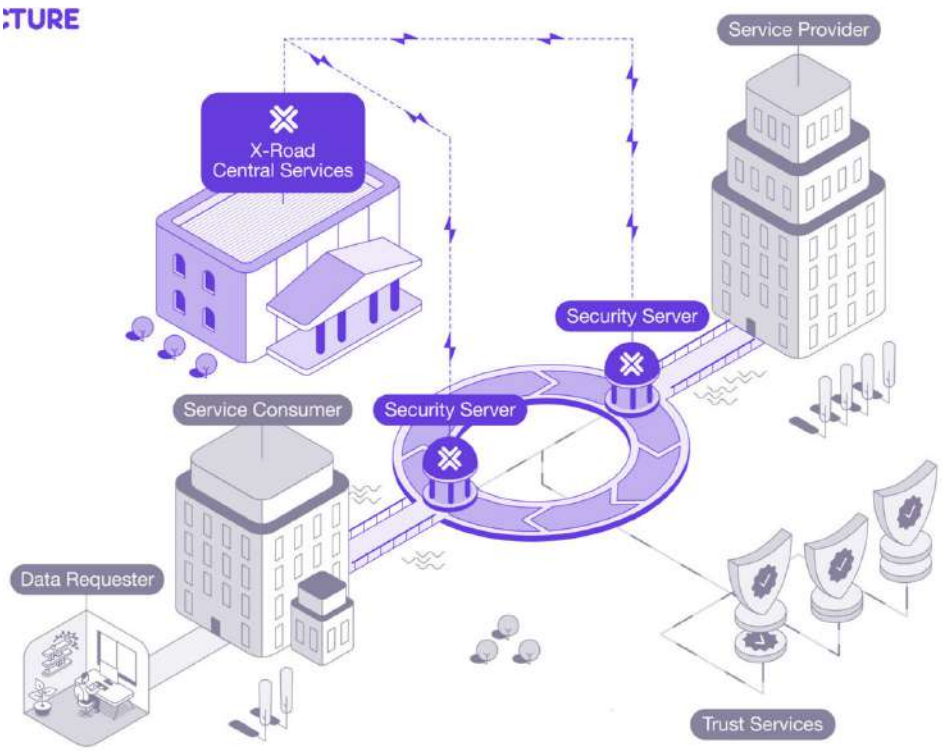


Figura 3. Arquitectura de X-Road y funcionamiento general

Entre las características clave de esta plataforma se incluyen: conexiones y comunicaciones entre operadores, consumidores y productores seguras (encriptadas), trazables (registradas en

bitácoras) y no repudiables (firmadas); y que cada productor de servicio es dueño de sus datos y de la administración de acceso a los mismos. Es decir, formar parte de una red en *X-Road* no hace los datos de una organización accesibles para los demás de forma automática, el acceso es granular y las condiciones deben ser acordadas de antemano.

En temas de gobernanza cívica de datos, *X-Road* permite que las organizaciones, especialmente las instituciones de gobierno, compartan datos entre sí con mayor control y de forma más responsable:

1. En contraste a un método tradicional en el que los datos son compartidos en archivos o conjuntos que fácilmente se pueden filtrar, robar o alterar, *X-Road* permite un intercambio de datos sin que estos sean manipulados de forma manual.
2. Cada interacción de intercambio de datos entre productor / consumidor es registrado en una bitácora, realizado de forma privada y firmado digitalmente por ambas partes. De esta forma es posible rastrear el origen de los datos o la forma en la cual fueron utilizados.
3. Dado que cada productor de datos decide quién, cómo, cuándo y por qué se accede a sus datos, se ejerce un mayor control sobre ellos y permite a la organización definir los términos de acceso.

fAIr LAC
Jalisco

Reporte elaborado por C Minds
Mayo 2023

BID | BID LAB | Tecnológico de Monterrey Escuela de Ingeniería y Ciencias | C MINDS | Jalisco