Orientaciones Específicas para el Cumplimiento de los Principios y Derechos que Rigen la Protección de los Datos Personales en los Proyectos de Inteligencia Artificial

RED IBEROAMERICANA DE PROTECCION DE DATOS

Texto aprobado por las Entidades integrantes de la Red Iberoamericana de Protección de Datos en la sesión del 21 de junio de 2019, en Naucalpan de Juárez, México.

Este documento fue sometido a consulta pública por parte de la RIPD y las observaciones recibidas fueron consideradas para la redacción de la versión final.

RED IBEROAMERICANA DE PROTECCION DE DATOS

RED IBEROAMERICANA DE PROTECCION DE DATOS

Tabla de contenidos

Página

01. Introducción 5

02. Principios y Derechos que rigen la Protección de Datos Personales 7

03. Orientaciones específicas para el cumplimiento de los Principios Rectores de la Protección de Datos Personales 10

04. Orientaciones Específicas para el cumplimiento de las Obligaciones por los encargados del Tratamiento (Artículos 25, 33 y 34 de los Estándares) 30

05. Orientaciones Específicas para el cumplimiento de los Derechos (Artículos 24 32 de los Estándares) 33

06. Orientaciones Específicas para la aplicación de Medidas Proactivas en el Tratamiento de los Datos Personales de los Proyectos de Inteligencia Artificial 38

07. Glosario 42

RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 01. Introducción

/ 01. Introducción

El avance de nuevas tecnologías en el entorno tecnológico actual conlleva modelos de procesamiento de datos personales innovadores, variados e intensivos, los cuales son sujetos de monitoreo y control por parte de las autoridades de protección de datos personales en el mundo, en aras de preservar que el desarrollo vaya acompañado del respeto de las libertades de las personas.

Así, entre los temas de la agenda internacional en protección de datos personales el cómputo en la nube; la minería digital; el procesamiento masivo de datos identificado como big data; la conectividad de dispositivos y appificación en un internet de todo; el registro confiable y seguro de las operaciones y transacciones a través de la criptografía, aplicaciones blockchain y smartcontract; la automatización de procesos y el uso de algoritmos en la industria y la robótica; son solamente ejemplos de capacidades tecnológicas, de cómputo y conectividad que se redefinen continuamente.

Entre las principales tendencias en nuestro entorno digital se encuentra la inteligencia artificial, que ha causado especial interés por parte de la industria y gobiernos dada la gran cantidad de aplicaciones en la que puede ser implementada y los resultados en los procesos derivados, por lo que la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (ICDPPC, por sus siglas en inglés) en su edición 38, celebrada en Marrakech, Marruecos, el año 2016 inició con el análisis y discusión en torno a la protección de datos personales y privacidad en inteligencia artificial y robótica.

Posteriormente, en el marco de la 40ª ICDPPC, que se llevó a cabo en el año 2018, en Bruselas, Bélgica, se aprobó la "*Declaración relativa a la ética y protección de datos en Inteligencia Artificial*", postulando seis principios rectores como valores fundamentales para preservar derechos humanos en el desarrollo de la inteligencia artificial.

A la vez, en el marco del XVII EIPD en la sesión del 21 de junio de 2019, en la Ciudad de Naucalpan de Juárez, México, se aprobó por las Entidades integrantes de la RIPD, el documento denominado: "*Recomendaciones para el tratamiento de datos personales en la inteligencia artificial*".

Este documento contiene unas directrices complementarias y más detalladas de las que se recogen en el otro documento de la RIPD denominado "Recomendaciones generales para el tratamiento de datos personales en la Inteligencia Artificial". Y todo ello en el marco del instrumento normativo que constituye la referencia común para las entidades integrantes de la RIPD, como son los Estándares de Protección de Datos Personales para los Estados Iberoamericanos que se aprobaron en Santiago de Chile, en 2017.

RED IBEROAMERICANA DE PROTECCION DE DATOS

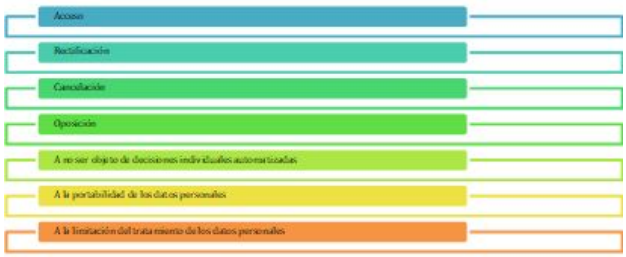
/ 02. Principios y Derechos que Rigen la Protección de los Datos Personales

/ 02. Principios y Derechos que Rigen la Protección de los Datos Personales

Con la adopción de los Estándares, se reconocen una serie de principios y derechos rectores de la protección de datos personales, que los Estados Iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de garantizar un debido tratamiento de los datos personales y contar con reglas homogéneas en la región.

De acuerdo con los Estándares, los **principios** rectores de la protección de datos personales son:

Asimismo, los responsables del tratamiento deberán garantizar y facilitar a los titulares de los datos personales el ejercicio de los siguientes **derechos**:



En suma:

Tomando en cuenta lo anterior, en el siguiente apartado se realizará un análisis de los aspectos que se deberán considerar para cumplir con cada uno de estos principios y derechos en el tratamiento de datos personales en el desarrollo de inteligencia artificial.

RED IBEROAMERICANA DE PROTECCION DE DATOS

RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 03. Orientaciones Específicas para el Cumplimiento de los Principios Rectores de la Protección de los Datos Personales

/ 03. Orientaciones Específicas para el Cumplimiento de los Principios Rectores de la Protección de los Datos Personales

El tratamiento adecuado o debido de datos personales debe realizarse en apego a diversos principios a través de los cuales, responsables y encargados, estarán en aptitud de acreditar su uso seguro, supuesto que incluye el que se realice en el marco de aplicativos de IA, ya sea como parte del procesamiento o en su interacción con clientes, administradores y demás perfiles de usuarios, así como con otros sistemas o aplicativos.

Principio de Legitimación (Artículo 11 de los Estándares)

¿En qué consiste este principio?

De conformidad con este principio, el responsable solo podrá tratar datos personales cuando se presente alguno de los siguientes supuestos:

a. El titular otorgue su consentimiento para una o varias finalidades específicas.
b. El tratamiento sea necesario para el cumplimiento de una orden judicial, resolución o mandato fundado y motivado de autoridad pública competente.
c. El tratamiento sea necesario para el ejercicio de facultades propias de las autoridades públicas o se realice en virtud de una habilitación legal.
d. El tratamiento sea necesario para el reconocimiento o defensa de los derechos del titular ante una autoridad pública.
e. El tratamiento sea necesario para la ejecución de un contrato o precontrato en el que el titular sea parte.
f. El tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al responsable.
g. El tratamiento sea necesario para proteger intereses vitales del titular o de otra persona física.
h. El tratamiento sea necesario por razones de interés público establecidas o previstas en ley.
i. El tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del titular que requiera la protección de datos personales, en particular cuando el titular sea niño, niña o adolescente. Lo anterior, no resultará aplicable a los tratamientos de datos personales realizados por las autoridades públicas en el ejercicio de sus funciones.

/ 03. Orientaciones Específicas para el Cumplimiento de los Principios Rectores de la Protección de los Datos Personales

Orientaciones específicas para el principio de legitimación en el tratamiento de datos personales en el desarrollo de IA

- Considerar desde el desarrollo de IA que lleve a cabo tratamiento de datos personales, la implementación de mecanismos sencillos, ágiles, eficaces y gratuitos que permitan obtener el consentimiento de los titulares, o bien, implementarlos previo al uso de la IA.
- Para que se cumpla con este compromiso adquirido mediante los Estándares y que el tratamiento sea lícito, los datos deben ser tratados con el consentimiento del interesado o, sobre alguna otra base legítima, como lo son el interés público, la necesidad contractual, el cumplimiento de obligaciones legales, el interés vital del individuo, o la investigación científica, en cualquier supuesto de aplicación de alguna de las bases legítimas señaladas en el tratamiento se deberá observar el cumplimiento de los principios rectores que rigen la protección de datos personales.
- En caso de que se considere necesario obtener el consentimiento del titular de los datos, se recomienda que sea:
    - Libre: Que no medie error, mala fe, violencia o dolo que puedan afectar la manifestación de la voluntad del titular.
    - Informado: Que el titular tenga el conocimiento del tratamiento al que serán sometidos sus datos personales y que conozca las consecuencias de otorgar su consentimiento.
- Para recabar el consentimiento, se pueden tomar en cuenta las siguientes opciones, siempre y cuando no se contrapongan con lo establecido en la legislación nacional del país de que se trate:
    - Consentimiento tácito: El consentimiento tácito se obtiene si el titular no se niega a que sus datos personales sean tratados, después de haber conocido el aviso de privacidad. Es decir, no es necesario que quede registrado que el titular autorizó el tratamiento de su información personal, sino que es suficiente con que no se niegue al tratamiento.

/ 03. Orientaciones Específicas para el Cumplimiento de los Principios Rectores de la Protección de los Datos Personales

- Consentimiento expreso: El titular deberá expresamente señalar que consiente el tratamiento de sus datos personales. La voluntad del titular se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o cualquier otra tecnología.
- Consentimiento expreso-por escrito: se deberá otorgar por escrito, mediante firma autógrafa, huella dactilar, firma electrónica del titular o cualquier otro mecanismo autorizado que permita identificarlo plenamente.

- Cuando se considere necesario obtener el consentimiento, la solicitud deberá ir siempre ligada a las finalidades concretas o finalidades compatibles del tratamiento que se informe al titular, es decir, el consentimiento se deberá solicitar para tratar los datos personales para finalidades específicas, no en lo general.
- Solicitar el consentimiento previo a la obtención de los datos personales o en el momento en que lo indique la normatividad que resulte aplicable.
- Facilitar al titular medios sencillos y gratuitos para que, en su caso, pueda manifestar su consentimiento o negativa al mismo.
- Obtener el consentimiento para nuevas finalidades, cuando se pretenda tratar los datos personales para fines distintos, que no sean compatibles o análogos a los establecidos de origen.
- Tomar en cuenta que, si las decisiones automatizadas involucran categorías especiales de datos, como datos sensibles, sean tratados solamente si el titular ha dado su consentimiento o si la ley local aplicable contempla excepciones al consentimiento que permitan dar el tratamiento de manera legítima

/ 03. Orientaciones Específicas para el Cumplimiento de los Principios Rectores de la Protección de los Datos Personales

- Documentar que se ha otorgado el consentimiento para el tratamiento de datos en los casos en que sea aplicable.
- Llevar un control para identificar a los titulares que en su caso hayan negado su consentimiento para el tratamiento de finalidades específicas, que no se traten de aquéllas que originan y sustentan la relación jurídica entre el titular y el responsable.
- En los casos de datos personales de niñas, niños y adolescentes, el responsable debe verificar si su legislación nacional permite que el menor de edad pueda brindar directamente la autorización para el tratamiento de sus datos o en su caso, obtener el permiso del titular de la patria potestad o tutela conforme los criterios establecidos en la ley nacional aplicable.

Principio de Licitud (Artículo 14 de los Estándares)

¿En qué consiste este principio?

De conformidad con este principio, el responsable tratará los datos personales en su posesión con estricto apego y cumplimiento de lo dispuesto por el derecho interno del Estado Iberoamericano que resulte aplicable, el derecho internacional y los derechos y libertades de las personas.

De manera adicional a lo anterior, en el tratamiento de datos personales que realicen las autoridades públicas se sujetará a las facultades o atribuciones que el derecho interno del Estado Iberoamericano de que se trate les confiera expresamente.

Orientaciones específicas para el principio de licitud en el tratamiento de datos personales en el desarrollo de IA

- Conocer la normatividad que en lo específico regula y aplica a la actividad en la que son tratados los datos personales y realizar el tratamiento en plena observancia de la misma. De manera adicional, se sugiere revisar la jurisprudencia e instrumentos de soft law en materia de derechos humanos que pudieran resultar aplicables al caso específico.
- Si el responsable pertenece al sector público, los datos personales deberán tratarse conforme las facultades o atribuciones que la normatividad les otorgue.

/ 03. Orientaciones Específicas para el Cumplimiento de los Principios Rectores de la Protección de los Datos Personales

- Revisar si existe normatividad que se vincule, de manera directa o indirecta, con la protección o el tratamiento de datos personales, como las disposiciones en materia de salud, financieras y/o bancarias.
- Incluir previsiones sobre la obligación de cumplir con este principio en las cláusulas, contratos u otros instrumentos jurídicos que se firmen con terceros.

Principio de Lealtad (Artículo 15 de los Estándares)

¿En qué consiste este principio?

De conformidad con este principio, el responsable tratará los datos personales en su posesión privilegiando la protección de los intereses del titular y absteniéndose de tratar éstos a través de medios engañosos o fraudulentos.

Para efectos de los Estándares, se considerarán desleales aquellos tratamientos de datos personales que den lugar a una discriminación injusta o arbitraria contra los titulares.

Orientaciones específicas para el principio de lealtad en el tratamiento de datos personales en el desarrollo de IA

- Evitar utilizar medios engañosos o fraudulentos para tratar datos personales siempre en estricto apego a los principios éticos de la IA de prevención de daño y lealtad.
- Realizar el tratamiento de los datos personales respetando los intereses del titular.
- Tener en cuenta las expectativas razonables de privacidad de los individuos en relación con el uso de datos personales y debe considerar el impacto de la IA en la sociedad en general. Los sistemas deben desarrollarse de manera que faciliten el desarrollo humano y no lo obstruyan o pongan en peligro.
- Cuando se apliquen decisiones automatizadas, se recomienda implementar medidas para proteger los derechos, libertades e intereses legítimos del titular de los datos personales.

/ 03. Orientaciones Específicas para el Cumplimiento de los Principios Rectores de la Protección de los Datos Personales

- El modelo de IA no debe enfatizar la información relacionada con el origen racial o étnico, la opinión política, la religión o la creencia, la afiliación sindical, el estado genético, el estado de salud, la orientación sexual, la condición económica, el género o la existencia de alguna discapacidad si esto conduce a un tratamiento discriminatorio arbitrario.
- Establecer un sistema de monitoreo constante del modelo de IA con la finalidad de identificar la existencia de sesgos y en la medida de lo posible implementar una gestión de riesgos. Como producto final del sistema de monitoreo se deberán generar reportes y estadísticas que permitan al responsable analizar los resultados.
- Tener en cuenta que la interconexión de diferentes tipos de datos personales puede revelar información confidencial sobre los individuos.
- Reducir y/o mitigar los prejuicios o discriminaciones que pudieran resultar de la utilización de datos en la AI, priorizando el respeto a los instrumentos internacionales de derechos humanos y no-discriminación.
- Asegurar que los sistemas de IA se diseñen de tal forma que faciliten el desarrollo humano, a través de un enfoque orientado a evitar y mitigar los riesgos potenciales del procesamiento de datos personales.
- Evitar que la toma de decisiones a través de una tecnología de IA incremente las desigualdades estructurales que se encuentran en la sociedad y/o genere daño o sufrimiento a titulares en lo individual o de forma colectiva.
- Cuando un responsable haga uso de inteligencia artificial para el tratamiento de datos personales no debe “engañar” al titular sobre si se trata de una persona o justamente de inteligencia artificial.

Principio de Transparencia (Artículo 16 de los Estándares)

¿En qué consiste este principio?

En virtud de este principio, el responsable informará al titular sobre la existencia misma y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

/ 03. Orientaciones Específicas para el Cumplimiento de los Principios Rectores de la Protección de los Datos Personales

Por lo tanto, el responsable proporcionará al titular, al menos, la información siguiente:

- Su identidad y datos de contacto.
- Las finalidades del tratamiento a que serán sometidos sus datos personales.
- Las comunicaciones, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y las finalidades que motivan la realización de las mismas.
- La existencia, forma y mecanismos o procedimientos a través de los cuales podrá ejercer los derechos de acceso, rectificación, cancelación, oposición y portabilidad.
- En su caso, el origen de los datos personales cuando el responsable no los hubiere obtenido directamente del titular.

De manera adicional, a información proporcionada al titular tendrá que ser suficiente y fácilmente accesible, así como redactarse y estructurarse en un lenguaje claro, sencillo y de fácil comprensión para los titulares a quienes va dirigida, especialmente si se trata de niñas, niños y adolescentes.

Por último, todo responsable contará con políticas transparentes de los tratamientos de datos personales que realice.

Orientaciones específicas para el principio de transparencia en el tratamiento de datos personales en el desarrollo de IA

- Comunicar al titular las características principales del tratamiento al que será sometida su información personal.
- Informar expresamente a los titulares que en el tratamiento de sus datos personales se utilizarán procesos de automatización.
- Incluir el medio que se seleccione por los responsables para dar cumplimiento al principio de transparencia todas las finalidades para las cuales serán tratados los datos de los titulares.
- Además de la información señalada como mínimo para informar al titular, en el supuesto de que sus datos personales sean objeto de un tratamiento automatizado, se sugiere como buena práctica informar continuamente a los titulares de manera que puedan conocer la forma en cómo las decisiones automatizadas pueden afectarlos, y en su caso solicitar la intervención humana, con el objetivo de que puedan tomar una decisión informada respecto a si consiente o no el tratamiento.

/ 03. Orientaciones Específicas para el Cumplimiento de los Principios Rectores de la Protección de los Datos Personales

- La información que se proporcione respecto a la lógica del modelo de AI deberá incluir por lo menos aspectos básicos sobre su funcionamiento, así como la ponderación y correlación de los datos, redactados en un lenguaje claro, sencillo y de fácil comprensión, por lo que, no será necesario proporcionar una explicación completa de los algoritmos utilizados o incluso incluirlos. Lo anterior siempre buscando no afectar la experiencia del usuario.
- Promover la transparencia en la IA mediante el desarrollo de formas innovadoras de dar a conocer a los titulares las características principales del tratamiento y el nivel de riesgo relacionado con el aumento o disminución de la expectativa de privacidad.
- Salvaguardar el derecho a la autodeterminación informativa, al asegurarse que los titulares siempre estén informados de forma adecuada y oportuna de que estarán interactuando directamente con un sistema de IA o cuando su información será tratada por los mismos.
- Proporcionar información significativa sobre la finalidad y los efectos de los sistemas de IA para verificar la alineación continua con la expectativa de privacidad de los titulares permitiendo que en todo momento puedan ejercer control sobre el tratamiento de sus datos personales.
- El uso de IA reta a los responsables a ser tan innovadores en esta área como lo son al usar análisis, y a encontrar nuevas formas de transmitir información de manera concisa. Existen varios enfoques innovadores para proporcionar avisos de privacidad, incluido el uso de videos, caricaturas e íconos estandarizados. El uso de una combinación de enfoques puede ayudar a que la información compleja sobre IA sea más fácil de comprender para los titulares de los datos personales.
- Identificar y definir los términos comúnmente utilizados y crear una base de datos para que puedan ser reutilizados en diferentes contextos, con iconos estándar[1] para dar a conocer información a los titulares.

1. Al respecto el RGPD en su considerando 60 señala que la información que se proporcione en cumplimiento al principio de transparencia podrá transmitirse en combinación con unos de iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto.

/ 03. Orientaciones Específicas para el Cumplimiento de los Principios Rectores de la Protección de los Datos Personales

- Los responsables deberán ser transparentes acerca de su tratamiento de datos personales mediante el uso de una combinación de enfoques innovadores con el fin de proporcionar avisos de privacidad significativos en las etapas apropiadas a lo largo de un proyecto de IA.
- Informar el origen de los datos personales cuando éstos se obtengan a través de una transferencia y en el supuesto específico de que se pretendan utilizar para IA validar que esta finalidad haya sido informada por el primer responsable que los obtuvo para poder hacer uso de los datos para dicha finalidad.

Principio de Finalidad (Artículo 17 de los Estándares)

¿En qué consiste este principio?

En atención a este principio, todo tratamiento de datos personales se limitará al cumplimiento de finalidades determinadas, explícitas y legítimas.

El responsable no podrá tratar los datos personales en su posesión para finalidades distintas a aquéllas que motivaron el tratamiento original de éstos, a menos que concurra alguna de las causales que habiliten un nuevo tratamiento de datos conforme al principio de legitimación.

Por último, el tratamiento ulterior de datos personales con fines archivísticos, de investigación científica e histórica o con fines estadísticos, todos ellos, en favor del interés público, no se considerará incompatible con las finalidades iniciales.

Orientaciones específicas para el principio de finalidad en el tratamiento de datos personales en el desarrollo de IA

- Considerar dentro de las finalidades del tratamiento de los datos personales de forma explícita el uso para IA.
- Identificar finalidades del tratamiento en la etapa más temprana posible del desarrollo de IA y comunicarlo a los titulares en un lenguaje ciudadano, de modo que resulte comprensible para la población objetivo cómo se utilizan sus datos.
- Garantizar que el uso de los sistemas de IA sea coherente con las finalidades originales que motivaron el tratamiento de manera que los datos personales no se utilicen para finalidades incompatibles a las que dieron origen a su recolección.

/ 03. Orientaciones Específicas para el Cumplimiento de los Principios Rectores de la Protección de los Datos Personales

- Cuando el responsable identifique finalidades compatibles y proporcionales a las que dieron origen al tratamiento se deberán informar a los titulares para que estén en posibilidad de tomar decisiones informadas al respecto.
- Considerar si en el caso particular en el que se pretende utilizar IA se trata de un tratamiento con fines de investigación científica[2] en favor del interés público, pues en dicha situación no se considerará incompatible con las finalidades iniciales.
- Cuando en la IA se utilice un modelo dinámico o en línea[3], dada la naturaleza de estos, se debe tener especial cuidado al momento de dar a conocer a los titulares la finalidad para la cual se darán a conocer los datos personales.

Principio de Proporcionalidad (Artículo 18 de los Estándares)

¿En qué consiste este principio?

En atención a este principio sólo podrán ser objeto de tratamiento los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento.

Orientaciones específicas para el principio de proporcionalidad en el tratamiento de datos personales en el desarrollo de IA

- Recolectar y tratar el número mínimo de datos personales para IA, en estos supuestos recordar que es mejor tener calidad en los datos personales que cantidad.
- Evaluar si los datos recolectados son necesarios para las finalidades que fueron informadas a los titulares.
- En caso de ser posible, se sugiere implementar IA que no requiera para su funcionamiento el tratamiento de datos personales.
- Limitar el periodo de tratamiento de los datos personales al mínimo indispensable, especialmente si son sensibles.
- Hacer uso de técnicas de pseudonimización o cifrado para proteger la identidad del titular de los datos personales, de forma tal que se limite el grado de intervención o afectación a su derecho a la privacidad y protección de datos.
- Para los desarrolladores de IA se sugiere examinar el área de aplicación previsto para el modelo con el objetivo de facilitar la selección de los datos que sean

2. Con relación al término investigación científica, existen dificultades sobre la concepción de qué se entiende por ésta, por lo que se deberá atender a lo dispuesto, en su caso, por la legislación nacional de los Estados Iberoamericanos aplicable en la materia. Al respecto, se sugiere consultar lo que el RGPD en su considerando 159 señala por investigación científica, así como las reglas previstas en su artículo 89.

3. Como referencia sobre los modelos dinámicos o en línea se sugiere consultar el Reporte sobre “Inteligencia artificial y Privacidad” del año 2018, elaborado por la Autoridad Noruega de Protección de Datos.

/ 03. Orientaciones Específicas para el Cumplimiento de los Principios Rectores de la Protección de los Datos Personales

adecuados, pertinentes y relevantes para la finalidad que se persigue.

- Los desarrolladores de AI deberán evaluar de forma crítica la calidad, la naturaleza, el origen y la cantidad de datos personales utilizados, reduciendo los datos innecesarios, redundantes o marginales durante las fases de desarrollo y entrenamiento, y posteriormente monitorear la precisión del modelo a medida que se alimenta con datos nuevos[4].
- El uso de datos sintéticos[5] puede considerarse como una posible solución para minimizar la cantidad de datos personales procesados por las aplicaciones de AI.
- Cuando se esté desarrollando IA considerar la posibilidad de lograr los objetivos de una manera menos invasiva para los titulares.
- En el supuesto de que se pretenda implementar IA se sugiere realizar evaluaciones de impacto a la protección de datos personales y documentarlas, para que, en un momento específico, puedan presentarse a la Autoridad de Protección de Datos en el caso de una inspección o si surge una controversia al respecto en concordancia con lo señalado en la sección 41.1 de los Estándares.
- Si bien es complicado establecer la información exacta que será necesaria y relevante para el desarrollo de un algoritmo en IA, y esta podría ser modificada, es importante que de forma continua se sometan a una evaluación para identificar si la misma continúa siendo necesaria, con el objeto de cumplir con el criterio de minimización.
- El realizar análisis periódicos respecto a lo adecuado o pertinente que resulta un dato personal, no solo protege la expectativa razonable de privacidad del titular, sino que también, minimiza el riesgo en IA de que la información personal irrelevante lleve al algoritmo a encontrar correlaciones que, en lugar de ser significativas, sean coincidentes y no aporten un valor agregado.
- Finalmente, el principio de proporcionalidad juega un papel importante en el desarrollo de la IA, en la medida en que su aplicación efectiva protegerá el derecho a la protección de datos de los titulares, impactando de forma positiva en generar confianza en el uso de la misma.

---

4. Directrices de Inteligencia Artificial y Protección de Datos del Comité Consultivo de la Convención para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

5.Para conocer una definición de datos sintéticos consultar http://ec.europa.eu/eurostat/ramon/coded_files/OECD_glossary_stat_terms.pdf

/ 03. Orientaciones Específicas para el Cumplimiento de los Principios Rectores de la Protección de los Datos Personales

Principio de Calidad (Artículo 19 de los Estándares)

¿En qué consiste este principio?

El principio de calidad significa que, el responsable adoptará las medidas necesarias para mantener exactos, completos y actualizados los datos personales en su posesión, de tal manera que no se altere la veracidad de éstos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento.

Asimismo, cuando los datos personales hubieren dejado de ser necesarios para el cumplimiento de las finalidades que motivaron su tratamiento, el responsable los suprimirá o eliminará de sus archivos, registros, bases de datos, expedientes o sistemas de información, o en su caso, los someterá a un procedimiento de anonimización.

Ahora bien, para la supresión de los datos personales, el responsable implementará métodos y técnicas orientadas a la eliminación definitiva y segura de éstos.

Por último, los datos personales únicamente serán conservados durante el plazo necesario para el cumplimiento de las finalidades que justifiquen su tratamiento o aquéllas relacionadas con exigencias legales aplicables al responsable. No obstante, la legislación nacional de los Estados Iberoamericanos aplicable en la materia podrá establecer excepciones respecto al plazo de conservación de los datos personales, con pleno respeto a los derechos y garantías del titular.

Orientaciones específicas para el principio de calidad en el tratamiento de datos personales en el desarrollo de IA

- Revisar de manera periódica los algoritmos que utilicen IA a fin de que los datos que se procesan para la toma de decisiones se mantengan exactos, completos y actualizados.
- Clasificar de manera precisa la información, es decir utilizando categorías de datos, a fin de que el sistema de IA haga predicciones, recomendaciones o decisiones correctas basadas en datos y modelos.
- Establecer medidas y mecanismos para evitar que se altere la veracidad de la información, en especial para los procesos de IA que generen bases de conocimiento.

/ 03. Orientaciones Específicas para el Cumplimiento de los Principios Rectores de la Protección de los Datos Personales

- Establecer plazos de conservación de la información personal en los sistemas de IA y de los medios de almacenamiento que la contiene, considerando que los datos personales deben ser suprimidos, destruidos, borrados o eliminados cuando ya no exista razón válida, legítima o lícita para su conservación.
- La destrucción de los medios de almacenamiento que contengan datos personales en los sistemas de IA debe hacerse utilizando métodos y técnicas de borrado seguro, basados en estándares y mejores prácticas, que garanticen que los datos no puedan ser recuperados y utilizarse de manera indebida.
- Establecer procesos periódicos de comunicación con responsables o autoridades para mejorar el gobierno de los datos y su gobernanza.

Principio de responsabilidad (Artículo 20 de los Estándares)

¿En qué consiste este principio?

El responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en los Estándares, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al titular y a la autoridad de control, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines.

Lo anterior, aplicará cuando los datos personales sean tratados por parte de un encargado a nombre y por cuenta del responsable, así como al momento de realizar transferencias de datos personales.

Entre los mecanismos que el responsable podrá adoptar para cumplir con el principio de responsabilidad se encuentran, de manera enunciativa más no limitativa, los siguientes:

a. Destinar recursos para la instrumentación de programas y políticas de protección de datos personales.
b. Implementar sistemas de administración de riesgos asociados al tratamiento de datos personales.
c. Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable.

/ 03. Orientaciones Específicas para el Cumplimiento de los Principios Rectores de la Protección de los Datos Personales

d. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales.

e. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.

f. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

g. Establecer procedimientos para recibir y responder dudas y quejas de los titulares.

Por último, el responsable revisará y evaluará permanentemente los mecanismos que para tal efecto adopte voluntariamente para cumplir con el principio de responsabilidad, con el objeto de medir su nivel de eficacia en cuanto al cumplimiento de la legislación nacional aplicable.

Orientaciones específicas para el principio de responsabilidad en el tratamiento de datos personales en el desarrollo de IA

- En el desarrollo y el uso de tecnología de IA, velar por el cumplimiento de los principios establecidos en los Estándares,debiendo adoptar las medidas necesarias para su aplicación, además de implementar mecanismos para acreditar su cumplimiento, esto aplicará aún y cuando en el tratamiento de los datos a través de esta tecnología, intervenga un tercero a solicitud del responsable.
- Para el cumplimiento con los principios establecidos en los Estándares, los responsables y desarrolladores de tecnología de IA, podrán valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que se determine adecuado para tales fines.
- Determinar responsabilidades y obligaciones claras de cada uno de los actores que intervienen en el proceso de diseño, desarrollo, implementación y uso de la tecnología.

/ 03. Orientaciones Específicas para el Cumplimiento de los Principios Rectores de la Protección de los Datos Personales

- Evitar que la toma de decisiones a través de una tecnología de IA incremente las desigualdades estructurales que se encuentran en la sociedad y/o genere daño o sufrimiento a individuos o grupo de personas.
- Revisar los sistemas de AI para evitar que produzcan resultados sociales sesgados, amplifiquen el sesgo humano o que sirvan como pretexto para tomar decisiones sesgadas.
- El responsable se asegurará que los servicios prestados por cualquier encargado que realice tratamiento de datos personales a través de tecnología de IA se apegue a lo establecido en el artículo 34 de los Estándares.
- Conservar la documentación que sustenta la selección de datos, cómo se desarrolló el algoritmo y si se probó adecuadamente antes de que se pusiera en uso.
- Supervisar constantemente las actividades realizadas por proveedores externos que ofrezcan servicios de IA que involucren el tratamiento de datos personales.
- Considerar la creación de normas para la industria, código de ética, así como foros con expertos en los campos de la tecnología y la protección de datos personales que proporcionen un asesoramiento sobre los desafíos legales, éticos, sociales, tecnológicos y las oportunidades vinculadas al uso de la IA.
- Adoptar esquemas de autorregulación o buenas prácticas en el tratamiento de datos personales a través de tecnologías de IA.
- Realizar evaluaciones regulares a los sistemas IA para asegurar que cumple con los requerimientos regulatorios.
- Recordar que dentro de los principios éticos que se deben observar en los sistemas de IA se encuentra el principio de explicabilidad, el cuál es necesario para construir y mantener la confianza de los usuarios de sistemas de IA, este busca que los procesos sean transparentes, es decir, que las capacidades y finalidades de los sistemas de IA se comuniquen abiertamente y las decisiones se expliquen, en la medida de lo posible a los afectados directa o indirectamente con el objetivo de rendir cuentas al titular sobre el tratamiento de datos personales en su posesión.

/ 03. Orientaciones Específicas para el Cumplimiento de los Principios Rectores de la Protección de los Datos Personales

Principio de Seguridad (Artículo 21 de los Estándares)

¿En qué consiste este principio?

En atención a este principio, el responsable establecerá y mantendrá, con independencia del tipo de tratamiento que efectúe, medidas de carácter administrativo, físico y técnico suficientes para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

Para la determinación de las medidas referidas, el responsable considerará los siguientes factores:

a. El riesgo para los derechos y libertades de los titulares, en particular, por el valor potencial cuantitativo y cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.
b. El estado de la técnica.
c. Los costos de aplicación.
d. La naturaleza de los datos personales tratados, en especial si se trata de datos personales sensibles.
e. El alcance, contexto y las finalidades del tratamiento.
f. Las transferencias internacionales de datos personales que se realicen o pretendan realizar.
g. El número de titulares.
h. Las posibles consecuencias que se derivarían de una vulneración para los titulares.
i. Las vulneraciones previas ocurridas en el tratamiento de datos personales.

Asimismo, el responsable llevará a cabo una serie de acciones que garanticen el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de las medidas de seguridad aplicables al tratamiento de los datos personales, de manera periódica.

Cuando el responsable tenga conocimiento de una vulneración de seguridad de datos personales ocurrida en cualquier fase del tratamiento, entendida como cualquier daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los datos personales aun cuando ocurra de manera accidental, notificará a la autoridad de control y a los titulares afectados dicho acontecimiento, sin dilación alguna.

Lo anterior, no resultará aplicable cuando el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de la vulneración de seguridad ocurrida, o bien, que ésta no represente un riesgo para los derechos y las libertades de los titulares involucrados.

/ 03. Orientaciones Específicas para el Cumplimiento de los Principios Rectores de la Protección de los Datos Personales

La notificación que realice el responsable a los titulares afectados estará redactada en un lenguaje claro y sencillo.

La notificación a que se refieren los numerales anteriores contendrá, al menos, la siguiente información:

a. La naturaleza del incidente.
b. Los datos personales comprometidos.
c. Las acciones correctivas realizadas de forma inmediata.
d. Las recomendaciones al titular sobre las medidas que éste pueda adoptar para proteger sus intereses.
e. Los medios disponibles al titular para obtener mayor información al respecto.

El responsable documentará toda vulneración de seguridad de los datos personales ocurrida en cualquier fase del tratamiento, identificando, de manera enunciativa más no limitativa, la fecha en que ocurrió; el motivo de la vulneración; los hechos relacionados con ella y sus efectos y las medidas correctivas implementadas de forma inmediata y definitiva, la cual estará a disposición de la autoridad de control.

La legislación nacional de los Estados Iberoamericanos aplicable en la materia establecerá los efectos de las notificaciones de vulneraciones de seguridad que realice el responsable a la autoridad de control, en lo que se refiere a los procedimientos, forma y condiciones de su intervención, con el propósito del salvaguardar los intereses, derechos y libertades de los titulares afectados.

Orientaciones específicas para el principio de seguridad en el tratamiento de datos personales en el desarrollo de IA

- Involucrar a las partes interesadas a lo largo del ciclo de vida del sistema de IA, a fin de decidir en conjunto, la solución respecto a las diferencias que pueda haber entre los principios de protección de datos personales y los requisitos del sistema de IA.
- Adoptar un marco de gobierno de datos que promueva el diseño, estructura y supervisión de las tecnologías de IA al interactuar durante los tratamientos de datos personales.

/ 03. Orientaciones Específicas para el Cumplimiento de los Principios Rectores de la Protección de los Datos Personales

- Identificar, evaluar, documentar y comunicar continuamente las políticas, concesiones, y soluciones, respecto al marco de gobierno de datos establecido.
- Evaluar y documentar los riesgos identificados al comenzar un desarrollo de inteligencia artificial y durante todo el ciclo de vida de los datos, a fin de prever las medidas de seguridad para evitar cualquier impacto adverso no deseado.
- Desarrollar sistemas de IA robustos con un enfoque preventivo de los riesgos, de manera tal que sean confiables, según lo previsto, a fin de minimizar los daños no intencionados, inesperados e inaceptables.
- Adoptar resiliencia a ataques de seguridad para los sistemas de IA, a fin de protegerse contra vulnerabilidades que puedan ser explotadas por atacantes.
- Establecer medidas de seguridad administrativas, físicas y técnicas, proporcionalmente a la magnitud del riesgo planteado en los distintos tratamientos de datos personales en IA y dependiendo de las capacidades del sistema.
- Asegurar que el desarrollo, despliegue y uso de los sistemas de IA cumplan con requisitos como: supervisión humana, robustez técnica y seguridad, privacidad y gobierno de datos, transparencia y responsabilidad.
- Facilitar la trazabilidad de datos y llevar a cabo auditorías de los sistemas de IA, especialmente en contextos o situaciones críticas.
- Fomentar la capacitación y la educación para que todas las partes interesadas estén informadas y capacitadas en IA confiable.

Principio de Confidencialidad (Artículo 23 de los Estándares)

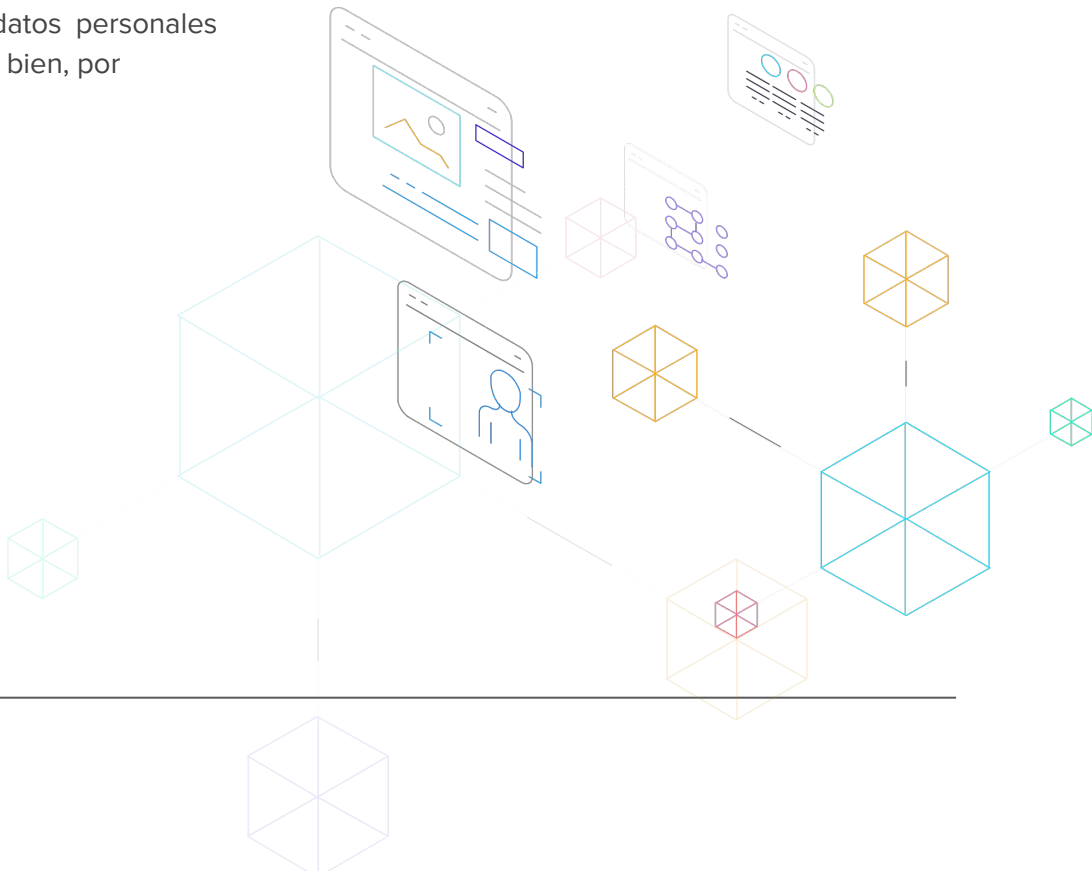
¿En qué consiste este principio?

El responsable establecerá controles o mecanismos para que quienes intervengan en cualquier fase del tratamiento de los datos personales mantengan y respeten la confidencialidad de los mismos, es decir, que los datos personales solamente sean tratados por personas y procesos autorizados, obligación que subsistirá aun después de finalizar sus relaciones con el titular.

/ 03. Orientaciones Específicas para el Cumplimiento de los Principios Rectores de la Protección de los Datos Personales

Orientaciones específicas para el principio de confidencialidad en el tratamiento de datos personales en el desarrollo de IA

- Evitar la difusión de datos personales tratados mediante tecnología de IA, sin el consentimiento de su titular.
- Mantener el secreto de la información relacionada con datos personales tratados mediante tecnología de IA, excepto cuando su comunicación se encuentre permitida en términos de una disposición legal.
- Definir claramente al personal autorizado para tener acceso la tecnología de IA que realiza el tratamiento de los datos personales de la organización, o bien, por terceros que actúen a nombre y por cuenta del responsable. Al respecto, se considera el uso de cláusulas contractuales que delimiten las obligaciones de los empleados dentro de la organización, así como de los encargados.
- Implementar medidas de seguridad necesarias para garantizar la secrecía de los datos personales tratados mediante la tecnología de IA.
- Considerar la pseudonimización o anonimización de los datos personales si es que la tecnología de IA lo permite sin que impacte en su funcionamiento.



RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 04. Orientaciones Específicas para el Cumplimiento de las Obligaciones por los Encargados del Tratamiento (Artículos 33 y 34 de los Estándares)

/ 04. Orientaciones Específicas para el Cumplimiento de las Obligaciones por los Encargados del Tratamiento (Artículos 33 y 34 de los Estándares)

El encargado realizará las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido del mismo, así como limitará sus actuaciones a los términos fijados por el responsable.

Es importante considerar que, la prestación de servicios entre el responsable y encargado se formalizará mediante la suscripción de un contrato o cualquier otro instrumento jurídico, en el que se establecerá al menos, el objeto, alcance, contenido, duración, naturaleza y finalidad del tratamiento; el tipo de datos personales; las categorías de titulares, así como las obligaciones y responsabilidades del responsable y encargado.

En todo caso, el contrato o instrumento jurídico establecerá, al menos, las siguientes cláusulas generales relacionadas con los servicios que preste el encargado:

a. Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable.
b. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable.
c. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables.
d. Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones.
e. Guardar confidencialidad respecto de los datos personales tratados.
f. Suprimir, devolver o comunicar a un nuevo encargado designado por el responsable los datos personales objeto de tratamiento, una vez cumplida la relación jurídica con el responsable o por instrucciones de éste, excepto que una disposición legal exija la conservación de los datos personales, o bien, que el responsable autorice la comunicación de éstos a otro encargado.
g. Abstenerse de transferir los datos personales, salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad de control.

/ 04. Orientaciones Específicas para el Cumplimiento de las Obligaciones por los Encargados del Tratamiento (Artículos 33 y 34 de los Estándares)

h. Permitir al responsable o autoridad de control inspecciones y verificaciones en sitio.

i. Generar, actualizar y conservar la documentación que sea necesaria y que le permita acreditar sus obligaciones.

j. Colaborar con el responsable en todo lo relativo al cumplimiento de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.

Cuando el encargado incumpla las instrucciones del responsable y decida por sí mismo sobre el alcance, contenido, medios y demás cuestiones del tratamiento de los datos personales asumirá la calidad de responsable.

Orientaciones específicas para la relación responsable-encargado en el tratamiento de los datos personales en el desarrollo de IA

- Supervisar constantemente las actividades realizadas por proveedores externos que ofrezcan servicios de IA que involucren el tratamiento de datos personales.
- Incluir en los contratos o instrumentos jurídicos instrucciones específicas[6] respecto a la forma en que los datos personales pueden ser usados por los encargados y las finalidades específicas para su tratamiento, lo anterior, debido a la complejidad de distinguir claramente entre responsable y encargados en el desarrollo de IA.

6. Se debe tener en cuenta que si la organización a la que se le encomendó el análisis de datos para el desarrollo de IA cuenta con la libertad y experiencia suficiente para decidir qué datos se obtienen y como aplicar sus propias técnicas analíticas, se convierte en responsable.

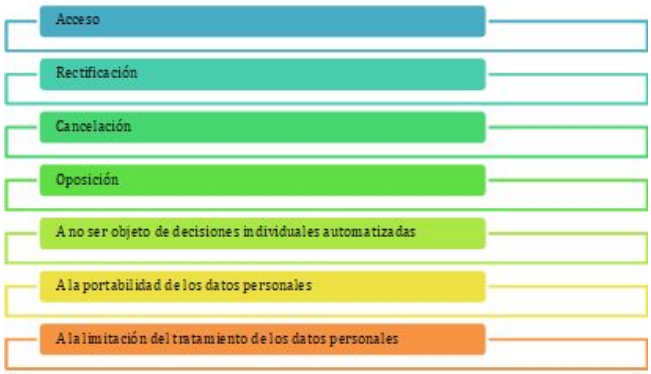
RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 05. Orientaciones Específicas para el Cumplimiento de los Derechos (Artículos 24 a 32 de los Estándares)

/ 05. Orientaciones Específicas para el Cumplimiento de los Derechos (Artículos 24 a 32 de los Estándares)

¿Cuáles son los derechos del titular?

El derecho a la protección de los datos personales permite a los individuos tener control sobre su información personal. Los Estándares reconocen los derechos de los titulares respecto del tratamiento de sus datos personales, los cuales son:



¿En qué consiste el derecho de acceso?

El titular tendrá el derecho de solicitar el acceso a sus datos personales que obren en posesión del responsable, así como a conocer cualquier información relacionada con las condiciones generales y específicas de su tratamiento.

¿En qué consiste el derecho de rectificación?

El titular tendrá el derecho a obtener del responsable la rectificación o corrección de sus datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados.

¿En qué consiste el derecho de cancelación?

El titular tendrá derecho a solicitar la cancelación o supresión de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.

/ 05. Orientaciones Específicas para el Cumplimiento de los Derechos (Artículos 24 a 32 de los Estándares)

¿En qué consiste el derecho de oposición?

El titular podrá oponerse al tratamiento de sus datos personales cuando:

1. Tenga una razón legítima derivada de su situación particular.
2. El tratamiento de sus datos personales tenga por objeto la mercadotecnia directa, incluida la elaboración de perfiles, en la medida que esté relacionada con dicha actividad. Cuando el titular se oponga al tratamiento con fines de mercadotecnia directa, sus datos personales dejarán de ser tratados para dichos fines.

¿En qué consiste el derecho a no ser objeto de decisiones individuales automatizadas?

El titular tendrá derecho a no ser objeto de decisiones que le produzcan efectos jurídicos o le afecten de manera significativa que se basen únicamente en tratamientos automatizados 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.

Lo anterior no resultará aplicable cuando el tratamiento automatizado de datos personales sea necesario para la celebración o la ejecución de un contrato entre el titular y el responsable; esté autorizado por el derecho interno de los Estados Iberoamericanos, o bien, se base en el consentimiento demostrable del titular.

No obstante, cuando sea necesario para la relación contractual o el titular hubiere manifestado su consentimiento tendrá derecho a obtener la intervención humana; recibir una explicación sobre la decisión tomada; expresar su punto de vista e impugnar la decisión.

Por último, el responsable no podrá llevar a cabo tratamientos automatizados de datos personales que tengan como efecto la discriminación de los titulares por su origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, así como datos genéticos o datos biométricos.

/ 05. Orientaciones Específicas para el Cumplimiento de los Derechos (Artículos 24 a 32 de los Estándares)

¿En qué consiste el derecho a la portabilidad de los datos personales?

Cuando se traten datos personales por vía electrónica o medios automatizados, el titular tendrá derecho a obtener una copia de los datos personales que hubiere proporcionado al responsable o que sean objeto de tratamiento, en un formato electrónico estructurado, de uso común y lectura mecánica, que le permita seguir utilizándolos y transferirlos a otro responsable, en caso de que lo requiera.

Para el ejercicio de este derecho se deberá tomar en cuenta que:

- El titular podrá solicitar que sus datos personales se transfieran directamente de responsable a responsable cuando sea técnicamente posible;
- El derecho a la portabilidad de los datos personales no afectará negativamente a los derechos y libertades de otros.
- Sin perjuicio de otros derechos del titular, el derecho a la portabilidad de los datos personales no resultará procedente cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.

¿En qué consiste el derecho a la limitación del tratamiento de los datos personales?

El titular tendrá derecho a que el tratamiento de datos personales se limite a su almacenamiento durante el periodo que medie entre una solicitud de rectificación u oposición hasta su resolución por el responsable.

Asimismo, el titular tendrá derecho a la limitación del tratamiento de sus datos personales cuando éstos sean innecesarios para el responsable, pero los necesite para formular una reclamación.

Orientaciones específicas para la atención de solicitudes de ejercicio de derechos en el tratamiento de datos personales en el desarrollo de IA

- Informar a los titulares cuando interactúan con una aplicación de IA.

/ 05. Orientaciones Específicas para el Cumplimiento de los Derechos (Artículos 24 a 32 de los Estándares)

- Asegurar que los sistemas de IA permitan el ejercicio de los derechos, estableciendo medios y procedimientos sencillos, expeditos, accesibles y gratuitos en cumplimiento a lo señalado por los Estándares.
- Revisar que el desarrollo de IA se encuentre programado de tal manera que cuando un titular ejerza alguno de estos derechos, el responsable pueda cumplir con lo solicitado de forma ordenada.
- En ejercicio del derecho de acceso: permitir que los titulares conozcan la lógica de los algoritmos utilizados en IA, por ejemplo, explicando, de ser posible, las variables que se utilizan y su peso; informar sobre el tipo de datos de entrada y de salida esperada; considerar la implementación de mecanismos para que los titulares verifiquen su perfil, incluidos los detalles de la información y las fuentes utilizadas para desarrollarlo.
- Considerar incluir herramientas para la administración de preferencias, como un panel de privacidad, de tal forma que, a través de este, el titular podrá administrar lo que sucede con su información a través de diversos servicios, además podrán modificar la configuración, actualizar sus datos personales, revisar o editar su perfil para corregir cualquier inexactitud.
- Informar a los titulares sobre el razonamiento subyacente en las operaciones de procesamiento de datos de IA que se les aplican. En la medida de lo posible, se debería considerar informar sobre las consecuencias de tal razonamiento.
- Reconocer el derecho de los titulares a no ser objeto de una decisión basada únicamente en el procesamiento automatizado si los afecta de manera significativa y, cuando no corresponda, garantizar el derecho de los individuos a impugnar tal decisión.
- Cuando se haga uso de un tratamiento automatizado, reconocer al titular el derecho a obtener intervención humana, de forma tal que pueda recibir una explicación del tratamiento y expresar su punto de vista, respetando siempre su expectativa razonable de privacidad.
- Contar con herramientas que de forma simple permitan a los titulares portar sus datos personales en caso de que sea viable a través de la tecnología de IA.[7]

7. Guidelines on the right to data portability https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 06. Orientaciones Específicas para la Aplicación de Medidas Proactivas en el Tratamiento de los Datos Personales de los Proyectos de IA.

/ 06. Orientaciones Específicas para la Aplicación de Medidas Proactivas en el Tratamiento de los Datos Personales de los Proyectos de IA.

La implementación de medidas proactivas en el tratamiento de datos personales en la legislación nacional de los Estados Iberoamericanos buscará promover el mejor cumplimiento de su legislación y coadyuvar a fortalecer y elevar los controles de protección de datos personales implantados por el responsable.

Privacidad por diseño y privacidad por defecto (artículo 38 de los Estándares).

¿Qué es la privacidad por diseño y por defecto?

El responsable aplicará, desde el diseño, en la determinación de los medios del tratamiento de los datos personales, durante el mismo y antes de recabar los datos personales, medidas preventivas de diversa naturaleza que permitan aplicar de forma efectiva los principios, derechos y demás obligaciones previstas en la legislación nacional que le resulte aplicable.

El responsable garantizará que sus programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen un tratamiento de datos personales, cumplan por defecto o se ajusten a los principios, derechos y demás obligaciones previstas en la legislación nacional que le resulte aplicable. Específicamente, con el fin de que únicamente sean objeto de tratamiento el mínimo de datos personales y se limite la accesibilidad de éstos, sin la intervención del titular, a un número indeterminado de personas.

Orientaciones específicas para la privacidad por diseño y por defecto en el tratamiento de los datos personales en el desarrollo de IA

- Desde el diseño de IA en el programa, sistema, plataforma o cualquier otra tecnología que implique el tratamiento de datos personales, el responsable deberá aplicar medidas que posibiliten el cumplimiento efectivo de las obligaciones que deriven de la normativa aplicable en materia de datos personales.
- Cuando se esté desarrollando IA, considerar la posibilidad de lograr los objetivos de una manera menos invasiva para los titulares, en términos de ética, cumplimiento de principios y valorando la relación entre usabilidad y privacidad.

/ 06. Orientaciones Específicas para la Aplicación de Medidas Proactivas en el Tratamiento de los Datos Personales de los Proyectos de IA.

- Reconocer la importancia de embeber la privacidad como requisito en el diseño y la arquitectura del programa, servicio, sistema, plataforma o cualquier otra tecnología de IA, con el objetivo de proponer medidas técnicas para los riesgos de privacidad identificados antes de que éstos se materialicen.
- Considerar que los desarrolladores de IA adapten la lógica de los algoritmos, de modo que los sistemas de IA permitan garantizar por defecto, la seguridad de los datos personales y así dar cumplimiento a las obligaciones en la materia.

Evaluación de impacto en la protección de datos personales (artículo 41 de los Estándares).

¿Qué es la Evaluación de Impacto en la protección de datos personales?

Cuando el responsable pretenda llevar a cabo un tipo de tratamiento de datos personales que, por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, realizará, de manera previa, a la implementación del mismo una evaluación del impacto a la protección de los datos personales.

Es decir, realizará un análisis documentado mediante el cual los responsables que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informática, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar posibles riesgos para dichos datos, con el objeto de conocer las medidas implementadas y por implementarse, para protegerlos y mitigar los riesgos identificados.

Ahora bien, la legislación nacional de los Estados Iberoamericanos que resulte aplicable en la materia señalará los tratamientos que requieran de una evaluación de impacto a la protección de datos personales; el contenido de éstas, los supuestos en que resulte procedente presentar el resultado ante la autoridad de control, así como los requerimientos de dicha presentación, entre otras cuestiones.

/ 06. Orientaciones Específicas para la Aplicación de Medidas Proactivas en el Tratamiento de los Datos Personales de los Proyectos de IA.

Orientaciones específicas para la evaluación de impacto en la protección de datos personales cuando se traten datos personales en el desarrollo de IA

- Realizar una Evaluación de impacto a la protección de datos personales siempre que se presente alguno de los siguientes supuestos:
  - Se traten datos personales.
  - Se utilice algún tipo de inteligencia artificial que pudiera percibirse como particularmente intrusiva de la privacidad.
  - La política pública, programa, sistema o plataforma informática en la que se pretende desarrollar IA, arroje resultados que pudieran llevar a la toma de acciones o decisiones con un impacto o afectación a los titulares.
- Elaborar la identificación del riesgo, que incluya los siguientes elementos:
  - Evaluar la necesidad de las operaciones de procesamiento en la utilización de IA, así como su proporcionalidad en relación con las finalidades de la política pública, programa, sistema o plataforma informática que se está desarrollando.
  - Identificar, en el contexto del uso de IA los riesgos potenciales para los titulares, incluyendo aquellos derivados del análisis de datos personales sensibles.
  - Evaluar los riesgos potenciales a los derechos y libertades de los titulares tutelados por la normativa que resulte aplicable de cada país.
- Evaluar las medidas implementadas y a implementar para mitigar los riesgos identificados en la utilización de IA.
- Evaluar periódicamente las operaciones de procesamiento con IA, a fin de revisar si las medidas implementadas para mitigar los riesgos por su uso están funcionando como se esperaba.
- Documentar las evaluaciones de impacto a la privacidad que se realicen, para que, en un momento específico, puedan presentarse a la Autoridad de Control o Autoridad de Protección de Datos competente, en el caso de una inspección o si surge una controversia al respecto.

RED IBEROAMERICANA DE PROTECCION DE DATOS

/ 07. Glosario

/ 07. Glosario

EIPD

Encuentro Iberoamericano de Protección de Datos

Estándares Iberoamericanos

Estándares de Protección de Datos Personales para los Estados

IA

Inteligencia Artificial

RIPD

Red Iberoamericana de Protección de Datos

RED
IBEROAMERICANA DE
PROTECCION
DE DATOS