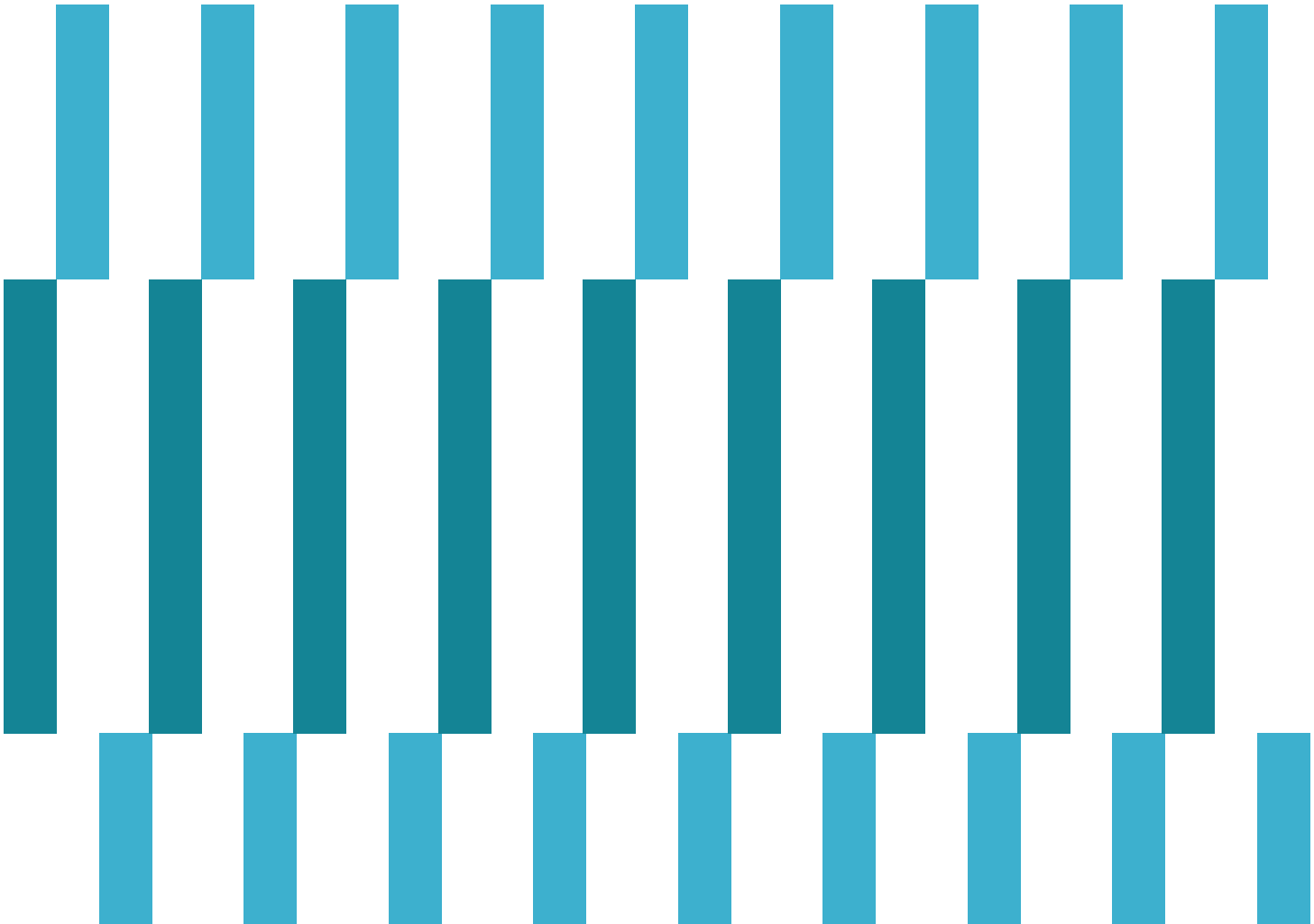
RED IBEROAMERICANA DE PROTECCION DE DATOS

Red Iberoamericana
Rede Ibero-Americana

Estándares de Protección de Datos de los Estados Iberoamericanos



Aprobados el 26 de mayo de 2026
en Cartagena de Indias, Colombia.

Antecedentes

En el marco del XV Encuentro Iberoamericano de Protección de Datos, la Red Iberoamericana de Protección de Datos (RIPD o Red) aprobó y presentó oficialmente los llamados "Estándares de Protección de Datos de los Estados Iberoamericanos", dando cumplimiento así a un objetivo largamente anhelado por todas las entidades integrantes de la misma, así como a uno de los acuerdos adoptados en la XXV Cumbre Iberoamericana de Jefes de Estado y de Gobierno, celebrada el 28 y 29 de octubre de 2016 en Colombia, relacionado con solicitar a la Red la elaboración de una propuesta para la cooperación efectiva relacionada con la protección de datos personales y privacidad.

El texto aprobado trataba de dar respuesta a uno de los ejes de la estrategia acordada por la RIPD en noviembre de 2016 en Montevideo, plasmada en el documento "RIPD 2020", consistente en "impulsar y contribuir al fortalecimiento y adecuación de los procesos regulatorios en la región, mediante la elaboración de directrices que sirvan de parámetro para futuras regulaciones o para la revisión de las existentes".

En este sentido, los Estándares Iberoamericanos se constituyen en un conjunto de directrices orientadoras que contribuyan a la emisión de iniciativas regulatorias de protección de datos personales en la región iberoamericana de aquellos países que aún no cuentan con estos ordenamientos, o en su caso, sirvan como referente para la modernización y actualización de las legislaciones existentes.

Entre los **objetivos** de los Estándares Iberoamericanos destacan los siguientes:

- Establecer un conjunto de principios y derechos comunes de protección de datos personales que los Estados Iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de contar con reglas homogéneas en la región.

- Garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física en los Estados Iberoamericanos, mediante el establecimiento de reglas comunes que aseguren el debido tratamiento de sus datos personales.

- Facilitar el flujo de los datos personales entre los Estados Iberoamericanos y más allá de sus fronteras, con la finalidad de coadyuvar al crecimiento económico y social de la región.

- Favorecer la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, con otras autoridades de control no pertenecientes a la región y autoridades y organismos internacionales en la materia.

Como antecedentes directos de estos Estándares, pueden citarse, por un lado, la adopción por la propia RIPD, en 2007, con ocasión del V Encuentro Iberoamericano de Protección de Datos, de las "Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana", con las que se pretendió establecer un "marco armonizado" de referencia para las iniciativas regulatorias nacionales que surgieran en la región en materia de protección de datos y, por otro, los estándares que fueron aprobados en la

Conferencia Internacional de Autoridades de Privacidad y de Protección de Datos, celebrada en Madrid en 2009, los llamados "Estándares de Madrid", que constituyeron, sin duda, un avance en la búsqueda de soluciones y disposiciones específicas "que podrían aplicarse independientemente de las diferencias que puedan existir entre los diferentes modelos existentes de protección de datos y privacidad".

En la elaboración de los Estándares Iberoamericanos también se tomaron como referencia otros instrumentos internacionales y emblemáticos en materia de protección de datos personales como son las Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales de la Organización para la Cooperación y Desarrollo Económicos; el Convenio número 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo; el Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico, y el Reglamento del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, entre otros.

Con la aprobación de estos Estándares, la RIPD dispuso de una herramienta esencial con la que poder afrontar con rigor el seguimiento y apoyo a los futuros desarrollos legislativos en la Región, debido a que los Estándares Iberoamericanos se caracterizan por ser un modelo normativo que:

- Responde a las necesidades y exigencias nacionales e internacionales que demanda el derecho a la protección de datos personales, en una sociedad donde las tecnologías de la información y del conocimiento cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana.

- Incluye las mejores prácticas nacionales e internacionales en la materia.

- Propone una serie de estándares tan flexibles que faciliten su adopción entre los Estados Iberoamericanos, sin contravenir de ninguna manera su derecho interno, de tal manera que este documento sea una realidad viva y viable en la región iberoamericana en beneficio del propio titular.

- Garantiza un nivel adecuado de protección de los datos personales en la región iberoamericana, con la finalidad de no establecer barreras a la libre circulación de éstos en los Estados Iberoamericanos y, en consecuencia, favorecer las actividades comerciales entre la región, así como con otras regiones económicas

Los Estados Iberoamericanos:

(1) Considerando que la protección de las personas físicas en relación con el tratamiento de sus datos personales es un derecho fundamental que se encuentra reconocido con rango máximo en la mayoría de las Constituciones Políticas de los Estados Iberoamericanos, bajo la forma del derecho a la protección de datos personales o habeas data, y que en algunos casos ha sido definido jurisprudencialmente por sus Tribunales o Cortes Constitucionales;

(2) Determinando que el derecho a la protección de datos personales se ha conceptualizado en algunos países Iberoamericanos, legislativamente o jurisprudencialmente, como un derecho de naturaleza distinta a los derechos a la vida privada y familiar, a la intimidad, al honor, al buen nombre y otros derechos similares, que en su conjunto garantizan el libre desarrollo de la personalidad de la persona física, hasta conformarse en un derecho autónomo, con características y dinámica propias, que tiene por objeto salvaguardar el poder de disposición y control que tiene toda persona física con respecto a la información que le concierne, fundamentalmente en atención al empleo de las tecnologías de la información y las comunicaciones que cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana;

(3) Asumiendo que salvaguardar el derecho de las personas físicas respecto al tratamiento de sus datos personales es compatible con el objetivo de garantizar y proteger otros derechos, los cuales se reconocen como indivisibles e interdependientes unos con otros, y que requieren de una protección conforme para resguardar en su esfera más amplia a las personas físicas en contra de intrusiones ilegales o arbitrarias, incluso aquellas derivadas del tratamiento de datos personales.

(4) Recordando que la Red Iberoamericana de Protección de Datos surgió con motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos, celebrado en La Antigua, Guatemala, del 1 al 6 de junio de 2003, con la asistencia de representantes de 14 países iberoamericanos. Iniciativa que contó desde sus inicios con un apoyo político reflejado en la Declaración Final de la XIII Cumbre de Jefes de Estado y de Gobierno de los países Iberoamericanos, celebrada en Santa Cruz de la Sierra, Bolivia, el 14 y 15 de noviembre de 2003, conscientes del carácter de la protección de datos personales como un derecho fundamental;

(5) Teniendo en cuenta que con motivo de la Resolución adoptada en la XXV Cumbre Iberoamericana de Jefes de Estado y de Gobierno, que tuvo lugar en Cartagena de Indias, Colombia, los días 28 y 29 de octubre de 2016, se reafirmó que la adopción, elaboración e impulso de diversos manuales, programas, iniciativas y proyectos fortalecerían la gestión e impacto de las acciones de cooperación entre los países de Iberoamérica;

(6) Asumiendo que la Red Iberoamericana de Protección de Datos se constituye en un foro permanente de intercambio de información abierto a todos los países miembros de la Comunidad Iberoamericana y que permite el involucramiento de los sectores público, privado y social, con la finalidad de promover los desarrollos normativos necesarios para garantizar una regulación avanzada del derecho a la protección de datos personales en un contexto democrático y global;

(7) Recordando que con motivo de la reunión celebrada en Santa Cruz de la Sierra, Bolivia, del 3 a 5 de mayo de 2006, se elaboró el documento denominado Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana, el cual establece un conjunto de disposiciones que tienen por objeto contribuir a la elaboración de las iniciativas regulatorias de la protección de datos que surjan en la Comunidad Iberoamericana, constituyéndose como un referente para el desarrollo de los Estándares;

(8) Teniendo en cuenta que la Unión Europea adoptó en su momento un nuevo marco normativo en la materia, con el objetivo de modernizar sus disposiciones y garantizar mayor solidez y coherencia en la protección efectiva del derecho fundamental a la protección de datos personales y, a su vez, facilitar el desarrollo de la economía digital, tanto en su mercado interior como en sus relaciones globales; marco normativo que se posiciona como un referente obligado y determinante para la elaboración de las legislaciones nacionales de protección de datos en Iberoamérica;

(9) Reconociendo que existe una falta de armonización en los Estados Iberoamericanos respecto al reconocimiento, adopción, definición y desarrollo de las figuras, principios, derechos y procedimientos que dan contenido al derecho a la protección de datos personales en sus legislaciones nacionales, lo cual, sin duda, dificulta actualmente hacer frente a los nuevos retos y desafíos para la protección de este derecho derivados de la constante y vertiginosa evolución tecnológica y la globalización en diversos ámbitos;

(10) Haciendo apremiante, en el marco de una constante innovación tecnológica, la adopción de instrumentos regulatorios que garanticen, por una parte, la protección de las personas físicas con relación al tratamiento de sus datos personales y, por la otra, el libre flujo de los datos personales que actualmente constituyen la base para el desarrollo, fortalecimiento e intercambio de bienes y servicios en una economía global y digital, sobre los cuales se erigen las economías de los Estados Iberoamericanos; incluyendo mecanismos efectivos de gobernanza del tratamiento, trazabilidad y supervisión de sistemas automatizados y de inteligencia artificial, orientados a garantizar la protección de los derechos y libertades fundamentales.

Tomando también en consideración las "Orientaciones Específicas para el Cumplimiento de los Principios y Derechos que Rigen la Protección de los Datos Personales en los Proyectos de Inteligencia Artificial" y las "Recomendaciones Generales para el Tratamiento de Datos en Inteligencia Artificial" aprobadas por la Red Iberoamericana de Protección de Datos el 21 de junio de 2019, en Naucalpan de Juárez, México

(11) Acordando que para garantizar un nivel alto de protección de los derechos y libertades de las personas físicas, entre otras cuestiones, se requiere, a su vez, un nivel uniforme y elevado de protección de las personas físicas con respecto a su información personal que responda a las necesidades y exigencias actuales en un contexto global, con la finalidad de no establecer barreras a la libre circulación de los datos personales en los Estados Iberoamericanos y, en consecuencia, favorecer las actividades comerciales entre la región, así como con otras regiones económicas;

(12) Aceptando que con el objetivo de ampliar y fortalecer el régimen de protección de las personas físicas respecto al tratamiento de sus datos personales, es imperioso establecer un equilibrio entre los intereses de todos los actores del sector público, privado y social y titulares involucrados, incluyendo el establecimiento de excepciones por cuestiones de interés público que sean razonables y compatibles con los derechos y libertades, para evitar incurrir en restricciones o limitaciones injustificadas o desproporcionadas que no sean acordes con los fines perseguidos en sociedades democráticas;

(13) Estando conscientes acerca de los riesgos potenciales que pueden derivarse en la esfera de las personas físicas con motivo del tratamiento de sus datos personales a gran escala efectuado por parte de organismos públicos y privados y, en particular, teniendo en cuenta la especial vulnerabilidad de las niñas, niños y adolescentes, quienes demandan de garantías adecuadas y suficientes de protección frente a usos indebidos o arbitrarios de su información personal, preservando de esta manera su interés superior, el libre desarrollo de su personalidad, su seguridad y otros valores que son objeto de máxima protección por parte de los Estados Iberoamericanos. Estos riesgos pueden verse amplificados mediante tratamientos automatizados, incluyendo aquellos realizados mediante sistemas de inteligencia artificial capaces de inferir, clasificar, perfilar o influir significativamente en las personas.

(14) Conviniendo que el desarrollo tecnológico facilita el tratamiento de nuevas categorías de datos personales que presentan riesgos específicos, en particular el uso inadecuado de los mimos; por lo que resulta altamente relevante lograr un consenso mínimo respecto de las categorías de datos personales considerados con el carácter de sensible o especialmente protegidos, así como de las reglas para su tratamiento, teniendo en cuenta que las consecuencias e injerencias negativas que pueden derivarse a partir del uso indebido de este tipo de datos personales pueden generar condiciones injustas o discriminatorias para las personas físicas;

(15) Admitiendo que no todos los Estados Iberoamericanos cuentan con una legislación en la materia, situación que puede provocar afectaciones en el resguardo y tratamiento de la información personal, si se considera el acelerado uso de las tecnologías de la información que facilitan y permiten una comunicación masiva de datos personales de manera inmediata y casi ilimitada;

(16) Estableciendo que las legislaciones en materia de protección de datos personales de los Estados Iberoamericanos deben adoptar los referentes contenidos en los presentes Estándares para contar con un marco regulatorio armonizado que ofrezca un nivel de protección a las personas físicas respecto al tratamiento de sus datos personales y, a su vez, garantizando el desarrollo comercial y económico de la zona;

(17) Enfatizando la necesidad de que en los Estados Iberoamericanos se traten los datos personales bajo los mismos estándares y reglas homogéneas que ofrezcan a los titulares las mismas garantías de protección, a través del establecimiento de un catálogo de principios de obligado cumplimiento que responda a los actuales estándares nacionales e internacionales en la materia, así como a las exigencias que demanda un efectivo ejercicio y respeto de este derecho fundamental;

(18) Reconociendo que con el propósito de garantizar de manera efectiva el derecho a la protección de datos personales, es preciso adoptar un marco regulatorio que reconozca a cualquier persona física, en su carácter de titular de sus datos personales, la posibilidad de ejercer, por regla general de manera gratuita y excepcionalmente con costos asociados por razones naturales de reproducción, envío, certificación u otras, los derechos de acceso, rectificación, cancelación, oposición y portabilidad, inclusive en el contexto de tratamientos de datos personales efectuados por motores o buscadores de Internet; derechos que complementan las condiciones necesarias

para que los titulares ejerzan de manera plena su derecho a la autodeterminación informativa;

(19) Resaltando la importancia y el papel fundamental que desempeñan los prestadores de servicios que tratan datos personales a nombre y por cuenta del responsable, incluyendo aquéllos que prestan servicios de cómputo en la nube y otras materias, lo cual conlleva a los Estados Iberoamericanos a adoptar, en un mundo globalizado, un régimen que les permita regular este tipo de servicios con la finalidad de establecer una serie de garantías para la protección de los datos personales que con motivo de su encargo poseen y tratan, sin eximir al responsable de sus obligaciones y responsabilidades que tiene ante los titulares y las autoridades de control;

(20) Considerando que el desarrollo de las nuevas tecnologías de la información y las comunicaciones así como los servicios desarrollados en el contexto de la economía digital están contribuyendo al crecimiento continuado de los flujos transfronterizos de datos personales en el marco de una sociedad global, es ineludible la obligación de establecer una base mínima que facilite y permita a responsables y encargados, en su calidad de exportadores, la realización de transferencias internacionales de datos personales con pleno respeto a los derechos de los titulares;

(21) Teniendo en cuenta que mediante el Internet es posible acceder y recabar información disponible en cualquier país, así como llevar a cabo un tratamiento de la misma, como recabar datos de millones de personas sin estar físicamente domiciliado allí, circunstancia que no debería constituirse en un factor que impida la efectiva protección de los derechos y libertades de las personas en el ciberespacio;

(22) Reconociendo la importancia de la adopción de medidas preventivas que permitan al responsable responder proactivamente ante los posibles problemas relacionados con el derecho a la protección de datos personales como son la adopción de esquemas de autorregulación vinculante o sistemas de certificación en la materia; la designación de un oficial de protección de datos personales; la elaboración de evaluaciones de impacto a la protección de datos personales y la privacidad por defecto y por diseño, entre otras, lo cual resulta esencial en el ámbito de las tecnologías de la información y las telecomunicaciones; la gobernanza algorítmica, la trazabilidad, la supervisión humana efectiva, la evaluación continua de riesgos, la documentación técnica y la auditoría periódica de sistemas automatizados y de inteligencia artificial.

(23) Admitiendo la imperiosa necesidad de que cada Estado Iberoamericano cuente con una autoridad de control independiente e imparcial en sus potestades cuyas decisiones únicamente puedan ser recurribles por el control judicial, ajena a toda influencia externa, con facultades de supervisión e investigación en materia de protección de datos personales y encargada de vigilar el cumplimiento de la legislación nacional en la materia, la cual esté dotada de recursos humanos y materiales suficientes para garantizar el ejercicio de sus poderes y el desempeño efectivo de sus funciones;

(24) Reconociendo que los Estados Iberoamericanos están obligados a adoptar un régimen que garantice a los titulares una serie de mecanismos y procedimientos para

presentar sus reclamaciones ante la autoridad de control cuando consideren vulnerado su derecho a la protección de datos personales, así como para ser indemnizados cuando hubieren sufrido daños y perjuicios como consecuencia de una violación de su derecho;

(25) Destacando la importancia de establecer una base mínima para la cooperación internacional entre las autoridades de control latinoamericanas y entre éstas y las de ter- ceros países, con la finalidad de favorecer y facilitar la aplicación de la legislación en la materia y una protección efectiva de los titulares;

Han convenido en adoptar los presentes Estándares como máxima prioridad en la Comunidad Iberoamericana para que con el carácter de directrices orientadoras contribuyan a la emisión de iniciativas regulatorias de protección de datos personales en la región de los países que aún no cuentan con estos ordenamientos, o en su caso, sirvan como referente para la modernización y actualización de las legislaciones existentes, favoreciendo la adopción de un marco regulatorio armonizado que ofrezca un nivel adecuado de protección de las personas físicas respecto al tratamiento de sus datos personales y garantizando, a su vez, el desarrollo comercial y económico de la región.

Capítulo I
Disposiciones generales

1. Objeto

1.1 Los presentes Estándares tienen por objeto:

a. Establecer un conjunto de parámetros normativos, en torno al derecho a la protección de datos personales, que sirvan de orientación a legisladores, hacedores de política pública y, en general, tomadores de decisión, en los Estados Iberoamericanos para la construcción, diseño o modernización de legislación, reglamentos y, en general, cualquier regulación en la materia.

b. Contribuir al impulso de la interoperabilidad de regulaciones en el ámbito de la protección de los datos personales, con el objetivo de favorecer el desarrollo de marcos normativos que faciliten la cooperación entre autoridades de protección de datos personales y, especialmente, el fortalecimiento de la protección de los derechos y libertades fundamentales, en Iberoamérica, en beneficio de las personas.

c. Fomentar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física o natural, en los Estados Iberoamericanos, mediante el desarrollo de directrices, criterios y parámetros comunes que contribuyan a al fortalecimiento de este derecho en el ámbito nacional, así como en la región iberoamericana.

d. Establecer bases comunes en materia de transferencias internacionales de datos, para facilitar el flujo de los datos personales entre los Estados Iberoamericanos y más allá de sus fronteras, con la finalidad de coadyuvar al desarrollo social y crecimiento económico de la región.

e. Impulsar el desarrollo de mecanismos para la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, autoridades de control no pertenecientes a la región y autoridades y entidades internacionales en la materia.

f. Impulsar y promover el reconocimiento y aplicación efectiva de la autodeterminación informativa, como condición indispensable para el libre desarrollo de la personalidad, con la finalidad de permitir a las personas decidir sobre la forma en la que cada uno se ve a sí mismo y como desea proyectarse hacia los demás, entre otros aspectos.

1.2. Perspectiva de derechos humanos y de género

a. La aplicación e interpretación de normativa sobre protección de datos personales deberá orientarse conforme a una perspectiva transversal de género y de derechos humanos, procurando mitigar, al máximo posible, todo impacto negativo en la esfera de derechos de las personas, particularmente, en las que enfrentan situaciones de vulnerabilidad.

1.3. Interrelación normativa y ecosistema digital

Con la finalidad de propiciar la existencia de marcos regulatorios, equilibrados y efectivos, se procurará tener en cuenta los siguientes parámetros:

a. La coherencia normativa, ya sea evitando la duplicidad entre regulaciones, o bien la inconsistencia conceptual, tratándose de contenidos transversales. Lo anterior, en especial con relación a las normas del ecosistema digital.

b. El impacto de la regulación en términos de evitar cargas administrativas desproporcionadas, con una eficacia limitada.

c. La promoción de mecanismos de gobernanza digital y algorítmica que permitan asegurar la trazabilidad, supervisión, auditabilidad y control de tratamientos automatizados, sistemas de inteligencia artificial y otras tecnologías emergentes o disruptivas.

2. Definiciones

2.1 Los presentes Estándares recomiendan el diseño y alcance de las siguientes definiciones:

a. **Anonimización:** procedimiento en virtud del cual se realiza un tratamiento de datos personales con fines de impedir la identificación o reidentificación del titular de los mismos. Es irreversible por la imposibilidad de reidentificar razonablemente al titular de los datos personales.

b. **Autoridad de protección de datos personales:** institución pública del Estado, de carácter administrativo, dotada de plena autonomía e independencia para ejercer adecuadamente sus funciones de supervisión del cumplimiento de la regulación, así como de garante del efectivo ejercicio de los derechos y libertades fundamentales de los titulades.

c. **Consentimiento:** manifestación de la voluntad, libre, específica, inequívoca e informada, del titular a través de la cual acepta y autoriza el tratamiento de los datos personales que le conciernen.

d. **Datos Personales:** cualquier información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando esto no requiera plazos o actividades desproporcionadas.

e. **Datos biométricos:** aquellos obtenidos a partir de un tratamiento técnico específico relativos a las características físicas, fisiológicas o conductuales de una persona física o natural que permitan identificarla o verificar su identidad de manera única.

f. **Datos genéticos:** datos personales relativos a las características genéticas heredadas o adquiridas de una persona física o natural que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

g. **Datos de salud:** datos personales relativos a la salud física o mental de una persona física o natural, incluida la información sobre prestación de servicios de atención sanitaria, siempre que dicha información revele datos sobre el estado de salud de un titular de datos.

h. **Datos personales sensibles o categorías especiales de datos:** aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen de las personas; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud; datos biométricos; neurodatos; información neuronal que pueda inferir información personal, sensible o de estados emocionales; preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física.

i. **Elaboración de perfiles:** tratamiento automatizado de datos personales para evaluar determinados aspectos personales de una persona física o natural, entre otros para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona.

j. **Encargado:** prestador de servicios, que con el carácter de persona física o jurídica o autoridad pública, ajena a la organización del responsable, trata datos personales a nombre y por cuenta de éste.

k. **Exportador:** persona física o jurídica de carácter privado, autoridad pública, servicios, organismo o prestador de servicios situado en territorio de un Estado que efectúe transferencias internacionales de datos personales, conforme a lo dispuesto en los presentes Estándares.

l. **Investigación científica:** cualquier investigación que pueda apoyar la innovación, el desarrollo tecnológico y la demostración. Estas acciones deberán contribuir al conocimiento científico existente o aplicar el conocimiento existente de maneras novedosas, llevarse a cabo con el objetivo de contribuir al crecimiento del conocimiento general y el bienestar de la sociedad y ajustarse a las normas éticas en el área de investigación pertinente. Esto no excluye que la investigación pueda también perseguir un interés comercial.

m. **Limitación del tratamiento:** identificación de los datos personales para ser conservados con el fin de limitar su tratamiento, en el sucesivo, hasta en tanto se levante dicha medida o se deje sin efectos.

n. **Neurodatos:** datos relacionados con el funcionamiento, la actividad o la estructura del cerebro humano, de una persona física o natural, viva, que incluyen información única sobre su fisiología, salud o estados mentales que permiten la identificación o hacen identificable a su titular.

ñ. **Responsable:** persona física o jurídica de carácter privado, autoridad pública, servicio u organismo que, solo o en conjunto con otros, determina los fines, medios, alcance y demás cuestiones relacionadas con un tratamiento de datos personales.

o. **Seudonimización:** proceso mediante el cual los datos personales se modifican de modo que no resulte posible atribuirlos a su titular, sin requerir información adicional, siempre que dicha información adicional se encuentre por separado y esté sujeta a medidas de seguridad destinadas a asegurar que los datos personales no se puedan atribuir a una persona, física o natural, identificada o identificable.

p. **Titular:** persona física o natural a quien le conciernen o corresponden los datos personales.

q. **Tercero:** persona física, natural, o jurídica, autoridad, institución, servicio u organismo público, distinto del titular, del responsable y del encargado.

r. **Tratamiento:** cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre datos personales, relacionadas, de manera enunciativa mas no limitativa, con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales.

s. **Vulneración de la seguridad de los datos personales:** toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. Ámbito de aplicación subjetivo

3.1. Los presentes Estándares están diseñados para ser un marco de referencia destinado para tener por sujetos regulados a las personas, físicas o naturales, o jurídicas de carácter privado, autoridades y organismos públicos, que traten datos personales en el ejercicio de sus actividades y funciones.

4. Ámbito de aplicación objetivo

4.1. Los presentes Estándares fueron diseñados para ser un marco de referencia destinado a ser aplicable al tratamiento de datos personales que obren en soportes físicos, automatizados total o parcialmente, o en ambos soportes, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

4.2. Los presentes Estándares fueron diseñados para ser un marco de referencia destinado a ser aplicable a los datos personales de personas físicas o naturales, en su calidad de titulares de datos.

4.3. Los Estándares fueron diseñados para ser un marco de referencia en el que se consideran excepciones válidas los siguientes supuestos:

a) Cuando los datos personales estén destinados a actividades exclusivamente en el marco de la vida familiar o doméstica de una persona física o natural, esto es, la utilización de datos personales en un entorno de amistad, parentesco o grupo personal cercano y que no tengan como propósito una divulgación o utilización comercial.

b) Los datos personales sometidos a un proceso efectivo de anonimización.

4.4. La legislación nacional de los Estados Iberoamericanos podrá establecer excepciones o limitaciones al cumplimiento del marco general de protección de datos personales.

Para su legitimidad, estas excepciones o limitaciones se deberán diseñar, exclusivamente, como medida necesaria en una sociedad democrática para hacer frente a amenazas a la seguridad del Estado, la seguridad pública y su prevención, o bien, a las autoridades competentes con fines de prevención, investigación y enjuiciamiento de infracciones penales, así como su ejecución de sanciones.

Para el diseño adecuado de disposiciones destinadas a crear excepciones, se deberá seguir el esquema previsto en el numeral 6 de estos Estándares.

5. Ámbito de aplicación territorial

5.1. Los Estándares recomiendan que las legislaciones nacionales correspondientes se diseñen para ser aplicables al tratamiento de datos personales efectuado:

a. Por un responsable o encargado establecido en territorio de los Estados Iberoamericanos.

b. Por un responsable o encargado no establecido en territorio de los Estados Iberoamericanos, cuando las actividades del tratamiento estén relacionadas con la oferta de bienes o servicios dirigidos a los residentes de los Estados Iberoamericanos, o bien, estén relacionadas con el control de su comportamiento, en la medida en que éste tenga lugar en los Estados Iberoamericanos.

c. Por un responsable o encargado que no esté establecido en un Estado Iberoamericano pero le resulte aplicable la legislación nacional de dicho Estado, derivado de la celebración de un contrato o en virtud del derecho internacional público.

d. Por un responsable o encargado no establecido en territorio de los Estados Iberoamericanos y que utilice o recurra a medios, automatizados o no, situados en ese territorio para tratar datos personales, salvo que dichos medios se utilicen solamente con fines de tránsito.

5.2. Para los efectos de los presentes Estándares, se entenderá por establecimiento el lugar de la administración central o principal del responsable o encargado, el cual deberá determinarse en función de criterios objetivos e implicar el ejercicio efectivo y real de actividades de gestión que determinen las principales decisiones en cuanto a los fines y medios del tratamiento de datos personales que lleve a cabo, a través de modalidades estables.

5.3. La presencia y utilización de medios técnicos y tecnologías para el tratamiento de datos personales o las actividades de tratamiento no constituirán, en sí mismas, un establecimiento principal y no serán considerados como criterios determinantes para la definición del establecimiento principal del responsable o encargado.

5.4. Cuando el tratamiento de datos personales lo realice un grupo empresarial, el establecimiento principal de la empresa que ejerce el control deberá considerarse el establecimiento principal del grupo empresarial, excepto cuando los fines y medios del tratamiento los determine efectivamente otra de las empresas del grupo.

6. Excepciones generales al derecho a la protección de datos personales

6.1. La legislación nacional de los Estados Iberoamericanos aplicable en la materia podrá limitar el derecho a la protección de datos en términos de lo previsto en el numeral 4.4.

6.2. Las excepciones y limitaciones serán reconocidas de manera expresa en una ley en sentido formal y material, con el propósito de brindar certeza suficiente a los titulares acerca de la naturaleza y alcances de la medida.

6.3. En el caso de que alguno de los Estados Iberoamericanos advierta la necesidad de prever alguna excepción o limitación al derecho a la protección de datos personales, se

recomienda que la legislación, donde se establezca, indique, como mínimo, disposiciones relativas a:

a. La finalidad del tratamiento.

b. Las categorías de datos personales de que se trate.

c. El alcance de las limitaciones establecidas.

d. Las garantías adecuadas para evitar accesos o transferencias ilícitas o desproporcionadas.

e. La determinación del responsable o responsables.

f. Los plazos de conservación de los datos personales.

g. Los posibles riesgos para los derechos y libertades de los titulares.

h. El derecho de los titulares a ser informados sobre la limitación, salvo que resulte perjudicial o incompatible a los fines de ésta.

6.4. Las leyes deberán ser necesarias, adecuadas y proporcionales en una sociedad democrática, y deberán respetar los derechos y las libertades fundamentales de los titulares.

7. Ponderación del derecho a la protección de datos personales

7.1. Los Estados Iberoamericanos podrán establecer excepciones, en su constitución, legislación o en resoluciones de los tribunales, al cumplimiento de ciertos principios o derechos en materia de protección de datos personales, exclusivamente en la medida en que resulte necesario para la salvaguarda de otros derechos y libertades fundamentales, que así lo ameriten y justifiquen, como podría presentarse en el caso la libertad de expresión, prensa e información, entre otros.

Las excepciones deberán aplicarse de forma estricta, adoptando medidas proporcionales a los objetivos perseguidos, debiendo en todo momento, esa limitación, estar justificada, así como ser adecuada y proporcional en una sociedad democrática.

7.2. Esta exención deberá requerir de un ejercicio de ponderación con la finalidad de determinar la necesidad, idoneidad y proporcionalidad de la restricción o excepción conforme a las reglas y criterios que establezcan los Estados Iberoamericanos en su derecho interno.

8. Tratamiento de datos personales de niñas, niños y adolescentes, responsabilidad reforzada

8.1. En el tratamiento de datos personales concernientes a niñas, niños y adolescentes, los Estados Iberoamericanos privilegiarán la protección del interés superior de éstos,

conforme a la Convención sobre los Derechos del Niño y demás instrumentos internacionales que busquen su bienestar, el respeto de su autonomía progresiva y protección integral.

8.2. Los Estados Iberoamericanos promoverán:

a. En la formación académica de las niñas, niños y adolescentes, el uso responsable, adecuado y seguro de las tecnologías de la información y comunicación y los eventuales riesgos a los que se enfrentan en ambientes digitales respecto del tratamiento indebido de sus datos personales, así como el respeto de sus derechos y libertades.

b. El diseño e implementación de políticas destinadas a lograr que la información dirigida a menores se presente en lenguaje claro, sencillo y accesible para que comprenda las implicaciones sobre el tratamiento de sus datos personales.

8.3. El tratamiento de datos personales de niñas, niños y adolescentes deberá ser objeto de medidas especiales de responsabilidad reforzada. La naturaleza e intensidad de dichas medidas deberá determinarse con un enfoque basado en riesgo, de acuerdo con su interés superior y protección integral.

Entre el tipo de medidas a considerar están las configuraciones por defecto protectoras, las limitaciones de acceso, restricciones a perfiles y publicidad comportamental, la verificación efectiva de la edad, cuando resulte pertinente, los sistemas de recomendación ajustados para evitar contenidos nocivos, las herramientas para bloquear, silenciar y controlar grupos, la prohibición de descargas y/o capturas de pantalla de contenido sobre menores, entre otras.

9. Tratamiento de neurodatos

9.1. El tratamiento de datos neuronales deberá ser objeto de medidas especiales de responsabilidad reforzada. La naturaleza e intensidad de dichas medidas deberá determinarse con un enfoque basado en riesgo.

En el tratamiento de datos neuronales se deberá tener especial cuidado en el cumplimiento de los principios de minimización, exactitud, transparencia, lealtad, seguridad y responsabilidad proactiva.

9.2. Se consideran tratamientos de alto riesgo con datos neuronales, los que tengan por objeto:

a. Inferir indebidamente estados mentales o convicciones íntimas.

b. Modificar indebidamente la voluntad, las decisiones o el comportamiento de las personas.

c. Vigilar masivamente en contextos laborales, educativos o gubernamentales, con fines de control o supervisión.

d. Identificar o autenticar a las personas por medio de patrones neuronales.

Los tratamientos descritos podrían ser materia de prohibiciones en la legislación de los Estados Iberoamericanos.

10. Tratamiento de datos personales de carácter sensible o de categorías especiales de datos

10.1. El responsable no podrá tratar datos personales sensibles, o categorías especiales de datos, salvo que se presente alguna de las excepciones que se describen:

a. El tratamiento resulte indispensable por razones de interés público, para lo cual, se deberá analizar la proporcionalidad en atención al objetivo perseguido, respetando en lo esencial el derecho a la protección de datos y estableciendo medidas adecuadas para la protección de los intereses y derechos fundamentales del titular.

b. El tratamiento se produzca con relación a datos personales que su titular haya hecho manifiestamente públicos.

c. El tratamiento sea necesario para la protección de intereses vitales del titular o de otra persona, en el caso de que de que el titular de datos no esté capacitado, física o jurídicamente, para dar su consentimiento.

d. El tratamiento sea requerido para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.

e. El tratamiento sea necesario con fines de investigación científica o histórica o fines estadísticos, para lo cual, se deberá analizar la proporcionalidad en atención al objetivo perseguido, respetando en lo esencial el derecho a la protección de datos y estableciendo medidas adecuadas para la protección de los intereses y derechos fundamentales del titular de los datos.

f. El tratamiento resulte necesario por razones de interés público, en el ámbito de la salud pública, frente a amenazas transfronterizas graves para la salud, para garantizar niveles adecuados de calidad y de seguridad de la asistencia sanitaria y de medicamentos o productos sanitarios, para lo cual, deberán adoptarse las medidas adecuadas para proteger los derechos y libertades del titular de datos.

g. Se trate de datos biométricos necesarios con el propósito de confirmar la identidad de un titular de datos, siempre y cuando los citados datos biométricos, o los medios necesarios para la verificación, estén bajo el control exclusivo del titular de datos.

10.2. La legislación nacional de los Estados Iberoamericanos aplicable en la materia podrá establecer excepciones, garantías y condiciones adicionales para asegurar el debido tratamiento de los datos personales sensibles, de conformidad con su derecho interno.

Capítulo II
Principios de protección de datos personales

11. Principios aplicables al tratamiento de datos personales

11.1. En el tratamiento de datos personales se deberá cumplir los principios de legitimación o licitud, lealtad, transparencia, finalidad, o minimización, calidad, responsabilidad proactiva y demostrada, seguridad y confidencialidad.

La lectura, interpretación, aplicación e implementación de estos principios deberá realizarse desde un enfoque respetuoso de la dignidad humana, particularmente, con el propósito de hacer efectiva la autonomía personal, la integridad física y psíquica, así como para evitar la instrumentalización de las personas o su discriminación.

En todo caso, se deberá evitar que se produzcan limitaciones o afectaciones desproporcionadas, en torno a la autonomía y a la no instrumentalización de las personas, especialmente en el contexto de tratamientos de alto riesgo o relacionados con inferencias sobre datos sensibles o especialmente protegidos. Las inferencias, perfiles, predicciones o datos derivados generados a partir del tratamiento de datos personales deberán estar sujetos a garantías adecuadas de calidad, pertinencia, proporcionalidad y supervisión.

12. Principio de legitimación y licitud

12.1. Se consideran causas habilitantes válidas para el tratamiento de datos personales, las siguientes:

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, de conformidad con la ley aplicable en cada país, siempre que se cumpla con las siguientes condiciones:

1) Estar en presencia de un interés legítimo lícito relacionado con actividades reales, por lo que, de tratarse de situaciones hipotéticas, no será válido.

2) Haber valorado y determinado que no existen alternativas razonables, igual de eficaces, menos intrusivas, para lograr los fines perseguidos. De existir alguna alternativa razonable, con la misma eficacia, no es procedente el interés legítimo.

3) Haber desarrollado un ejercicio de ponderación para cerciorarse que los intereses individuales, junto con los derechos y libertades fundamentales, de los titulares, no prevalecen ante ese interés legítimo. Para este propósito, se deberá considerar los intereses de los titulares, el impacto del tratamiento y sus expectativas razonables, así como la existencia de salvaguardas adicionales que podrían limitar el impacto en el titular de los datos. Durante este ejercicio de ponderación se deberá tener especial cuidado si el titular es un niño, niña o adolescente.

Las autoridades, instituciones, entidades, organismos o servicios públicos del Estado, estarán impedidos para utilizar el interés legítimo como causa habilitante para el tratamiento de datos personales, en el ejercicio de sus funciones o atribuciones.

13. Condiciones para el consentimiento

13.1. Cuando sea necesario obtener el consentimiento del titular, el responsable demostrará de manera indubitable que el titular otorgó su consentimiento, ya sea a través de una declaración o una acción afirmativa clara.

13.2. En el caso de que el consentimiento se produzca en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de esos otros asuntos, de forma comprensible y de fácil acceso y con un lenguaje claro y sencillo. Todo consentimiento obtenido mediante prácticas contrarias a la normativa aplicable carecerá de validez.

13.3. Siempre que sea requerido el consentimiento para el tratamiento de los datos personales, el titular podrá revocarlo en cualquier momento, para lo cual el responsable establecerá mecanismos sencillos, ágiles, eficaces y gratuitos.

14. Consentimiento para el tratamiento de datos personales de niñas, niños y adolescentes

14.1. En la obtención del consentimiento de niñas, niños y adolescentes, el responsable obtendrá la autorización del titular de la patria potestad o tutela, conforme a lo dispuesto

en las reglas de representación previstas en el derecho interno de los Estados Iberoamericanos, o en su caso, solicitará directamente la autorización del menor de edad si el derecho interno de cada Estado Iberoamericano ha establecido una edad mínima para que lo pueda otorgar directamente y sin representación alguna del titular de la patria potestad o tutela. El consentimiento obtenido de forma contraria a lo aquí establecido se considerará ilícito.

14.2. El responsable realizará esfuerzos razonables para verificar que el consentimiento fue otorgado por el titular de la patria potestad o tutela, o bien, por el menor directamente atendiendo a su edad de acuerdo con el derecho interno de cada Estado Iberoamericano, teniendo en cuenta la tecnología disponible.

14.3. El tratamiento para la elaboración de perfiles con fines publicitarios requeriría, en su caso, de un consentimiento específico y separado del consentimiento para otros tratamientos.

15. Principio de lealtad

15.1. 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.

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

16. Principio de transparencia

16.1. 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.

16.2. El titular tiene derecho, al menos, a conocer la información siguiente:

a. Su identidad y datos de contacto.

b. Las categorías, clases o tipos de datos objeto del tratamiento.

c. La causa válida conforme a la cual se realiza el tratamiento.

d. Las finalidades del tratamiento a que serán sometidos sus datos personales.

e. Los datos de contacto del delegado de protección de datos, en su caso.

f. El interés legítimo perseguido, así como la información indispensable para dar certeza a los titulares de que sus derechos y libertades fundamentales no se ven trastocados por este tratamiento basado en un interés legítimo. Este supuesto, únicamente en el caso de que el interés legítimo sea la causa habilitante del tratamiento.

g. Las comunicaciones, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y las finalidades que motivan la realización de las mismas.

h. El plazo de conservación de los datos. Si no es posible informar el plazo, los criterios utilizados para establecer el plazo.

i. La existencia, forma y mecanismos o procedimientos a través de los cuales podrá ejercer los derechos de acceso, rectificación, cancelación supresión o derecho al olvido, oposición, portabilidad, limitación del tratamiento y a no ser objeto de decisiones automatizadas.

j. La existencia de decisiones automatizadas con información útil para los titulares sobre la lógica aplicada, la relevancia del tratamiento y sus consecuencias, en un lenguaje claro, sencillo y de fácil comprensión. También, cuando resulte pertinente, se informará, a los titulares, sobre la elaboración de perfiles, las fuentes de datos de referencia y las consecuencias principales de ese tratamiento. Cuando se utilicen sistemas de inteligencia artificial, deberá proporcionarse información significativa sobre el papel del sistema en la toma de decisiones, el grado de automatización existente, las principales variables o criterios utilizados y las limitaciones relevantes del sistema.

k. En su caso, el origen de los datos personales cuando el responsable no los hubiere obtenido directamente del titular.

16.3. La 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.

16.4. Todo responsable contará con políticas transparentes de los tratamientos de datos personales que realice.

17. Principio de finalidad

17.1. Todo tratamiento de datos personales se limitará al cumplimiento de finalidades determinadas, explícitas y legítimas.

17.2. 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.

El tratamiento de datos para fines distintos de los que motivaron el tratamiento será factible siempre y cuando se evalúe y corrobore, previamente, que dichos fines son compatibles con los que motivaron el tratamiento inicialmente. Para evaluar la compatibilidad se deberá tener en cuenta los siguientes factores:

a. El vínculo entre la finalidad inicial y la nueva.

b. La naturaleza de los datos, particularmente si se está en presencia de datos sensibles.

c. El contexto conforme al cual se obtuvieron los datos.

d. La existencia de garantías técnicas y organizativas en beneficio de los titulares.

e. Las expectativas razonables de los titulares.

f. La existencia de medidas adecuadas de gobernanza, trazabilidad y protección de derechos, particularmente cuando se pretenda la reutilización de datos para el entrenamiento, ajuste, validación o mejora de sistemas automatizados o de inteligencia artificial.

Este supuesto no se aplicará a los tratamientos basados en el consentimiento.

17.3. 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.

17.4. En el caso del tratamiento de datos de menores, para un nuevo propósito, la protección de los derechos del niño deberá ser considerada con la misma importancia que cuando se obtuvieron los datos por primera vez.

18. Principio de finalidad

18.1. El responsable tratará únicamente los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento. La utilización de tecnologías automatizadas o sistemas de inteligencia artificial no justificará, por sí sola, la obtención masiva, indiscriminada o desproporcionada de datos personales.

19. Principio de calidad

19.1. El responsable adoptará las medidas necesarias para mantener exactos, completos, pertinentes y actualizados los datos personales en su posesión, de tal manera que no se altere su veracidad, fiabilidad y adecuación a las finalidades que motivaron su tratamiento. La calidad de los datos personales deberá evaluarse atendiendo a la naturaleza, contexto, finalidades y posibles efectos del tratamiento sobre los derechos y libertades de las personas.

En tratamientos automatizados, incluyendo los realizados mediante sistemas de inteligencia artificial, el responsable deberá adoptar medidas razonables para garantizar la calidad, pertinencia, representatividad, integridad y actualización de los datos utilizados a lo largo del ciclo de vida del sistema, incluyendo los datos de entrenamiento, validación, prueba, ajuste, entrada, supervisión y funcionamiento.

Asimismo, deberá implementar mecanismos de gobernanza y supervisión destinados a prevenir o mitigar sesgos indebidos, inferencias inexactas, discriminación arbitraria, asociaciones erróneas, degradación de la calidad de los datos o resultados manifiestamente falsos, inexactos, desproporcionados o engañosos, o derivados de datos incompletos, desactualizados, no representativos o descontextualizados.

Cuando el tratamiento implique elaboración de perfiles, sistemas predictivos o inteligencia artificial, el responsable deberá evaluar periódicamente la fiabilidad, pertinencia, exactitud, proporcionalidad y calidad de las inferencias, clasificaciones, recomendaciones, predicciones o resultados generados por el sistema, especialmente cuando puedan producir efectos jurídicos o impactos significativos sobre las personas.

19.2. 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. En tratamientos automatizados, incluyendo los realizados mediante sistemas de inteligencia artificial, el responsable deberá adoptar medidas razonables para evitar la reutilización incompatible, persistencia indebida o conservación desproporcionada de datos personales e inferencias derivadas de éstos.

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

19.4. 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.

20. Principio de responsabilidad proactiva y demostrada

20.1. El responsable implementará medidas técnicas y organizativas, proporcionales al riesgo para acreditar el cumplimiento de la normativa sobre protección de datos personales.

Para la determinación del riesgo se deberá tener en cuenta la naturaleza, ámbito, contexto y propósitos del tratamiento, así como la probabilidad, y gravedad, de que se produzcan afectaciones a los derechos y libertades fundamentales de los titulares.

Las certificaciones, las normas corporativas vinculantes, los códigos de conducta, o esquemas análogos, podrán servir para demostrar el cumplimiento, siempre que los mencionados mecanismos posean los siguientes atributos: sean reconocidos por una autoridad de protección de datos personales, ese reconocimiento se base en una supervisión independiente y acreditada y sean mecanismos transparentes y verificables públicamente.

20.2. 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.

20.3. 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.

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.

h. Mantener mecanismos razonables de gobernanza, trazabilidad, documentación, registro de decisiones relevantes, supervisión, control y gestión de riesgos, incluyendo, cuando resulte pertinente, mecanismos de supervisión humana efectiva y revisión periódica de impactos

20.4. 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.

21. Principio de seguridad

21.1. El responsable y el encargado establecerán y mantendrán, con independencia del tipo de tratamiento que efectúe, medidas de carácter administrativo, físico y técnico idóneas para garantizar un nivel de seguridad adecuado al riesgo que, en su caso, comprenda, los elementos para garantizar la confidencialidad, integridad, resiliencia y disponibilidad permanentes de los sistemas y servicios de tratamiento, la seudonimización y cifrado de datos, la posibilidad de restaurar la disponibilidad y acceso a los datos personales, de forma rápida, cuando se haya tenido un incidente físico o técnico.

21.2. Para la determinación de las medidas referidas en el numeral anterior, 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.

21.3. El responsable y el encargado llevarán 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.

El responsable y el encargado implementarán medidas destinadas a asegurar que toda persona, que actúe bajo su autoridad en el tratamiento datos, esté obligada a cumplir con las instrucciones y compromisos destinados a garantizar la seguridad, en toda la cadena de tratamiento.

En tratamientos automatizados, incluyendo los realizados mediante sistemas de inteligencia artificial, estas medidas deberán incluir, cuando resulte pertinente, controles sobre integridad de datos, control de versiones, monitorización de funcionamiento, protección frente a manipulación del sistema y mitigación de comportamientos no previstos.

22. Notificación de vulneraciones a la seguridad de los datos personales

22.1. Cuando el responsable tenga conocimiento de una vulneración de seguridad de datos personales, ocurrida en cualquier fase del tratamiento, notificará a la autoridad de protección de datos personales dicho acontecimiento, sin dilación alguna, salvo que, después de evaluarla, se determine que no genera un riesgo para los derechos y libertades de los titulares.

La notificación que el responsable lleve a cabo ante la autoridad de protección de datos personales deberá describir al menos los siguientes contenidos:

a. La naturaleza de la vulneración de la seguridad de los datos personales.

b. Las posibles consecuencias de la vulneración de la seguridad de los datos personales.

c. Las medidas adoptadas o propuestas, por el propio responsable, para remediar la citada violación.

d. Las medidas destinadas a mitigar los posibles efectos negativos, de ser el caso.

El encargado deberá notificar al responsable, sin dilación alguna, las vulneraciones de seguridad de que tenga conocimiento.

22.2. Los titulares deberán ser notificados de las vulneraciones de la seguridad de datos personales que conlleven un alto riesgo para sus derechos y libertades. El responsable deberá hacer la notificación sin dilación indebida.

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

22.4. La notificación que el responsable comunique al titular 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.

22.5. El responsable documentará toda vulneración de seguridad de los datos personales ocurrida en cualquier fase del tratamiento, identificando, de manera enunciativa mas 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.

22.6. 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 de salvaguardar los intereses, derechos y libertades de los titulares afectados.

23. Principio de confidencialidad

23.1. 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, obligación que subsistirá aun después de finalizar sus relaciones con el titular.

Lo anterior, no obsta para que las comunicaciones y transferencias de datos personales se realicen de conformidad con lo previsto en la legislación.

Capítulo III
Derechos del titular

24. Derechos

24.1. En todo momento el titular o su representante podrán solicitar al responsable, el acceso, rectificación, supresión y derecho al olvido, oposición, derecho a no ser objeto de decisiones exclusiva o esencialmente automatizadas, la portabilidad de los datos personales y la limitación del tratamiento de los datos que le conciernen.

24.2. El ejercicio de cualquiera de los derechos referidos en el numeral anterior no es requisito previo, ni impide el ejercicio de otro.

25. Derecho de acceso

25.1. 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.

26. Derecho de rectificación

26.1. 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.

27. Derecho de supresión y derecho al olvido

27.1. El titular tendrá derecho a solicitar la supresión de sus datos personales al responsable, a fin de que los mismos se supriman sin dilación alguna en los siguientes casos:

a. Los datos no resulten necesarios en atención a los propósitos para los que se obtuvieron.

b. El titular revoque su consentimiento, en el caso de que el tratamiento se haya basado en el mismo.

c. El titular se haya opuesto al tratamiento, conforme al numeral 28.1, letra a, y no prevalezcan otros motivos legítimos, o el interesado se oponga conforme a la letra b del citado numeral.

d. Los datos hayan sido tratados de forma ilícita.

En el caso de que los datos personales se hayan hecho públicos, especialmente en entornos digitales, y el responsable esté obligado a suprimir los datos en términos de alguno de los casos descritos, dicho responsable deberá informar a los otros responsables que estén tratando los datos, la solicitud de supresión de cualquier enlace a esos datos o a cualquier copia o réplica de los mismos. El ejercicio de este derecho podrá limitarse válidamente cuando el tratamiento sea indispensable para el ejercicio de la libertad de expresión e información, el cumplimiento de una obligación legal, por motivos de interés público, para fines de investigación científica, histórica o estadísticos y para la formulación, ejercicio y defensa de reclamaciones.

28. Derecho de oposición

28.1. El derecho de oposición únicamente podrá ejercerse en el caso de que tratamiento se haya producido con motivo del cumplimiento de una actuación basada en el interés público, derivado del ejercicio de funciones, atribuciones o potestades públicas, o bien, para la satisfacción de intereses legítimos.

El titular podrá ejercer su derecho de oposición:

a. Por motivos relacionados con su situación particular, incluida la elaboración de perfiles. El responsable deberá cesar el tratamiento salvo que acredite motivos legítimos imperiosos que prevalezcan respecto de los derechos y libertades fundamentales del titular, o bien, para la formulación, el ejercicio o defensa de reclamaciones.

b. 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.

28.2 Tratándose del inciso anterior, cuando el titular se oponga al tratamiento con fines de mercadotecnia directa, sus datos personales dejarán de ser tratados para dichos fines.

28.3. Cuando el tratamiento de datos personales se haya realizado con motivo de los intereses legítimos del responsable, en el contexto del desarrollo y la explotación de un sistema de inteligencia artificial, en cuyo caso el derecho de oposición será incondicional para su titular.

El responsable deberá adoptar medidas razonables de gobernanza, trazabilidad y control destinadas a facilitar el ejercicio efectivo de este derecho, teniendo en cuenta la naturaleza del tratamiento y los casos en que la supresión, desvinculación o cesación plena del

uso de los datos personales o de las inferencias derivadas de éstos no resulte técnica o materialmente viable.

29. Derecho a no ser objeto de decisiones individuales automatizadas

29.1. El titular tendrá derecho a no ser objeto de decisiones que le produzcan efectos jurídicos o le afecten de manera significativa cuando se basen exclusiva o esencialmente en tratamientos automatizados, incluyendo los realizados mediante sistemas de inteligencia artificial destinados a evaluar, clasificar, recomendar, perfilar, analizar o predecir aspectos personales del titular.

Los menores no deberán ser objeto de decisiones que produzcan efectos jurídicos o significativos, basadas únicamente en tratamiento automatizado, salvo que existan garantías reforzadas.

29.2. Lo dispuesto en el numeral 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.

29.3. No obstante, cuando sea necesario para la relación contractual o el titular hubiere manifestado su consentimiento tendrá derecho a obtener la intervención humana calificada significativa y efectiva, implicando capacidad real de comprender los fundamentos principales del sistema, evaluar críticamente sus resultados y apartarse razonadamente de ellos; recibir una explicación significativa y clara sobre la lógica aplicada, de manera que pueda conocer de los criterios principales y factores determinantes en torno a la decisión tomada; la importancia y las consecuencias principales de dicho tratamiento para su titular, así como a expresar su punto de vista e impugnar la decisión.

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

30. Derecho de oposición

30.1. 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 (formato interoperable), que le permita seguir utilizándolos y transferirlos a otro responsable, en caso de que lo requiera.

Este derecho podrá ejercerse, únicamente, en el caso de que:

a. Se esté en presencia de un tratamiento automatizado, exclusivamente.

b. El tratamiento esté basado en el consentimiento, o bien, en un contrato.

30.2. El titular podrá solicitar que sus datos personales se transfieran directamente de responsable a responsable cuando sea técnicamente posible.

30.3. El derecho a la portabilidad de los datos personales no afectará negativamente a los derechos y libertades de otros.

30.4. 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.

31. Derecho a la limitación del tratamiento de los datos personales

31.1. El titular tendrá derecho a la limitación del tratamiento de datos personales en los siguientes casos:

a. El titular ejerza su derecho de rectificación, durante el plazo que permita al responsable hacer efectivo dicho derecho.

b. El titular se oponga al tratamiento de sus datos, durante el tiempo que haga posible al responsable constatar la existencia de intereses legítimos imperiosos que prevalezcan sobre los del titular.

c. El titular solicite que los datos no sean suprimidos, ante tratamientos ilícitos con sus datos, para ejercer o defender sus derechos.

El titular lo solicite para la formulación, ejercicio o defensa de reclamaciones, en el caso de datos que hayan cumplido sus finalidades.

31.2. Los titulares serán informados del cese de la limitación del tratamiento, en todos los casos, previo al levantamiento de dicha medida.

32. Ejercicio de los derechos para la protección de los datos personales

32.1. El responsable establecerá medios y procedimientos sencillos, expeditos, accesibles y gratuitos que permitan al titular ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad.

32.2. La legislación nacional de los Estados Iberoamericanos aplicable en la materia establecerá los requerimientos, plazos, términos y condiciones en que los titulares podrán ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad, así como las causales de improcedencia al ejercicio de los mismos como podrían ser, de manera enunciativa mas no limitativa:

a. Cuando el tratamiento sea necesario para el cumplimiento de un objetivo importante de interés público.

b. Cuando el tratamiento sea necesario para el ejercicio de las funciones propias de las autoridades públicas.

c. Cuando el responsable acredite tener motivos legítimos para que el tratamiento prevalezca sobre los intereses, los derechos y las libertades del titular.

d. Cuando el tratamiento sea necesario para el cumplimiento de una disposición legal.

e. Cuando los datos personales sean necesarios para el mantenimiento o cumplimiento de una relación jurídica o contractual.

32.3. La legislación nacional de los Estados Iberoamericanos aplicable en la materia podrá reconocer que las personas físicas vinculadas a fallecidos o designados por éstos, ejerzan los derechos a que se refiere el presente estándar respecto a los datos personales de fallecidos que les conciernan.

32.4. La legislación nacional de los Estados Iberoamericanos aplicable en la materia reconocerá el derecho que tiene el titular de inconformarse o impugnar las respuestas otorgadas por el responsable ante una solicitud de ejercicio de los derechos aludidos en el presente numeral, o ante la falta de respuesta de éste ante la autoridad de control y, en su caso, ante instancias judiciales de conformidad con el derecho interno de cada Estado Iberoamericano.

32.5. La existencia de mecanismos alternativos de solución de controversias será posible, siempre que se garantice su revisión judicial, que se trata de una alternativa voluntaria, imparcial y que no excluye la vía judicial. La autoridad de protección de datos personales deberá supervisar que estas condiciones se cumplan, para reconocer la validez de las actuaciones desarrolladas a través de estos mecanismos.

Capítulo IV
Encargado

33. Alcance del encargado

33.1. 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.

34. Formalización de la prestación de servicios del encargado

34.1. La prestación de servicios entre el responsable y encargado se formalizará mediante la suscripción de un contrato o cualquier otro instrumento jurídico que consideren los Estados Iberoamericanos en la legislación nacional aplicable en la materia.

34.2. El contrato o instrumento jurídico 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.

34.3. 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.

h. Permitir al responsable y autoridad de control inspecciones y verificaciones en las instalaciones y dependencias del encargado.

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.

k. Cuando el servicio implique sistemas automatizados, inteligencia artificial u otras tecnologías emergentes, proporcionar al responsable información suficiente sobre el funcionamiento general del sistema, sus limitaciones relevantes, medidas de seguridad, trazabilidad, calidad de datos, supervisión y gestión de riesgos, en la medida necesaria para que el responsable pueda cumplir sus obligaciones.

34.4. 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, conforme a la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.

35. Subcontratación de servicios

35.1. El encargado podrá, a su vez, subcontratar servicios que impliquen el tratamiento de datos personales, siempre y cuando exista una autorización previa por escrito, específica o general del responsable, o bien, se estipule expresamente en el contrato o instrumento jurídico suscrito entre este último y el encargado.

35.2. El subcontratado asumirá el carácter de encargado en los términos que estipulen la legislación nacional del Estado Iberoamericano aplicable en la materia.

35.3. El encargado formalizará la prestación de servicios del subcontratado a través de un contrato o cualquier otro instrumento jurídico que determine la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.

35.4. Cuando el subcontratado incumpla sus obligaciones y responsabilidades respecto al tratamiento de datos personales que lleve a cabo conforme a lo instruido por el encargado, asumirá la calidad de responsable conforme a la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.

Capítulo V
Transferencias internacionales de datos personales

36. Reglas generales para las transferencias internacionales de datos personales

Las únicas transferencias internacionales de datos personales, que se recomiendan como válidas, serán las que responsables y encargados realicen conforme a las reglas de este apartado.

El responsable y encargado podrán realizar transferencias internacionales de datos personales en cualquiera de los siguientes supuestos:

a. Un país tercero, parte de su territorio, sector, actividad, o bien, una organización internacional, haya sido reconocido con un nivel adecuado de protección de datos personales, por parte del país desde el que se exportarán los datos.

Para llevar a cabo el reconocimiento de nivel adecuado, las autoridades de protección de datos personales deberán evaluar, al menos, los siguientes aspectos:

1) El Estado de Derecho, concretamente, el respeto por los derechos fundamentales y las libertades individuales, la legislación relevante en materia de protección de datos personales, tanto general como sectorial, la legislación sobre seguridad nacional, seguridad pública, del ámbito penal, así como la relativa al acceso, por parte de las autoridades del Estado, a los datos personales, con el propósito de corroborar el nivel de equivalencia, entre ambos países en los temas descritos.

2) La existencia y funcionamiento efectivo de una o más autoridades de protección de datos personales, para lo cual se deberá verificar que esa autoridad o autoridades responden al diseño y características previstas en el numeral 42 de los Estándares.

3) La existencia de derechos individuales que puedan ser efectivamente ejercidos por sus titulares ante las autoridades de protección de datos y los tribunales competentes.

4) Los compromisos internacionales de los que sea parte el país tercero o la organización internacional, para comprobar los alcances de sus compromisos, al respecto, en materia de datos personales.

Concluida la evaluación, se podrá adoptar una decisión sobre la posibilidad de reconocer, o no, a un país tercero u organización internacional, con nivel adecuado de protección. En el propio documento donde se adopte la decisión favorable al reconocimiento, se deberá establecer el mecanismo de revisión periódica, de permanencia de las condiciones al paso del tiempo. La revisión deberá llevarse a cabo, al menos, cada 5 años.

b. En el caso de que el país tercero u organización internacional al que se desea hacer una transferencia internacional de datos personales no cuente con el reconocimiento de nivel adecuado por parte del país desde el que se exportarán los datos, el responsable o el encargado, podrán ofrecer las garantías adecuadas a través de los siguientes instrumentos:

1) Cláusulas tipo de protección de datos personales adoptadas por la autoridad de protección de datos personales para que responsables y encargados se puedan adherir, y mediante esa adhesión garantizar el cumplimiento de la legislación de protección de datos del país desde el que se exportan los datos.

2) Códigos de conducta vinculantes y exigibles, representativos de una asociación o entidad sectorial, sujetos a mecanismos de supervisión independientes y efectivos, que aseguren que se respetará la legislación de protección de datos del país desde el que se exportan los datos, y que deben ser evaluados y aprobados por la autoridad de protección de datos personales del citado país.

3) Normas corporativas vinculantes, que aseguren y demuestren que se respetará la legislación de protección de datos del país desde el que se exportan los datos, revisadas y aprobadas por la autoridad de protección de datos personales de dicho país.

4) Certificaciones que aseguren y demuestren que se respetará la legislación de protección de datos del país desde el que se exportan los datos, revisadas y aprobadas por la autoridad de protección de datos personales del mencionado país.

5) Instrumentos jurídicamente vinculantes y exigibles entre instituciones y entidades públicas del Estado.

6) Cláusulas contractuales entre un responsable o un encargado, en el país desde el que se exportan los datos, con un destinatario en un país tercero u organización internacional. Estas cláusulas requieren ser autorizadas, por la autoridad de protección de datos personales, para su validez.

c. Ante la ausencia de una decisión de adecuación o de garantías adecuadas, las transferencias internacionales de datos se podrán llevar a cabo en los siguientes casos de excepción:

1) El titular haya otorgado expresamente su consentimiento para la transferencia una vez informado de los posibles riesgos de la misma.

2) Resulte indispensable para la celebración o ejecución de un contrato, o de medidas precontractuales, que guarden relación con el titular.

3) Por razones de interés público.

4) Para la formulación, ejercicio y defensa de reclamaciones.

5) Para la protección de intereses vitales del titular, o de un tercero, cuando el titular esté imposibilitado para otorgar su consentimiento.

6) Se realice desde un registro público, cuyo objeto sea facilitar información y estar abierto a la consulta del público, en general, o de cualquier persona que acredite un interés legítimo, únicamente en la medida que se cumpla con los requisitos, de la normativa aplicable, para la consulta.

Los supuestos descritos en los numerales 1) y 2), no serán aplicables a actividades llevadas a cabo por autoridades e instituciones públicas del Estado, en ejercicio de atribuciones, facultades o poderes públicos.

d. En el caso de que una transferencia internacional de datos personales no se pueda llevar a cabo a través de alguno de los mecanismos descritos en las literales a, b y c, se podrá realizar de manera excepcional siempre que se den todas las siguientes condiciones:

1) No sea repetitiva.

2) Impacte un número limitado de titulares.

3) Sea necesaria para intereses legítimos imperiosos del responsable, que prevalecen frente a los derechos y libertades de los titulares. Estos intereses legítimos deberán ser informados al titular.

4) El responsable haya ofrecido garantías apropiadas, acorde a la situación.

5) Se informe a la autoridad de protección de datos personales.

La excepción d) no será aplicable a actividades llevadas a cabo por autoridades e instituciones públicas del Estado, en ejercicio de atribuciones, facultades o poderes públicos.

Capítulo VI
Medidas proactivas en el tratamiento de datos personales

37. Reconocimiento de medidas proactivas

37.1. La legislación nacional de los Estados Iberoamericanos aplicable en la materia podrá reconocer y establecer medidas que promuevan el mejor cumplimiento de su legislación y coadyuven a fortalecer y elevar los controles de protección de datos personales implementados por el responsable, entre las cuales podrán encontrase las que a continuación se indican en el presente Capítulo.

38. Privacidad por diseño y privacidad por defecto

38.1. 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 del Estado Iberoamericano que le resulte aplicable. En tratamientos automatizados, incluyendo los realizados mediante sistemas de inteligencia artificial, las medidas deberán contemplar mecanismos razonables de supervisión, trazabilidad, documentación, gestión de riesgos y control del funcionamiento del sistema, atendiendo a la naturaleza, contexto y posibles efectos del tratamiento.

38.2. 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 del Estado Iberoamericano 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.

39. Oficial o delegado de protección de datos personales

39.1. El responsable y el encargado designarán un oficial o delegado de protección de datos personales para lo cual tendrán en consideración su formación y experiencia profesionales, sus conocimientos especializados, y debidamente acreditados, en el ámbito de la protección de los datos personales, así como a su capacidad para desempeñar las funciones descritas en el numeral 39.4.

La designación, de un oficial o delegado de protección de datos personales, será obligatoria en los siguientes casos:

a. Sea una autoridad pública. Para efectos de esta referencia, una autoridad pública no solamente es aquella que forma parte del Estado en estricto sentido, sino también aquellos particulares que desarrollan actividades propias del Estado a través de concesiones, permisos o autorizaciones, entre otros.

b. Lleve a cabo tratamientos de datos personales que tengan por objeto una observación habitual y sistemática de la conducta del titular.

c. Realice tratamientos de datos personales donde sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares considerando, entre otros factores y de manera enunciativa mas no limitativa, las categorías de datos personales tratados, en especial cuando se trate de datos sensibles; las transferencias que se efectúen; el número de titulares; el alcance del tratamiento; las tecnologías de información utilizadas o las finalidades de éstos.

39.2. El responsable que no se encuentre en alguna de las causales previstas en el numeral anterior podrá designar a un oficial de protección de datos personales si así lo estima conveniente.

39.3. El responsable estará obligado a respaldar al oficial de protección de datos personales en el desempeño de sus funciones, facilitándole los recursos necesarios para su desempeño y para el mantenimiento de sus conocimientos especializados y la actualización de éstos.

39.4. El oficial de protección de datos personales tendrá, al menos, las siguientes funciones:

a. Asesorar al responsable, o al encargado, respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales.

b. Coordinar al interior de la organización del responsable, o del encargado, las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento en materia de datos personales.

c. Supervisar al interior de la organización del responsable, o del encargado, el cumplimiento en materia de datos personales.

d. Cooperar con la autoridad de protección de datos personales y ser su punto de contacto.

39.5. El responsable y el encargado garantizarán que el oficial o delegado no reciba instrucciones en torno al desempeño de sus funciones, asegurándose que no llegue a ubicarse en situaciones de conflicto de interés derivado de otras actividades, dentro de la organización, en su caso. El oficial o delegado rendirá cuentas a la alta dirección o a la máxima autoridad del responsable o del encargado.

40. Mecanismos de autorregulación

40.1. El responsable podrá adherirse, de manera voluntaria, a esquemas de autorregulación vinculante, que tengan por objeto, entre otros, contribuir a la correcta aplicación de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia y establecer procedimientos de resolución de conflictos entre el responsable y titular sin perjuicio de otros mecanismos que establezca la legislación nacional de la materia aplicable, teniendo en cuenta las características específicas de los tratamientos de datos personales realizados, así como el efectivo ejercicio y respeto de los derechos del titular.

40.2. Para los efectos del numeral anterior se podrán desarrollar, entre otros, códigos deontológicos y sistemas de certificación y sus respectivos sellos de confianza que coadyuven a contribuir a los objetivos señalados en el presente numeral.

40.3. La legislación nacional de los Estados Iberoamericanos aplicable en la materia establecerá las reglas que correspondan para la validación, confirmación o reconocimiento de los mecanismos de autorregulación aludidos.

41. Evaluación de impacto a la protección de datos personales

41.1. Cuando el responsable pretenda llevar a cabo un tipo de tratamiento de datos personales, especialmente a través de tecnologías emergentes o disruptivas, incluyen-

do sistemas de inteligencia artificial, tecnologías biométricas, neurotecnologías, sistemas predictivos y otras tecnologías capaces de producir tratamientos intensivos, inferenciales o altamente automatizados de datos personales, que, por su naturaleza, alcance, contexto o finalidades, sea probable que conlleve un alto riesgo para los derechos y libertades de los titulares, realizará, de manera previa al tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de los datos personales.

La evaluación deberá incluir, al menos, lo siguiente:

a. Una descripción sistemática de las operaciones de tratamiento, que se tiene previsto realizar, sus finalidades y, en su caso, los intereses legítimos perseguidos por el responsable.

b. La valoración sobre la necesidad y proporcionalidad de las operaciones de tratamiento a realizar, en función de las finalidades.

c. La evaluación de riesgos para los derechos y libertades de los titulares.

d. Las medidas contempladas frente a los riesgos. Aquí se deberán indicar todas aquellas garantías y mecanismos destinados a asegurar y demostrar la protección de los datos personales y el cumplimiento de la normativa aplicable en la materia.

e. La descripción de las medidas de gobernanza algorítmica, las medidas previstas para la supervisión, trazabilidad, control y mitigación de riesgos asociados a sistemas automatizados o de inteligencia artificial.

En los casos que lo amerite, el responsable solicitará la opinión de los titulares, respecto del tratamiento a realizar, sin perjuicio del interés público, comercial o de seguridad, que en su caso pudieran implicar.

41.2 La evaluación de impacto a la protección de los datos se sugiere sea presentada, especialmente, en estos casos:

a. Tratamientos automatizados o basados en sistemas de inteligencia artificial, incluida la elaboración de perfiles, que generen recomendaciones o decisiones exclusiva o esencialmente automatizadas, que puedan producir efectos jurídicos, afectaciones significativas similares o influir de manera relevante en el comportamiento, decisiones, acceso a derechos, oportunidades, servicios esenciales o condiciones de vida de las personas físicas.

b. Tratamiento a gran escala de datos sensibles o de categorías especiales de datos.

c. Los tratamientos de alto riesgo descritos en estos Estándares.

d. Los tratamientos que impliquen la observación sistemática, a gran escala, en zonas de acceso público.

e. Las transferencias internacionales de datos personales a países no reconocidos con nivel adecuado siempre que no sea posible ofrecer alguna de las garantías adecua-

das reconocidas en el numeral 36.1, inciso b), o bien, no se acredite la existencia de alguna de las excepciones del numeral 36.1, inciso c).

En los casos en los que el resultado de la evaluación de impacto refleje que el tratamiento puede implicar un alto riesgo, de no implementarse las medidas de mitigación idóneas, el responsable estará obligado a consultar a la autoridad de protección de datos personales, previo a iniciar el tratamiento.

El objetivo de esta consulta es que la autoridad de protección de datos personales asesore al responsable. Para este propósito, el responsable deberá compartir con la citada autoridad la evaluación de impacto a la protección de datos realizada, así como toda aquella información que resulte necesaria.

Capítulo VII
Autoridades de protección de datos personales

42. Autoridades de protección de datos personales

42.1. La legislación de protección de datos personales deberá contemplar la existencia de una o más autoridades de protección de datos personales, con la finalidad de supervisar y asegurar el cumplimiento de la normativa, así como garantizar el respeto de los derechos y libertades de las personas.

42.2. Las autoridades de protección de datos personales deberán estar dotadas de plena autonomía desde la legislación y normativa que las regule. La plena autonomía deberá garantizar, mínimamente, cumplir con su objetivo y ejercer sus facultades, atribuciones, potestades y poderes de forma imparcial e independiente, ajenas a toda influencia externa, ya sea directa o indirecta, y sin requerir ni admitir orden ni instrucción alguna.

Aunque el máximo grado de autonomía que reconozca el orden jurídico de cada Estado Iberoamericano podría resultar el esquema más efectivo para el diseño de autoridades, en los casos que no resulte factible, se les podrá dotar de una autonomía funcionalmente eficaz que les garantice cumplir con su objetivo y ejercer cabalmente sus funciones.

42.3. Las autoridades podrán tener una integración unipersonal o colegiada al frente de su órgano máximo de dirección.

El miembro o los miembros de los órganos de dirección de las autoridades deberán contar con la experiencia y conocimientos especializados en derecho y protección de datos personales, especialmente en supervisión regulatoria y cooperación internacional.

El procedimiento de selección deberá ser transparente y asegurar su imparcialidad y credibilidad, así como la certeza de que se trata de un proceso de selección de perfil técnico, basado en méritos, esencialmente.

La o las personas designadas únicamente podrán ser destituidos por causas graves establecidas en la legislación nacional, conforme a las reglas del debido proceso, o bien, si deja de cumplir las condiciones exigidas para el desempeño de sus funciones.

El miembro o los miembros de los órganos de dirección de la autoridad deberá abstenerse de toda acción incompatible con sus responsabilidades durante la vigencia de su mandato.

42.4. Además de las funciones que se han señalado a lo largo de los Estándares, las autoridades de protección de datos personales deberán contar con facultades, atribuciones, potestades y poderes idóneos para alcanzar sus objetivos.

El diseño de las autoridades de protección de datos deberá reflejar, en la legislación, los contenidos que le posibiliten mínimamente para:

a. Investigar, supervisar o fiscalizar el cumplimiento de la normativa.

b. Ordenar medidas cautelares provisionales, proporcionales y revisables, como instrumento preventivo y urgente.

c. Dictar resoluciones.

d. Sancionar la comisión de infracciones.

e. Hacer efectivos los derechos de los titulares.

f. Emitir normativa.

g. Interpretar la regulación.

h. Diseñar e implementar políticas públicas.

i. Diseñar e implementar programas de construcción de capacidades.

j. Construir y fomentar una cultura de la protección de datos.

k. Crear y promover el conocimiento.

l. Cooperar internacionalmente con otras autoridades.

En el ejercicio de sus funciones las autoridades de protección de datos deberán instrumentar políticas destinadas a brindar a atención adecuada, para la tutela de los grupos con vulnerabilidad, de acuerdo con sus necesidades, que les permita el ejercicio efectivo de sus derechos.

42.5. Las resoluciones y actuaciones de la autoridad de protección de datos, en ejercicio de sus funciones, facultades, atribuciones, potestades y poderes, exclusivamente, estarán sujetas a la revisión judicial, por lo que la legislación nacional deberá adoptar las previsiones conducentes para garantizarlo.

42.6. Las autoridades de protección de datos personales deberán contar con los recursos humanos y materiales necesarios para el cumplimiento de sus funciones.

Cada Estado Iberoamericano deberá garantizar que los controles financieros a los que esté sujeta la autoridad de protección de datos personales no menoscaben su plena autonomía e independencia, por lo que contará con un presupuesto público independientemente de la existencia de otras fuentes de financiamiento que pudiera tener.

También, se deberá garantizar que cada autoridad elija y disponga libremente de su personal, y que ese personal dependa exclusivamente del órgano de dirección de la autoridad de protección de datos personales.

Capítulo VIII
Reclamaciones y sanciones

43. Régimen de reclamaciones y de imposición de sanciones

43.1. Todo titular tendrá derecho a presentar su reclamación ante la autoridad de protección de datos personales, así como recurrir a la tutela judicial para hacer efectivos sus derechos conforme a la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.

43.2. La legislación nacional de los Estados Iberoamericanos aplicable en la materia establecerá un régimen que permita al titular presentar una reclamación ante la autoridad de protección de datos personales cuando considere que el tratamiento de sus datos personales infringe la normativa nacional en la materia, así como a solicitar la tutela judicial.

43.3. La legislación nacional de los Estados Iberoamericanos aplicable en la materia establecerá un régimen que permita la adopción de medidas correctivas y sancionar las conductas que contravengan lo dispuesto en las legislaciones nacionales correspondientes, indicando, al menos, el límite máximo y los criterios objetivos para fijar las correspondientes sanciones a partir de la naturaleza, gravedad, duración de la infracción y sus consecuencias, así como las medidas implementadas por el responsable para garantizar el cumplimiento de sus obligaciones en la materia.

Capítulo IX
Derecho de indemnización

44. Régimen de reclamaciones y de imposición de sanciones

44.1. La legislación nacional de los Estados Iberoamericanos aplicable en la materia reconocerá el derecho que tiene el titular a ser indemnizado cuando hubiere sufrido daños y perjuicios, como consecuencia de una violación de su derecho a la protección de datos personales.

44.2. El derecho interno de los Estados Iberoamericanos señalará la autoridad competente para conocer de este tipo de acciones interpuestas por el titular afectado, así como los plazos, requerimientos y términos a través de los cuales será indemnizado éste en caso de resultar procedente.

Capítulo X

45. Establecimiento de mecanismos de cooperación internacional

45.1. Los Estados Iberoamericanos podrán adoptar mecanismos de cooperación internacional que faciliten la aplicación de las legislaciones nacionales aplicables en la materia, los cuales podrán comprender, de manera enunciativa mas no limitativa:

a. El establecimiento de mecanismos que permitan reforzar la asistencia y cooperación internacional en la aplicación de las respectivas legislaciones nacionales en la materia.

b. La asistencia entre las autoridades de control a través de la notificación y remisión de reclamaciones, la asistencia en investigaciones y el intercambio de información.

c. La adopción de mecanismos orientados al conocimiento e intercambio de mejores prácticas y experiencias en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países.

45.2. También, como parte de las acciones en materia de cooperación internacional, se podrán establecer vínculos con redes, foros, mecanismos, espacios de cooperación, entre otros, que permitan compartir experiencias regulatorias y casos significativos, facilitar asistencia mutua, construir posiciones comunes sobre fenómenos disruptivos y temas emergentes, impulsar la interoperabilidad normativa, diseñar estrategias de mitigación comunes contra la fragmentación normativa, impulsar protocolos que faciliten la simplificación administrativa, todo en el ámbito de la protección de datos.

Disposiciones transitorias

Única. Para la efectiva implementación de legislación, reglamentos y normativa, en general de datos personales, incluidas las modificaciones o reformas, resulta determinante proveer a responsables y encargados de las condiciones necesarias para que cumplan y que ese cumplimiento sea sostenible en el tiempo.

Una de esas condiciones se presenta en la temporalidad de la regulación, concretamente en el establecimiento de plazos razonables entre la publicación de la normativa y su entrada en vigor, teniendo en consideración la serie de implicaciones materiales, financieras, humanas y regulatorias, en general, que esta normativa suele conllevar.

RED
IBEROAMERICANA DE
PROTECCION
DE DATOS