ESTÁNDARES DE PROTECCIÓN

DE DATOS PERSONALES

inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

RED IBEROAMERICANA DE PROTECCION DE DATOS

ESTÁNDARES DE PROTECCIÓN DE DATOS PERSONALES PARA LOS ESTADOS IBEROAMERICANOS

En el marco del XV Encuentro Iberoamericano de Protección de Datos, la Red Iberoamericana de Protección de Datos (RIPD o Red) ha aprobado y presentado 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 ahora aprobado trata 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 han tomado 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.

El recorrido que se ha seguido para su elaboración, comprende las siguientes etapas:

- Junio, 2016: en el XIV Encuentro Iberoamericano de Protección de Datos, celebrado el 8 de junio de 2016 en Santa Marta, Colombia, se acordó la elaboración de los Estándares Iberoamericanos a cargo del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), en ese entonces en su calidad de presidente de la Red.

- Noviembre, 2016: en el Seminario de la RIPD en el Centro de la Cooperación Española en Montevideo, celebrado los días 8 y 9 de noviembre en Montevideo, Uruguay, el INAI presentó a los miembros presentes de la Red el anteproyecto de Estándares Iberoamericanos. En dicho seminario, se acordó que durante todo el mes de diciembre de 2016 al anteproyecto de Estándares Iberoamericanos estaría abierto para comentarios y observaciones de los miembros de la Red.

- Mayo, 2017: en el Taller de la RIPD en el Centro de la Cooperación Española en Cartagena de Indias se estudió y debatió, desde el punto de vista técnico, la versión de los Estándares Iberoamericanos que había resultado de todas las aportaciones recibidas durante el mes de diciembre de 2016. En dicho taller participaron las Autoridades miembros de la RIPD, una representación del Supervisor Europeo de Protección de Datos y de la Organización de Estados Americanos, así como, mediante videoconferencia, de la Unidad de Flujos Internacionales de la Comisión Europea.

- Junio, 2017: en el XV Encuentro Iberoamericano de Protección de Datos, celebrado del 20 al 22 de junio de 2017 en Santiago de Chile, se aprobó por unanimidad en la sesión cerrada del Encuentro la versión que resultó de los trabajos realizados durante el taller de Cartagena de Indias, siendo proclamados formalmente en la Sesión Abierta.

Con la aprobación de estos Estándares, la RIPD dispone de una herramienta esencial con la que puede 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.

Por otro lado, y no menos importante, los Estándares Iberoamericanos permitirán reforzar la posición de la Red en el ámbito internacional. Para ello, se van a poner en marcha iniciativas en los diversos foros internacionales (Comisión Europea, Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, Organización Estados Americanos, etc.), tratando de buscar la mayor difusión posible de los mismos.

En definitiva, el trabajo desplegado por las entidades que integran la RIPD, que ha llevado finalmente a la aprobación de los citados Estándares, constituye una experiencia concreta de cooperación que, a nuestro juicio, puede ser de gran utilidad para otras organizaciones, por lo que quedan a entera disposición de todas las entidades y profesionales que puedan beneficiarse de ellos, en aras de garantizar de la forma más eficaz el posible ejercicio y tutela del derecho a la protección de datos tanto en la región iberoamericana como en un contexto internacional.

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. Lo anterior, no impide que el derecho a la protección de datos personales resulte aplicable a las personas jurídicas en cumplimiento a lo establecido en el derecho interno de los Estados Iberoamericanos;

(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 presentes Estándares;

(8) Teniendo en cuenta que la Unión Europea ha adoptado 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 en la Unión Europea y con el fin de generar confianza en la sociedad en general 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;

(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;

(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) Admitiendo que actualmente las bases jurídicas que legitiman a todo organismo de carácter público o privado a tratar datos personales en su posesión son el consentimiento del titular; el cumplimiento de una disposición legal; el cumplimiento de una orden judicial, resolución o mandato fundado y motivado de autoridad pública competente; el ejercicio de facultades propias de las autoridades públicas; el reconocimiento o defensa de los derechos del titular ante una autoridad pública competente; la ejecución de un contrato o precontrato en el que el titular sea parte; el cumplimiento de una obligación legal aplicable al responsable; la protección de intereses vitales del titular o de otra persona física; el interés legítimo del organismo público o privado, o por razones de interés público;

(18) Enfatizando la necesidad 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;

(19) 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;

(20) 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;

(21) 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;

(22) 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;

(23) 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;

(24) 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;

(25) 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;

(26) Destacando la importancia de establecer una base mínima para la cooperación internacional entre las autoridades de control latinoamericanas y entre éstas y las de terceros 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, al tenor de lo siguiente:

Capítulo I

Disposiciones generales

1. Objeto

1.1 Los presentes Estándares tienen por objeto:

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

b. Elevar el nivel de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales, así como entre los Estados Iberoamericanos, el cual responda a las necesidades y exigencias internacionales que demanda el derecho a la protección de datos personales en una sociedad en la cual las tecnologías de la información y del conocimiento cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana.

c. 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.

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

2. Definiciones

2.1. Para los efectos de los presentes Estándares se entenderá por:

a. Anonimización: la aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o reidentificación de una persona física sin esfuerzos desproporcionados.

b. 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.

c. 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.

d. Datos personales sensibles: 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 racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física.

e. 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.

f. 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.

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

h. **Titular:** persona física a quien le conciernen los datos personales.

i. **Tratamiento:** cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre datos personales, relacionadas, de manera enunciativa más 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.

3. Ámbito de aplicación subjetivo

3.1. Los presentes Estándares serán aplicables a las personas físicas 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 serán aplicables 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. Por regla general, los presentes Estándares serán aplicables a los datos personales de personas físicas, lo cual no impide que los Estados Iberoamericanos en su legislación nacional dispongan que la información de las personas jurídicas sea salvaguardada acorde con el derecho a la protección de datos personales, en cumplimiento a lo establecido en su derecho interno.

4.3. Los Estándares no resultarán aplicables en 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, 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. La información anónima, es decir, aquélla que no guarda relación con una persona física identificada o identificable, así como los datos personales sometidos a un proceso de anonimización de tal forma que el titular no pueda ser identificado o reidentificado.

4.4. La legislación nacional de los Estados Iberoamericanos aplicable en la materia podrá establecer categorías de datos personales a las cuales no les resulte aplicable el régimen de protección previsto en los presentes Estándares, en cumplimiento de su derecho interno.

5. Ámbito de aplicación territorial

5.1. Los Estándares serán 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 para salvaguardar la seguridad nacional, la seguridad pública, la protección de la salud pública, la protección de los derechos y las libertades de terceros, así como por cuestiones de interés público.

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

6.3. Cualquier ley que tenga como propósito limitar el derecho a la protección de datos personales contendrá, 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 serán las 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 exentar, en su derecho interno, el cumplimiento de los principios y derechos previstos en los presentes Estándares, exclusivamente en la medida en que resulte necesario conciliar el derecho a la protección de datos personales con otros derechos y libertades fundamentales.

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

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 y protección integral.

8.2. Los Estados Iberoamericanos promoverán 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.

9. Tratamiento de datos personales de carácter sensible

9.1. Por regla general, el responsable no podrá tratar datos personales sensibles, salvo que se presente cualquiera de los siguientes supuestos:

a. Los mismos sean estrictamente necesarios para el ejercicio y cumplimiento de las atribuciones y obligaciones expresamente previstas en las normas que regulan su actuación.

b. Se dé cumplimiento a un mandato legal.

c. Se cuente con el consentimiento expreso y por escrito del titular.

d. Sean necesarios por razones de seguridad nacional, seguridad pública, orden público, salud pública o salvaguarda de derechos y libertades de terceros.

9.2. 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

10. Principios aplicables al tratamiento de datos personales

10.1. En el tratamiento de datos personales, el responsable observará los principios de legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad.

11. Principio de legitimación

11.1. Por regla general, el responsable solo podrá tratar datos personales cuando se presente alguno de los siguientes supuestos:

a. El titular otorgue su consentimiento para una o varias finalidades específicas.

b. El tratamiento sea necesario para el cumplimiento de una orden judicial, resolución o mandato fundado y motivado de autoridad pública competente.

c. El tratamiento sea necesario para el ejercicio de facultades propias de las autoridades públicas o se realice en virtud de una habilitación legal.

d. El tratamiento sea necesario para el reconocimiento o defensa de los derechos del titular ante una autoridad pública.

e. El tratamiento sea necesario para la ejecución de un contrato o precontrato en el que el titular sea parte.

f. El tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al responsable.

g. El tratamiento sea necesario para proteger intereses vitales del titular o de otra persona física.

h. El tratamiento sea necesario por razones de interés público establecidas o previstas en ley.

i. El tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del titular que requiera la protección de datos personales, en particular cuando el titular sea niño, niña o adolescente. Lo anterior, no resultará aplicable a los tratamientos de datos personales realizados por las autoridades públicas en el ejercicio de sus funciones.

11.2. Tratándose de este último inciso, se entenderá amparado por el interés legítimo el tratamiento de datos personales de contacto que sea imprescindible para la localización de personas físicas que prestan sus servicios al responsable, con la finalidad de mantener cualquier tipo de relación con ésta.

12. Condiciones para el consentimiento

12.1. 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.

12.2. 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.

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

13.1. 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.

13.2. 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. Principio de licitud

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

14.2. El tratamiento de datos personales que realicen las autoridades públicas se sujetará a las facultades o atribuciones que el derecho interno del Estado Iberoamericano de que se trate les confiera expresamente, además de lo previsto en el numeral anterior de los presentes Estándares.

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 responsable proporcionará al titular, al menos, la información siguiente:

a. Su identidad y datos de contacto.

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

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

d. La existencia, forma y mecanismos o procedimientos a través de los cuales podrá ejercer los derechos de acceso, rectificación, cancelación, oposición y portabilidad.

e. 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.

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.

18. Principio de proporcionalidad

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.

19. Principio de calidad

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

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.

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

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

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.

20.4. El responsable revisará y evaluará permanentemente los mecanismos que para tal afecto 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 establecerá y mantendrá, con independencia del tipo de tratamiento que efectúe, medidas de carácter administrativo, físico y técnico suficientes para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

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

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, entendida como cualquier daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los datos personales aun cuando ocurra de manera accidental, notificará a la autoridad de control y a los titulares afectados dicho acontecimiento, sin dilación alguna.

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

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

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

a. La naturaleza del incidente.

b. Los datos personales comprometidos.

c. Las acciones correctivas realizadas de forma inmediata.

d. Las recomendaciones al titular sobre las medidas que éste pueda adoptar para proteger sus intereses.

e. Los medios disponibles al titular para obtener mayor información al respecto.

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

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 del 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.

Capítulo III

Derechos del titular

24. Derechos ARCO

24.1. En todo momento el titular o su representante podrán solicitar al responsable, el acceso, rectificación, cancelación, oposición y portabilidad de los datos personales 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 cancelación

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

28. Derecho de oposición

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

a. Tenga una razón legítima derivada de su situación particular.

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.

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 que se basen únicamente en tratamientos automatizados destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

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; recibir una explicación sobre la decisión tomada; 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 racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, así como datos genéticos o datos biométricos.

30. Derecho a la portabilidad de los datos personales

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, que le permita seguir utilizándolos y transferirlos a otro responsable, en caso de que lo requiera.

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

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

32. Ejercicio de los derechos ARCO y de portabilidad

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 más 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.

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 o autoridad de control inspecciones y verificaciones en sitio.

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

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

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 de datos personales

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

a. El país, parte de su territorio, sector, actividad u organización internacional destinatario de los datos personales hubiere sido reconocido con un nivel adecuado de protección de datos personales por parte del país transferente, conforme a la legislación nacional de éste que resulte aplicable en la materia, o bien, el país destinatario o varios sectores del mismo acrediten condiciones mínimas y suficientes para garantizar un nivel de protección de datos personales adecuado.

b. El exportador ofrezca garantías suficientes del tratamiento de los datos personales en el país destinatario, y éste, a su vez, acredite el cumplimiento de las condiciones mínimas y suficientes establecidas en la legislación nacional de cada Estado Iberoamericano aplicable en la materia.

c. El exportador y destinatario suscriban cláusulas contractuales o cualquier otro instrumento jurídico que ofrezca garantías suficientes y que permita demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes y los derechos de los titulares. La autoridad de control podrá validar cláusulas contractuales o instrumentos jurídicos según se determine en la legislación nacional de los Estados Iberoamericanos aplicable en la materia.

d. El exportador y destinatario adopten un esquema de autorregulación vinculante o un mecanismo de certificación aprobado, siempre y cuando éste sea acorde con las disposiciones previstas en la legislación nacional del Estado Iberoamericano aplicable en la materia, que está obligado a observar el exportador.

e. La autoridad de control del Estado Iberoamericano del país del exportador autorice la transferencia, en términos de la legislación nacional que resulte aplicable en la materia.

36.2. La legislación nacional de los Estados Iberoamericanos aplicable en la materia podrá establecer expresamente límites a las transferencias internacionales de categorías de datos personales por razones de seguridad nacional, seguridad pública, protección de la salud pública, protección de los derechos y libertades de terceros, así como por cuestiones de interés público.

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.

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 de protección de datos personales

39.1. El responsable designará a un oficial de protección de datos personales o figura equivalente en los casos que establezca la legislación nacional de los Estados Iberoamericanos aplicable en la materia y cuando:

a. Sea una autoridad pública.

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 más 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 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, las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.

c. Supervisar al interior de la organización del responsable el cumplimiento de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.

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

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

Capítulo VII

Autoridades de control

42. Naturaleza de las autoridades de control y supervisión

42.1. En cada Estado Iberoamericano deberá existir una o más autoridades de control en materia de protección de datos personales con plena autonomía, de conformidad con su legislación nacional aplicable en la materia.

42.2 Las autoridades de control podrán ser órganos unipersonales o pluripersonales; actuarán con carácter imparcial e independiente en sus potestades, así como serán ajenas a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán orden ni instrucción alguna.

42.3. El miembro o los miembros de los órganos de dirección de las autoridades de control deberán contar con la experiencia y aptitudes, en particular respecto al ámbito de protección de datos personales, necesarios para el cumplimiento de sus funciones y el ejercicio de sus potestades. Se nombrarán mediante un procedimiento transparente en virtud de la legislación nacional aplicable y únicamente podrán ser removidos por causales graves establecidas en el derecho interno de cada Estado Iberoamericano, conforme a las reglas del debido proceso.

42.4. La legislación nacional de los Estados Iberoamericanos que resulte aplicable en la materia deberá otorgar a las autoridades de control suficientes poderes de investigación, supervisión, resolución, promoción, sanción y otros que resulten necesarios para garantizar el efectivo cumplimiento de ésta, así como el ejercicio y respeto efectivo del derecho a la protección de datos personales.

42.5. Las decisiones de las autoridades de control únicamente estarán sujetas al control jurisdiccional, conforme a los mecanismos establecidos en la legislación nacional de los Estados Iberoamericanos que resulte aplicable en la materia y su derecho interno.

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

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 control, 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 control 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. Reparación del daño

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

Cooperación internacional

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 más 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.