Quinto Suplemento del Registro Oficial No.459 , 26 de Mayo 2021

Normativa: Vigente

Última Reforma: Quinto Suplemento del Registro Oficial 459, 26-V-2021

LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES

(Ley s/n)

EL PLENO

CONSIDERANDO

Que, el artículo 1 de la Constitución de la República dispone que el *"Estado ecuatoriano es un Estado constitucional de derechos y justicia, social, democrático (...)";*

Que, el artículo 3 en sus numerales 1, 5 y 8 de la Carta Magna determinan que son deberes primordiales del Estado *"1. Garantizar sin discriminación alguna el efectivo goce de los derechos establecidos en la Constitución y en los instrumentos internacionales, en particular la educación, la salud, la alimentación, la seguridad social y el agua para sus habitantes. 5. Planificar el desarrollo nacional, erradicar la pobreza, promover el desarrollo sustentable y la redistribución equitativa de los recursos y la riqueza, para acceder al buen vivir. 8. Garantizar a sus habitantes el derecho a una cultura de paz, a la seguridad integral y a vivir en una sociedad democrática y libre de corrupción.";*

Que, el numeral 1 del artículo 11 de la Norma Suprema establece que *"Los derechos se podrán ejercer, promover y exigir deforma individual o colectiva. ante las autoridades competentes; estas autoridades garantizarán su cumplimiento.";*

Que, el numeral 2 del artículo 11 de la Norma Suprema prescribe que *"Todas las personas son iguales y gozarán de los mismos derechos y oportunidades";*

Que, el numeral 3 del artículo 11 de la Constitución de la República preceptúa que *"Los derechos y garantías establecidas en la Constitución y en los instrumentos internacionales de derechos humanos serán de directa c inmediata aplicación por y ante cualquier servidora o servidor público, administrativo o judicial, de oficio o a petición de parte";*

Que, el numeral 8 del artículo 11 de la Norma Suprema dispone que: *"El contenido de los derechos y garantías establecidos en la Constitución y en los instrumentos internacionales de derechos humanos, no excluirá los demás derechos derivados de la dignidad de las personas, comunidades, pueblos y nacionalidades, que sean necesarios para su pleno desenvolvimiento. Será inconstitucional cualquier acción u omisión de carácter regresivo*

que disminuya, menoscabe o anule injustificadamente el ejercicio de los derechos";

Que, el artículo 16 numerales 1 y 2 de la Carta Magna determina que *"Todas las personas, en forma individual o colectiva, tienen derecho a: 1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos; 2. El acceso universal a las tecnologías de información y comunicación";*

Que, el artículo 17 numeral 2 de la Norma Suprema preceptúa que *"El Estado fomentará pluralidad y la diversidad en la comunicación, y al efecto: 2. Facilitará la creación y el fortalecimiento de medios de comunicación públicos, privados y comunitarios, así como el acceso universal a las tecnologías de la información y comunicación en especial para las personas y colectividades que carezcan de dicho acceso o lo tengan de forma limitada";*

Que, el artículo 26 de la Constitución de la República reconoce que *"La educación es un derecho de las personas a lo largo de su vida y un deber inexcusable el Estado. Constituye un área prioritaria de la política pública y de la inversión estatal, garantía de la igualdad e inclusión social v condición indispensable para el buen vivir. Las personas, las familias y la sociedad tienen el derecho y la responsabilidad de participar en el proceso educativo"]*

Que, el artículo 35 de la Carta Magna establece que *"Las personas adultas mayores, niñas, niños y adolescentes, mujeres embarazadas, personas con discapacidad, personas privadas de libertad y quienes adolezcan de enfermedades catastróficas* o *de alta complejidad, recibirán atención prioritaria y especializada en los ámbitos públicos y privado. La misma atención prioritaria recibirán las personas en situación de riesgo, las víctimas de violencia doméstica y sexual, maltrato infantil, desastres naturales o antropogénicos. El Estado prestará especial protección a las personas en condición de doble vulnerabilidad"**;***

Que, el artículo 44 de la Norma Suprema dispone que *"El Estado, la sociedad, y la familia promoverán de forma prioritaria el desarrollo integral de los niñas, niños y adolescentes, y asegurarán el ejercicio pleno de sus derechos, se atenderá al principio de su interés superior y sus derechos prevalecerán sobre los de las demás personas. Las niñas, niños y adolescentes tendrán derecho a. su desarrollo integral, entendido como proceso de crecimiento, maduración y despliegue de su intelecto y de sus capacidades, potencialidades y aspiraciones, en un entorno familiar, escolar, social y comunitario de efectividad v seguridad. Este entorno permitirá la satisfacción de sus necesidades sociales, afectivo-emocionales y culturales, con el apoyo de políticas intersectoriales nacionales y locales.";*

Que, el artículo 66 numeral 19 de la Constitución de la República reconoce y garantiza a las personas: *"19. El derecho a la protección de datos carácter personal, que incluye el acceso y la. decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión*

de estos datos personales requerirán la autorización del titular o el mandato de ley":

Que, el numeral 6 del artículo 76 de la Carta Magna determina que *"En todo proceso que se determinen derechos y obligaciones de cualquier orden, se asegurará el derecho al debido proceso que incluirá las siguientes garantías básicas: 6. La ley establecerá la debida proporcionalidad entre las infracciones y las sanciones penales, administrativas o de otra naturaleza,";*

Que, el artículo 92 de la Norma Suprema prescribe que: *"Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación* o *anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados";*

Que, el artículo 227 de la Constitución de la República establece que: *"La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación.";*

Que, el artículo 277 de la Constitución de la República determina que: *"Para la consecución del buen vivir, serán deberes generales del Estado: 1. Garantizar los derechos de las personas, las colectividades y la naturaleza; 2. Dirigir, planificar y regular el proceso de desarrollo; 3. Generar y ejecutar las políticas públicas y controlar y sancionar su incumplimiento; 4. Producir bienes, crear y mantener infraestructura y proveer servicios públicos; 5. Impulsar el desarrollo de las actividades económicas mediante un orden jurídico e instituciones políticas que las promuevan, fomenten y defiendan mediante el cumplimiento de la Constitución y la ley; 6. Promover e impulsar la ciencia, la tecnología, las artes, los saberes ancestrales y en general las actividades de la iniciativa creativa, comunitaria, asociativa, cooperativa y privada. .;*

Que, el artículo 417 de la Norma Suprema dispone que *"Los tratados internacionales ratificados por el Ecuador se sujetarán a lo establecido en la Constitución. En el caso de los tratados y otros instrumentos internacionales de derechos humanos se aplicarán los principios pro ser humano, de no restricción de derechos, de aplicabilidad directa y de cláusula abierta establecida en la Constitución";*

Que, el numeral 3 del artículo 423 de la Constitución de la República prevé que *"La integración en especial con los países de Latinoamérica y el Caribe será un objetivo estratégico del Estado. En todas las instancias y procesos de integración, el Estado ecuatoriano se comprometerá a 3 Fortalecer la armonización de las legislaciones nacionales con énfasis en los derechos (...), de acuerdo con los principios de progresividad y no regresividad.";*

Que, el artículo 424 de la Carta Magna prescribe que *"La Constitución es la norma suprema y prevalece sobre cualquier otra del ordenamiento jurídico. Las normas y los actos del poder público deberán mantener conformidad con las disposiciones constitucionales, en caso contrario carecerán de eficacia jurídica. La Constitución y los tratados internacionales de derechos humanos ratificados por el Estado que reconozcan derechos más favorables a los contenidos en la Constitución, prevalecerán sobre cualquier otra norma jurídica o acto del poder público";*

Que, la Resolución 45/95 de 14 de diciembre de 1990 de la Organización de las Naciones Unidas adopta principios rectores para la reglamentación de los ficheros computarizados de datos personales, garantías mínimas que deberán preverse en legislaciones nacionales para efectivizar este derecho;

Que, uno de los ejes de la Estrategia acordada en el año 2016 de la red Iberoamericana de Datos Personales 2020 consiste en *"Impulsar y contribuir al fortalecimiento y adecuación de los procesos regulatorios en la región, mediante la elaboración de directrices que sirvan de parámetros para futuras regulaciones o para revisión de las existentes en materia de protección de datos personales?*[3]*;*

Que, el 20 de junio de 2017 se aprobaron los Estándares de Protección de Datos Personales para los Estados Iberoamericanos;

Que, el Comité Jurídico Interamericano de la Organización de Estados Americanos adoptó la propuesta de declaración de principios de privacidad y protección de datos personales en las Américas;

Que, la Organización de Estados Americanos el 27 de marzo de 2015 desarrolló el Proyecto de Ley Modelo sobre Protección de datos Personales;

Que, la protección de datos personales forma parte de los ejes estratégicos para la construcción de la sociedad de la información y el conocimiento en el Ecuador conforme el Libro Blanco de la Sociedad de la Información y del Conocimiento 2018;

Que, la Acción Estratégica clave del enfoque para Gobierno de protección de datos personales del Eje 6 del Plan Nacional de la Sociedad de la Información y del Conocimiento 2018-2021, es *"Promulgar una ley orgánica de protección de datos personales para*

garantizar el derecho constitucional";

Que, el principio de Legalidad de la Carta Iberoamericana de Gobierno Electrónico del año 2007 establece que *"(...) el uso de comunicaciones electrónicas promovidas por la Administración Pública deberá tener observancia de las normas en materia de protección de datos personales",* con el objetivo de precautelar el derecho que tienen los ciudadanos a relacionarse electrónicamente con el Estado;

Que, la Estrategia 3 del Programa de Gobierno Abierto del Plan Nacional de Gobierno Electrónico apunta a "Impulsar la protección de la información y datos personales"; y,

En uso de la atribución que le confiere el número 6 del artículo 120 de la Constitución de la República, expide la siguiente:

LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES

Capítulo I
ÁMBITO DE APLICACIÓN INTEGRAL

Art. 1.- Objeto y finalidad.- El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela.

Art. 2.- Ámbito de aplicación material.- La presente ley se aplicará al tratamiento de datos personales contenidos en cualquier tipo de soporte, automatizados o no, así como a toda modalidad de uso posterior. La ley no será aplicable a:

a) Personas naturales que utilicen estos datos en la realización de actividades familiares o domésticas;
b) Personas fallecidas, sin perjuicio de lo establecido en el artículo 28 de la presente Ley;
c) Datos anonimizados, en tanto no sea posible identificar a su titular. Tan pronto los datos dejen de estar disociados o de ser anónimos, su tratamiento estará sujeto al cumplimiento de las obligaciones de esta ley, especialmente la de contar con una base de licitud para continuar tratando los datos de manera no anonimizada o disociada;
d) Actividades periodísticas y otros contenidos editoriales;
e) Datos personales cuyo tratamiento se encuentre regulado en normativa especializada de igual o mayor jerarquía en materia de gestión de riesgos por desastres naturales; y, seguridad *y* defensa del Estado, en cualquiera de estos casos deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y a los principios de esta ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad;
f) Datos o bases de datos establecidos para la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, llevado a cabo por los organismos estatales competentes en cumplimiento de sus funciones legales. En cualquiera de estos casos deberá darse cumplimiento a los estándares internacionales

en la materia de derechos humanos y a los principios de esta ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad; y
g) Datos que identifican o hacen identificable a personas jurídicas.

Son accesibles al público y susceptibles de tratamiento los datos personales referentes al contacto de profesionales y los datos de comerciantes, representantes y socios y accionistas de personas jurídicas y servidores públicos, siempre y cuando se refieran al ejercicio de su profesión, oficio, giro de negocio, competencias, facultades, atribuciones o cargo y se trate de nombres y apellidos, funciones o puestos desempeñados, dirección postal o electrónica, y, número de teléfono profesional. En el caso de los servidores públicos, además serán de acceso público y susceptibles de tratamiento de datos, el histórico y vigente de la declaración patrimonial y de su remuneración.
Art. 3.- Ámbito de aplicación territorial.- Sin perjuicio de la normativa establecida en los instrumentos internacionales ratificados por el Estado ecuatoriano que versen sobre esta materia, se aplicará la presente Ley cuando;

1. El tratamiento de datos personales se realice en cualquier parte, del territorio nacional;
2. El responsable o encargado del tratamiento de datos personales se encuentre domiciliado en cualquier parte del territorio nacional;
3. Se realice tratamiento de datos personales de titulares que residan en el Ecuador por parte de un responsable o encargado no establecido en el Ecuador, cuando las actividades del tratamiento estén relacionadas con: 1) La oferta de bienes o servicios a dichos titulares, independientemente de si a estos se les requiere su pago, o, 2) del control de su comportamiento, en la medida en que este tenga lugar en el Ecuador; y,
4. Al responsable o encargado del tratamiento de datos personales, no domiciliado en el territorio nacional, le resulte aplicable la legislación nacional en virtud de un contrato o de las regulaciones vigentes del derecho internacional público.
Art. 4.- Términos y definiciones.- Para los efectos de la aplicación de la presente Ley se establecen las siguientes definiciones:

Autoridad de Protección de Datos Personales: Autoridad pública independiente encargada de supervisar la aplicación de la presente ley, reglamento y resoluciones que ella dicte, con el fin de proteger los derechos y libertades fundamentales de las personas naturales, en cuanto al tratamiento de sus datos personales.

Anonimización: La aplicación de medidas dirigidas a impedir la identificación o reidentificación de una persona natural, sin esfuerzos desproporcionados.

Base de datos o fichero: Conjunto estructurado de datos cualquiera que fuera la forma, modalidad de creación, almacenamiento, organización, tipo de soporte, tratamiento, procesamiento, localización o acceso, centralizado, descentralizado o repartido de forma funcional o geográfica.

Consentimiento: Manifestación de la voluntad libre, específica, informada e inequívoca,

por el que el titular de los datos personales autoriza al responsable del tratamiento de los datos personales a tratar los mismos.

Dato biométrico: Dato personal único, relativo a las características físicas o fisiológicas, o conductas de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre otros.

Dato genético: Dato personal único relacionado a características genéticas heredadas o adquiridas de una persona natural que proporcionan información única sobre la fisiología o salud de un individuo.

Dato personal: Dato que identifica o hace identificable a una persona natural, directa o indirectamente.

Datos personales crediticios: Datos que integran el comportamiento económico de personas naturales, para analizar su capacidad financiera.

Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos, datos relativos a las personas apátridas y refugiados que requieren protección internacional, y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.

Datos relativos a la salud: datos personales relativos a la salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

Datos sensibles: Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.

Delegado de protección de datos: Persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la Autoridad de Protección de Datos Personales, sirviendo como punto de contacto entre esta y la entidad responsable del tratamiento de datos.

Destinatario: Persona natural o jurídica que ha sido comunicada con datos personales.

Elaboración de perfiles: Todo tratamiento de datos personales que permite evaluar, analizar o predecir aspectos de una persona natural para determinar comportamientos o

estándares relativos a: rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, ubicación, movimiento físico de una persona, entre otros.

Encargado del tratamiento de datos personales: Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo que solo o conjuntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales.

Entidad Certificadora: Entidad reconocida por la Autoridad de Protección de Datos Personales, que podrá, de manera no exclusiva, proporcionar certificaciones en materia de protección de datos personales.

Fuente accesible al público: Bases de datos que pueden ser consultadas por cualquier persona, cuyo acceso es público, incondicional y generalizado.

Responsable de tratamiento de datos personales: persona natural o jurídica, pública o privada, autoridad pública, u otro organismo, que solo o conjuntamente con otros decide sobre la finalidad y el tratamiento de datos personales.

Sellos de protección de datos personales: Acreditación que otorga la entidad certificadora al responsable o al encargado del tratamiento de datos personales, de haber implementado mejores prácticas en sus procesos, con el objetivo de promover la confianza del titular, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales.

Seudonimización: Tratamiento de datos personales de manera tal que ya no puedan atribuirse a un titular sin utilizar información adicional, siempre que dicha información adicional, figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

Titular: Persona natural cuyos datos son objeto de tratamiento.

Transferencia o comunicación: Manifestación, declaración, entrega, consulta, interconexión, cesión, transmisión, difusión, divulgación o cualquier forma de revelación de datos personales realizada a una persona distinta al titular, responsable o encargado del tratamiento de datos personales. Los datos personales que comuniquen deben ser exactos, completos y actualizados.

Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión,

aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales.

Vulneración de la seguridad de los datos personales: Incidente de seguridad que afecta la confidencialidad, disponibilidad o integridad de los datos personales.

Art. 5.- Integrantes del sistema de protección de datos personales.- Son parte del sistema de protección de datos personales, los siguientes:

1) Titular;
2) Responsable del tratamiento;
3) Encargado del tratamiento;
4) Destinatario;
5) Autoridad de Protección de Datos Personales; y,
6) Delegado de protección de datos personales.

Art. 6.- Normas aplicables al ejercicio de derechos.- El ejercicio de los derechos previstos en esta Ley se canalizará a través del responsable del tratamiento, Autoridad de Protección de Datos Personales o jueces competentes, de conformidad con el procedimiento establecido en la presente Ley y su respectivo Reglamento de aplicación. El Reglamento a esta Ley u otra norma secundaria no podrán limitar al ejercicio de los derechos.

Art. 7.- Tratamiento legítimo de datos personas.- El tratamiento será legítimo y lícito si se cumple con alguna de las siguientes condiciones:

1) Por consentimiento del titular para el tratamiento de sus datos personales, para una o varias finalidades especificas;
2) Que sea realizado por el responsable del tratamiento en cumplimiento de una obligación legal;
3) Que sea realizado por el responsable del tratamiento, per orden judicial, debiendo observarse los principios de la presente ley;
4) Que el tratamiento de datos personales se sustente en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, derivados de una competencia atribuida por una norma con rango de ley, sujeto al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta ley y a los criterios de legalidad, proporcionalidad y necesidad;
5) Para la ejecución de medidas precontractuales a petición del titular o para el cumplimiento de obligaciones contractuales perseguidas por el responsable del tratamiento de datos personales, encargado del tratamiento de datos personales o por un tercero legalmente habilitado;
6) Para proteger intereses vitales, del interesado o de otra persona natural, como su vida, salud o integridad;
7) Para tratamiento de datos personales que consten en bases de datos de acceso público; u,

8) Para satisfacer un interés legítimo del responsable de tratamiento o de tercero, siempre que no prevalezca el interés o derechos fundamentales de los titulares al amparo de lo dispuesto en esta norma.

Art. 8.- Consentimiento.- Se podrán tratar y comunicar datos personales cuando se cuente con la manifestación de la voluntad del titular para hacerlo. El consentimiento será válido, cuando la manifestación de la voluntad sea:

1) Libre, es decir, cuando se encuentre exenta de vicios del consentimiento;
2) Específica, en cuanto a la determinación concreta de los medios y fines del tratamiento;
3) Informada, de modo que cumpla con el principio de transparencia y efectivice el derecho a la transparencia,
4) Inequívoca, de manera que no presente dudas sobre el alcance de la autorización otorgada por el titular.

El consentimiento podrá revocarse en cualquier momento sin que sea necesaria una justificación., para lo cual el responsable del tratamiento de datos personales establecerá mecanismos que garanticen celeridad, eficiencia, eficacia y gratuidad, así como un procedimiento sencillo, similar al proceder con el cual recabó el consentimiento.

El tratamiento realizado antes de revocar el consentimiento es lícito, en virtud de que este no tiene efectos retroactivos.

Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado Dará una pluralidad de finalidades será preciso que conste que dicho consentimiento se otorga para todas ellas.

Art. 9.- Interés legítimo.- Cuando el tratamiento de datos personales tiene como fundamente el interés legítimo:

a) Únicamente podrán ser tratados los datos que sean estrictamente necesarios para la realización de la finalidad.
b) El responsable debe garantizar que el tratamiento sea transparente para el titular.
c) La Autoridad de Protección de Datos puede requerir al responsable un informe con de riesgo para la protección de daros, en el cual se verificará si no hay amenazas concretas a las expectativas legitimas de los titúlales y a sus derechos fundamentales.

Capítulo II
PRINCIPIOS

Art. 10.- Principios.- Sin perjuicio de otros principios establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, la presente Ley se regirá por los principios de;

a) Juridicidad.- Los datos personales deben tratarse con estricto apego y cumplimiento a los principios, derechos y obligaciones establecidas en la Constitución, los instrumentos internacionales, la presente Ley, su Reglamento y la demás normativa y jurisprudencia

aplicable.

b) Lealtad.- El tratamiento de datos personales deberá ser leal, por lo que para los titulares debe quedar claro que se están recogiendo, utilizando, consultando o tratando de otra manera, datos personales que les conciernen, así como las formas en que dichos datos son o serán tratados.

En ningún caso los datos personales podrán ser tratados a través de medios o para fines, ilícitos o desleales.

c) Transparencia.- El tratamiento de cacos personales deberá ser transparente. por lo que toda información o comunicación relativa a este tratamiento deberá ser fácilmente accesible y fácil de entender y se deberá utilizar un lenguaje sencillo y claro.

Las relaciones derivadas del tratamiento de datos personales deben ser transparentes y se rigen en función de las disposiciones contenidas en la presente Ley, su reglamento y demás normativa atinente a la materia.

d) Finalidad.- Las finalidades del tratamiento deberán ser determinadas, explícitas, legítimas y comunicadas al titular; no podrán tratarse datos personales con fines distintos para los cuales fueron recopilados, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta ley.

El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. Para ello, habrá de considerarse el contexto en el que se recogieron los datos, la información facilitada al titular en ese proceso y, en particular, las expectativas razonables del titular basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los titulares del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista.

e) Pertinencia y minimización de datos personales.- Los datos personales deben ser pertinentes y estar limitados a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento.

f) Proporcionalidad del tratamiento.- El tratamiento debe ser adecuado, necesario, oportuno, relevante y no excesivo con relación a las finalidades para las cuales hayan sido recogidos o a la naturaleza misma, de las categorías especiales de datos.

g) Confidencialidad.- El tratamiento de datos personales debe concebirse sobre la base del debido sigilo y secreto, es decir, no debe tratarse o comunicarse para un fin distinto para el cual fueron recogidos, a menos que concurra una de las causales que habiliten un

nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta ley.

Para tal efecto, el responsable del tratamiento deberá adecuar las medidas técnicas organizativas para cumplir con este principio.

h) Calidad y exactitud.- Los datos personales que sean objeto de tratamiento deben ser exactos, íntegros, precisos, completos, comprobables, claros; y, de ser el caso, debidamente actualizados; de tal forma que no se altere su veracidad. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

En caso de tratamiento por parte de un encargado, la calidad y exactitud será obligación del responsable del tratamiento de datos personales.

Siempre que el responsable del tratamiento haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, no le será imputable la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos:

a) Hubiesen sido obtenidos por el responsable directamente del titular.
b) Hubiesen sido obtenidos por el responsable de un intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario que recoja en nombre propio los datos de los afectados para su transmisión al responsable.
c) Fuesen obtenidos de un registro público por el responsable.

i) Conservación.- Los datos personales serán conservados durante un tiempo no mayor al necesario para cumplir con la finalidad de su tratamiento.

Para garantizar que los datos personales no se conserven más tiempo del necesario, el responsable del tratamiento establecerá plazos para su supresión o revisión periódica.

La conservación ampliada de tratamiento de datos personales únicamente se realizará con fines de archivo en interés público, fines de investigación científica, histórica o estadística, siempre y cuando se establezcan las garantías de seguridad y protección de datos personales, oportunas y necesarias, para salvaguardar los derechos previstos en esta norma.

j) Seguridad de datos personales.- Los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas y necesarias, entendiéndose por tales las aceptadas por el estado de la técnica, sean estas organizativas, técnicas o de cualquier otra índole, para proteger los datos personales, frente a cualquier riesgo, amenaza, vulnerabilidad, atendiendo a la naturaleza de los datos de carácter personal, al ámbito y el contexto.

k) Responsabilidad proactiva y demostrada.- El responsable del tratamiento de datos personales deberá acreditar el haber implementado mecanismos para la protección de datos personales; es decir, el cumplimiento de los principios, derechos y obligaciones establecidos en la presente Ley, para lo cual, además de lo establecido en la normativa aplicable, podrá valerse de estándares, mejores prácticas, esquemas de auto y coregulación, códigos de protección, sistemas de certificación, sellos de protección de datos personales o cualquier otro mecanismo que se determine adecuado a los fines, la naturaleza del dato personal o el riesgo del tratamiento.

El responsable del tratamiento de datos personales está obligado a rendir cuentas sobre el tratamiento al titular y a la Autoridad de Protección de Datos Personales.

El responsable del tratamiento de datos personales deberá evaluar y revisar los mecanismos que adopte para cumplir con el principio de responsabilidad de forma continua y permanente, con el objeto de mejorar su nivel de eficacia en cuanto a la aplicación de la presente Ley.

l) Aplicación favorable al titular.- En caso de duda sobre el alcance de las disposiciones del ordenamiento jurídico o contractuales, aplicables a la protección de datos personales, los funcionarios judiciales y administrativos las interpretarán y aplicarán en el sentido más favorable al titular de dichos datos.

m) Independencia del control.- Para el efectivo ejercicio del derecho a la protección de datos personales, y en cumplimiento de las obligaciones de protección de los derechos que tiene el Estado, la Autoridad de Protección de Datos deberá ejercer un control independiente, imparcial y autónomo, así como llevar a cabo las respectivas acciones de prevención, investigación y sanción.

Capítulo III
DERECHOS

Art. 11.- Normativa especializada.- Los datos personales cuyo tratamiento se encuentre regulado en normativa especializada en materia de ejercicio de la libertad de expresión, sectores regulados por normativa específica, gestión de riesgos, desastres naturales, seguridad nacional y defensa del Estado; y, los datos personales que deban proporcionarse a autoridades administrativas o judiciales en virtud de solicitudes y órdenes amparadas en competencias atribuidas en la normativa vigente, estarán sujetos a los principios establecidos en sus propias normas y los principios establecidos en esta Ley, en los casos que corresponda y sea de aplicación favorable. En todo caso deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y a los principios de esta ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad.

Art. 12.- Derecho a la información.- El titular de datos personales tiene derecho a ser informado conforme los principios de lealtad y transparente por cualquier medio sobre:

1) Los fines del tratamiento;
2) La base legal para el tratamiento;
3) Tipos de tratamiento;
4) Tiempo de conservación;
5) La existencia de una base de datos en la que constan sus datos personales;
6) El origen de los datos personales cuando no se hayan obtenido directamente del titular;
7) Otras finalidades y tratamientos ulteriores;
8) Identidad y datos de contacto del responsable del tratamiento de datos personales, que incluirá: dirección del domicilio legal, número de teléfono y correo electrónico;
9) Cuando sea del caso, identidad y datos de contacto del delegado de protección de datos personales, que incluirá: dirección domiciliaria, número de teléfono y correo electrónico;
10) Las transferencias o comunicaciones, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y sus clases, así como las finalidades que motivan la realización de estas y las garantías de protección establecidas;
11) Las consecuencias para el titular de los datos personales de su entrega o negativa a ello;
12) El efecto de suministrar datos personales erróneos o inexactos;
13) La posibilidad de revocar el consentimiento;
14) La existencia y forma en que pueden hacerse efectivos sus derechos de acceso, eliminación, rectificación y actualización, oposición, anulación, limitación del tratamiento y a no ser objeto de una decisión basada únicamente en valoraciones automatizadas.
15) Los mecanismos para hacer efectivo su derecho a la portabilidad, cuando el titular lo solicite;
16) Dónde y cómo realizar sus reclamos ante el responsable del tratamiento de datos personales *y* la Autoridad de Protección de Datos Personales, y;
17) La existencia de valoraciones y decisiones automatizadas, incluida la elaboración de perfiles.

En el caso que los datos se obtengan directamente del titular, la información deberá ser comunicada de forma previa a este, es decir, en el momento mismo de la recogida del dato personal.

Cuando los datos personales no se obtuvieren de forma directa del titular o fueren obtenidos de una fuente accesible al público, el titular deberá, ser informado dentro de los siguientes treinta (30) días o al momento de la primera comunicación con el titular, cualquiera de las dos circunstancias que ocurra primero. Se le deberá proporcionar información expresa, inequívoca, transparente, inteligible, concisa, precisa y sin barreras técnicas.

La información proporcionada al titular podrá transmitirse de cualquier modo comprobable en un lenguaje claro, sencillo y de fácil comprensión, de preferencia propendiendo a que pueda ser accesible en la lengua de su elección.

En el caso de productos o servicios dirigidos, utilizados o que pudieran ser utilizados por niñas, niños y adolescentes, la información a la que hace referencia el presente arríenlo será, proporcionada a su representante legal conforme a lo dispuesto en la presente Ley.

Art. 13.- Derecho de acceso.- El titular tiene derecho a conocer y a obtener, gratuitamente, del responsable de tratamiento acceso a todos sus datos personales y a la información detallada en el artículo precedente, sin necesidad de presentar justificación alguna. El responsable del tratamiento de datos personales deberá establecer métodos razonables que permitan el ejercicio de este derecho, el cual deberá ser atendido dentro del plazo de quince (15) días

El derecho de acceso no podrá ejercerse de forma tal que constituya abuso del derecho.

Art. 14.- Derecho de rectificación y actualización.- El titular tiene el derecho a obtener del responsable del tratamiento la rectificación y actualización de sus datos personales inexactos o incompletos.

Para tal efecto, el titular deberá presentar los justificativos del caso, cuando sea pertinente. El responsable de tratamiento deberá atender el requerimiento en un plazo de quince (15) días y en este mismo plazo, deberá informar al destinatario de los datos, de ser el caso, sobre la rectificación, a fin de que lo actualice.

Art. 15.- Derecho de eliminación.- El titular tiene derecho a que el responsable del tratamiento suprima sus datos personales, cuando:

1) El tratamiento no cumpla con los principios establecidos en la presente ley;
2) El tratamiento no sea necesario o pertinente para el cumplimiento de la finalidad;
3) Los datos personales hayan cumplido con la finalidad para la cual fueron recogidos o tratados;
4) Haya vencido el plazo de conservación de los datos personales;
5) El tratamiento afecte derechos fundamentales o libertades individuales;
6) Revoque el consentimiento prestado o señale no haberlo otorgado para uno o varios fines específicos, sin necesidad de que medie justificación alguna; o,
7) Exista obligación legal.

El responsable del tratamiento de datos personales implementará métodos y técnicas orientadas a eliminar, hacer ilegible, o dejar irreconocibles de forma definitiva y segura los datos personales. Esta obligación la deberá cumplir en el plazo de quince (15) días de recibida la solicitud por parte del titular y será gratuito.

Art. 16.- Derecho de oposición.- El titular tiene el derecho a oponerse o negarse al tratamiento de sus datos personales, en los siguientes casos:

1) No se afecten derechos y libertades fundamentales de terceros, la ley se lo permita y no se trate de información pública, de interés público o cuyo tratamiento está ordenado por la ley.
2) El tratamiento de datos personales tenga por objeto la mercadotecnia directa; el

interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles; en cuyo caso los datos personales dejarán de ser tratados para dichos fines.
3) Cuando no sea necesario su consentimiento para el tratamiento como consecuencia de la concurrencia de un interés legítimo, previsto en el artículo 7, y se justifique en una situación concreta personal del titular, siempre que una ley no disponga lo contrario.

El responsable de tratamiento dejará de tratar los datos personales en estos casos, salvo que acredite motivos legítimos e imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del titular, o para la formulación, el ejercicio o la defensa de reclamaciones.

Esta solicitud deberá ser atendida dentro del plazo de quince (15) días
Art. 17.- Derecho a la portabilidad.- El titular tiene el derecho a recibir del responsable del tratamiento, sus datos personales en un formato compatible, actualizado, estructurado, común, ínter-operable y de lectura mecánica, preservando sus características; o a transmitirlos a otros responsables. La Autoridad de Protección de Datos Personales deberá dictar la normativa para el ejercicio del derecho a la portabilidad.

El titular podrá solicitar que el responsable del tratamiento realice la transferencia o comunicación de sus datos personales a otro responsable del tratamiento en cuanto fuera técnicamente posible y sin que el responsable pueda aducir impedimento de cualquier orden con el fin de ralentizar el acceso, la transmisión o reutilización de datos por parte del titular o de otro responsable del tratamiento. Luego de completada la transferencia de datos, el responsable que lo haga procederá a su eliminación, salvo que el titular disponga su conservación. El responsable que ha recibido la información asumirá las responsabilidades contempladas en esta Ley.

Para que proceda el derecho a la portabilidad de datos es necesario que se produzca al menos una de las siguientes condiciones;

1) Que el titular haya otorgado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. La transferencia o comunicación se hará entre responsables del tratamiento de datos personales cuando la operación sea técnicamente posible; en caso contrario los datos deberán ser transmitidos directamente al titular.
2) Que el tratamiento se efectúe por medios automatizados;
3) Que se trate de un volumen relevante de datos personales, según los parámetros definidos en el reglamento de la presente ley; o,
4) Que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos del responsable o encargado del tratamiento de datos personales, o del titular en el ámbito del derecho laboral y seguridad social

Esta transferencia o comunicación debe ser económica y financieramente eficiente,

expedita y sin trabas.

No procederá este derecho cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable del tratamiento de datos personales 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.

Art. 18.- Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad.- Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad. No proceden los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad, en los siguientes casos;

1) Si el solicitante no es el titular de los datos personales o su representante legal no se encuentre debidamente acreditado;
2) Cuando los datos son necesarios para el cumplimiento de una obligación legal o contractual;
3) Cuando los datos son necesarios para el cumplimiento de una orden judicial, resolución o mandato motivado de autoridad pública competente;
4) Cuando los datos son necesarios para la formulación, ejercicio o defensa de reclamos o recursos;
5) Cuando se pueda causar perjuicios a derechos o afectación a intereses legítimos de terceros y ello sea acreditado por el responsable de la base de datos al momento de dar respuesta al titular a su solicitud de ejercicio del derecho respectivo;
6) Cuando se pueda obstaculizar actuaciones judiciales o administrativas en curso, debidamente notificadas;
7) Cuando los datos son necesarios para ejercer el derecho a la libertad de expresión y opinión;
8) Cuando los datos son necesarios para proteger el interés vital del interesado o de otra persona natural;
9) En los casos en los que medie el interés público, sujeto al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta ley y a los criterios de legalidad, proporcionalidad y necesidad;
10) En el tratamiento de datos personales que sean necesarios para el archivo de información que constituya patrimonio del Estado, investigación científica, histórica o estadística.

Art. 19.- Derecho a la suspensión del tratamiento.- El titular tendrá derecho a obtener del responsable del tratamiento la suspensión del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

1) Cuando el titular impugne la exactitud de los datos personales, mientras el responsable de tratamiento verifica la exactitud de los mismos;
2) El tratamiento sea ilícito *y* el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

3) El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; y.
4) Cuando el interesado se haya opuesto al tratamiento en virtud del artículo 31 de la presente ley; mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

De existir negativa por parte del responsable o encargado del tratamiento de datos personales^ y el titular recurra por dicha decisión ante la Autoridad de Protección de Datos Personales, esta suspensión se extenderá hasta la resolución del procedimiento administrativo.

Cuando el titular impugne la exactitud de los datos personales, mientras el responsable de tratamiento verifica la exactitud de los mismos, deberá colocarse en la base de datos, en donde conste 1a información impugnada, que ésta ha sido objeto de inconformidad por parte del titular.

El responsable de tratamiento podrá tratar los datos personales, que han sido objeto del ejercicio del presente derecho por parte del titular, únicamente, en los siguientes supuestos; para la formulación, el ejercicio o la defensa de reclamaciones; con el objeto de proteger los derechos de otra persona natural o jurídica o por razones de interés público importante.
Art. 20.- Derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas.- El titular tiene derecho a no ser sometido a una decisión basada única o parcialmente en valoraciones que sean producto de procesos automatizados, incluida la elaboración de perfiles, que produzcan efectos jurídicos en el o que atenten contra sus derechos y libertades fundamentales, para lo cual podrá:

a. Solicitar al responsable del tratamiento una explicación motivada sobre la decisión tomada por el responsable c encargado del tratamiento de datos personales;
b. Presentar observaciones;
c. Solicitar los criterios de valoración sobre el programa automatizado; o,
d. Solicitar al responsable información sobre los tipos de datos utilizados y la fuente de la cual han sido obtenidos los mismos; e. Impugnar la decisión ante el responsable o encargado del tratamiento

No se aplicará este derecho cuando

1. La decisión es necesaria para la celebración o ejecución de un contrato entre el titular *y* el responsable o encargado del tratamiento de datos personales;
2. Está autorizada por la normativa aplicable, orden judicial, resolución o mandato motivado de autoridad técnica competente; para lo cual se deberá establecer medidas adecuadas para salvaguardar los derechos fundamentales y libertades del titular; o,

3. Se base en el consentimiento explícito del titular.
4. La decisión no conlleve impactos graves o riesgos verificables para el titular.

No se podrá exigir la renuncia a este derecho en forma adelantada a través de contratos de adhesión masivos A más lardar en el momento de la primera comunicación con el titular de los datos personales, para informar una decisión basada únicamente en valoraciones automatizadas, este derecho le será informado explícitamente por cualquier medio idóneo..

Art. 21.- **Derecho de niñas, niños y adolescentes a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas.-** Además de los presupuestos establecidos en el derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas, no se podrán tratar datos sensibles o datos de niñas, niños y adolescentes a menos que se cuente con la autorización expresa del titular o de su representante legal; o, cuando, dicho tratamiento esté destinado a salvaguardar un interés público esencial, el cual se evalúe en atención a los estándares internacionales de derechos humanos, y como mínimo satisfaga los criterios de legalidad, proporcionalidad y necesidad, y además incluya salvaguardas específicas para proteger los derechos fundamentales de los interesados.

Los adolescentes, en ejercicio progresivo de sus derechos, a partir de los 15 años, podrán otorgar, en calidad de titulares, su consentimiento explícito para el tratamiento de sus datos personales, siempre que se les especifique con claridad sus fines.

Art. 22.- **Derecho de consulta.-** Las personas tienen derecho a la consulta pública y gratuita ante el Registro Nacional de Protección de Datos Personales, de conformidad con la presente Ley.

Art. 23.- **Derecho a la educación digital.-** Las personas tienen derecho al acceso y disponibilidad del conocimiento, aprendizaje, preparación, estudio, formación; capacitación, enseñanza e instrucción relacionados con el uso y maneje adecuado, sano, constructivo, seguro y responsable de las tecnologías de la información y comunicación, en estricto apego a la dignidad e integridad humana, los derechos fundamentales y libertades individuales con especial énfasis en la intimidad, la vida privada, autodeterminación informativa, identidad y reputación en línea, ciudadanía digital y el derecho a la protección de datos personales, así como promover una cultura sensibilizada en el derecho de protección de datos personales.

El derecho a la educación digital tendrá un carácter inclusivo sobre todo en lo que respecta a los personas con necesidades educativas especiales.

El sistema educativo nacional, incluyendo el sistema de educación superior, garantizará la educación digital no solo a favor de los estudiantes de todos los niveles sino también de los docentes, debiendo incluir dicha temática en su proceso de formación.

Art. 24.- **Ejercicio de derechos.-** El Estado, entidades educativas, organizaciones de la sociedad civil, proveedores de servicios de la sociedad de la información y el conocimiento, y otros entes relacionados, dentro del ámbito de sus relaciones, están

obligados a proveer información y capacitación relacionadas con el uso y tratamiento responsable, adecuado y seguro de datos personales de niñas, niños y adolescentes, tanto a sus titulares como a sus representantes legales, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales.

Los adolescentes mayores de doce (12) años y menores de quince (15) años, así como las niñas y niños, para el ejercicio de sus derechos necesitarán de su representante legal. Los adolescentes mayores de quince (15) años y menores de dieciocho (18) años, podrán ejercitarlos de forma directa ante la Autoridad de Protección de Datos Personales o ante el responsable de la base de datos personales del tratamiento.

Los derechos del titular son irrenunciables. Será nula toda estipulación en contrario.

Capítulo IV
CATEGORÍAS ESPECIALES DE DATOS

Art. 25.- Categorías especiales de datos personales.- Se considerarán categorías especiales de datos personales, los siguientes:

a) Datos sensibles;-
b) Datos de niñas, niños y adolescentes:
c) Datos de salud; y,
d) Datos de personas con discapacidad y de sus sustitutos, relativos a la discapacidad.

Art. 26.- Tratamiento de datos sensibles.- Queda prohibido el tratamiento de datos personales sensibles salvo que concurra alguna de las siguientes circunstancias:

a) El titular haya dado su consentimiento explícito para el tratamiento de sus datos personales, especificándose claramente sus fines.
b) El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular en el ámbito del Derecho laboral y de la seguridad y protección social.
c) El tratamiento es necesario para proteger intereses vitales del titular o de otra persona natural, en el supuesto de que el titular no esté capacitado, física o jurídicamente, para dar su consentimiento.
d) El tratamiento se refiere a datos personales que el titular ha hecho manifiestamente públicos.
e) El tratamiento se lo realiza por orden de autoridad judicial.
f) El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular.
g) Cuando el tratamiento de los datos de salud se sujete a las disposiciones contenidas en la presente ley.

Art. 27.- Datos personales de personas fallecidas.- Los titulares de derechos sucesorios de las personas fallecidas, podrán dirigirse al responsable del tratamiento de datos personales con el objeto de solicitar el acceso, rectificación y actualización o eliminación de los datos personales del causante, siempre que el titular de los datos no haya, en vida, indicado otra utilización o destino para sus datos.

Las personas o instituciones que la o el fallecido haya designado expresamente para ello, podrán también solicitar con arreglo a las instrucciones recibidas, el acceso a los datos personales de éste; y, en su caso, su rectificación, actualización o eliminación.

En caso de fallecimiento de niñas, niños, adolescentes o personas que la ley reconozca come incapaces, las facultades de acceso, rectificación, actualización o eliminación, podrán ser ejercidas por quien hubiese sido su último representante legal. El Reglamento a la presente ley establecerá los mecanismos para el ejercicio de las facultades enunciadas en el presente artículo.

Art. 28.- Datos crediticios.- Salvo prueba en contrario será legítimo y lícito el tratamiento de datos destinados a informar sobre la solvencia patrimonial o crediticia, incluyendo aquellos relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial o crediticia que permitan evaluar la concertación de negocios en general, la conducta comercial o la capacidad de pago del titular de los datos, en aquellos casos en que los mismos sean obtenidos de fuentes de acceso público o procedentes de informaciones facilitadas por el acreedor. Tales datos pueden ser utilizados solamente para esa finalidad de análisis y no serán comunicados o difundidos, ni podrán tener cualquier finalidad secundaria.

La protección de datos personales crediticios se sujetará a lo previsto en la presente ley, en la legislación especializada sobre la materia y demás normativa dictada por la Autoridad de Protección de Datos Personales.

Sin perjuicio de lo anterior, en ningún caso podrán comunicarse los datos crediticios relativos a obligaciones de carácter económico, financiero, bancario o comercial una vez transcurridos cinco años desde que la obligación a la que se refieran se haya hecho exigible.

Art. 29.- Derechos de los Titulares de Datos Crediticios.-

1. Sin perjuicio de los derechos reconocidos en esta Ley, los Titulares de Datos Crediticios tienen los siguientes derechos:

a) Acceder de forma personal a la información de la cual son titulares;
b) Que el reporte de crédito permita conocer de manera clara y precisa la condición en que se encuentra su historial crediticio; y,
c) Que las fuentes de información actualicen, rectifiquen o eliminen, según el caso, la información que fuese ilícita, falsa, inexacta, errónea, incompleta o caduca

2. Sobre el derecho de acceso por el Titular del Dato Crediticio, éste será gratuito, cuantas veces lo requiera, respecto de La información que sobre sí mismos esté registrada ante los prestadores de servicios de referencia crediticia y a través de los siguientes mecanismos:

a) Observación directa a través de pantallas que los prestadores del servicio de referencia crediticia pondrán a disposición de dichos titulares; y,
b) Entrega de impresiones de los reportes que a fin de que el Titular del Dato Crediticio compruebe la veracidad y exactitud de su contenido, sin que pueda ser utilizado con fines crediticios o comerciales.

3. Sobre los derechos de actualización., rectificación o eliminación, el Titular del Dato Crediticio podrá exigir estos derechos frente a las fuentes de información mediante solicitud escrita. Las fuentes de información, dentro del plazo de quince días de presentada la solicitud, deberán resolverla admitiéndola o rechazándola motivadamente. El Titular del Dato Crediticio tiene derecho a solicitar a los prestadores del servicio de referencias crediticias que, en tanto se sigue el proceso de revisión, señalen en los reportes de crédito que emitan, que la información materia de la solicitud está siendo revisada a pedido del titular.

Art. 30.- Datos relativos a la salud.- Las instituciones que conforman el Sistema Nacional de Salud y los profesionales de la salud pueden recolectar y tratar los datos relativos a la salud de sus pacientes que estén o hubiesen estado bajo tratamiento de aquellos, de acuerde a lo previsto en la presente ley. en la legislación especializada sobre la materia y demás normativa dictada por la Autoridad de Protección de Datos Personales en coordinación con la autoridad sanitaria nacional.

Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este, estarán sujetas al deber de confidencialidad, de tal manera que se garantice una segundad adecuada de los datos personajes, incluida la protección contra, el tratamiento no autorizado o ilícito y contra su pérdida, destrucción c daño accidental, mediante la aplicación de medidas técnicas organizativas apropiadas. Esta obligación será complementaria del secreto profesional de conformidad con cada caso.

Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

No se requerirá el consentimiento de) titular para el tratamiento de datos de salud cuando ello sea necesario por razones de interés público esencial en el ámbito de la salud, el que en todo caso deberá ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular;

Asimismo, tampoco se requerirá el consentimiento del titular cuando el tratamiento sea

necesario por razones de interés público en el ámbito de la salud pública, como en el caso de amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, siempre y cuando se establezcan medidas adecuadas y específicas para proteger los derechos y libertades del titular y, en particular, el secreto profesional.

Art. 31.- Tratamiento de datos relativos a la salud.- Todo tratamiento de datos relativos a la salud deberá cumplir con los siguientes parámetros mínimos y aquellos que determine la Autoridad de Protección de Datos Personales en la normativa emitida para el efecto:

1. Los datos relativos a la salud generados en establecimientos de salud públicos o privados, serán tratados cumpliendo los principios de confidencialidad y secreto profesional. El titular de la información deberá brindar su consentimiento previo conforme lo determina esta Ley, salvo en los casos en que el tratamiento sea necesario para proteger intereses vitales del interesado, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento; o sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico,, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base de la legislación especializada sobre la materia o en virtud de un contrato con un profesional sanitario. En este último caso el tratamiento sólo podré, ser realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con la legislación especializada sobre la materia o con las demás normas que al respecto pueda establecer la Autoridad.
2. Los datos relativos a la salud que se traten, siempre que sea posible, deberán ser previamente anonimizados o seudonimizados, evitando la posibilidad de identificar a los titulares de los mismos.
3. Todo tratamiento de datos de salud anonimizados deberá ser autorizado previamente por la Autoridad de Protección de Datos Personales. Para obtener la autorización mencionada, el interesado deberá presentar un protocolo técnico que contenga los parámetros necesarios que garanticen la protección de dichos datos y el informe previo favorable emitido por la Autoridad Sanitaria.

Art. 32.- Tratamiento de datos de salud por entes privados y públicos con fines de investigación.- Los datos relativos a salud que consten en las instituciones que conforman el Sistema Nacional de Salud, podrán ser tratados por personas naturales y jurídicas privadas y públicas con fines de investigación científica, siempre que según el caso encuentren anonimizados, o dicho tratamiento sea autorizado por la Autoridad de Protección de Datos Personales, previo informe de la Autoridad Sanitaria Nacional.

Capítulo V
TRANSFERENCIA O COMUNICACIÓN Y ACCESO A DATOS PERSONALES POR TERCEROS

Art. 33.- Transferencia o comunicación de datos personales.- Los datos personales podrán transferirse o comunicarse a terceros cuando se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del responsable y del destinatario, cuando la transferencia se encuentre configurada dentro de una de las

causales de legitimidad establecidas en esta Ley, y se cuente, además, con el consentimiento del titular.

Se entenderá que el consentimiento es informado cuando para la transferencia o comunicación de datos personales el Responsable del tratamiento haya entregado información suficiente al titular que le permita conocer la finalidad a que se destinarán sus datos y el tipo de actividad del tercero a quien se pretende transferir o comunicar dichos datos.

Art. 34.- Acceso a datos personales por parte del encargado.- No se considerará transferencia o comunicación en el caso de que el encargado acceda a datos personales para la prestación de un servicio al responsable del tratamiento de datos personales. El tercero que ha accedido legítimamente a datos personales en estas consideraciones, será considerado encargado del tratamiento.

El tratamiento de datos personales realizado por el encargado deberá estar regulado por un contrato, en el que se establezca de manera clara y precisa que el encargado del tratamiento de datos personales tratará únicamente los mismos conforme las instrucciones del responsable y que no los utilizará para finalidades diferentes a las señaladas en el contrato, ni que los transferirá o comunicará ni siquiera para su conservación a otras personas.

Una vez que se haya cumplido la prestación contractual, los datos personales deberán ser destruidos o devueltos al responsable del tratamiento de datos personales bajo la supervisión de la Autoridad de Protección de Datos Personales.

El encargado será responsable de las infracciones derivadas del incumplimiento de las condiciones de tratamiento de datos personales establecidas en la presente ley.

Art. 35.- Acceso a datos personales por parte de terceros.- No se considerará transferencia o comunicación cuando el acceso a datos personales por un tercero sea necesario para la prestación de un servicio al responsable del tratamiento de datos personales. El tercero que ha accedido a datos personales en estas condiciones debió hacerlo legítimamente.

El tratamiento de datos personales realizado por terceros deberá estar regulado por un contrato, en el que se establezca de manera clara y precisa que el encargado del tratamiento de datos personales tratará únicamente los mismos conforme las instrucciones del responsable y que no los utilizará para finalidades diferentes a las Señaladas en el contrato, ni que los transferirá o comunicará ni siquiera para su conservación a otras personas.

Una vez que se haya cumplido la prestación contractual, los datos personales deberán ser destruidos o devueltos al responsable del tratamiento de datos personales bajo la supervisión de la autoridad de protección de datos personales.

El tercero será responsable de las infracciones derivadas del incumplimiento de las condiciones de tratamiento de datos personales establecidas en la presente ley.

Art. 36.- Excepciones de consentimiento para la transferencia o comunicación de datos personales.- No es necesario contar con el consentimiento del titular para la transferencia o comunicación de datos personales, en los siguientes supuestos:

1) Cuando los datos han sido recogidos de fuentes accesibles al público;
2) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica entre el responsable de tratamiento y el titular, cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con base de datos. En este caso la transferencia o comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique;
3) Cuando los datos personales deban proporcionarse a autoridades administrativas o judiciales en virtud de solicitudes y órdenes amparadas en competencias atribuidas en la norma vigente;
4) Cuando la comunicación se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando dichos datos se encuentren debidamente disociados o a lo menos anonimizados, y,
5) Cuando la comunicación de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que implique intereses vitales de su titular y este se encontrare impedido de otorgar su consentimiento.
6) Cuando la comunicación de datos de carácter personal relativos a la salud sea necesaria para realizar los estudios epidemiológicos de interés público, dando cumplimiento a los estándares internacionales en la materia de derechos humanos, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad. El tratamiento deberá ser de preferencia anonimizado, y en todo caso agregado» una vez pasada la urgencia de interés público.

Cuando sea requerido el consentimiento del titular para que sus datos personales sean comunicados a un tercero, este puede revocarlo en cualquier momento, sin necesidad de que medie justificación alguna.

La presente ley obligatoriamente debe ser aplicada por el destinatario, por el solo hecho de la comunicación de los datos; a menos que estos hayan sido anonimizados o sometidos a un proceso de

Capítulo VI
SEGURIDAD DE DATOS PERSONALES

Art. 37.- Seguridad de datos personales.- El responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de

aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos.

El responsable o encargado del tratamiento de datos personales, deberá implementar un proceso de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole, implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales.

El responsable o encargado del tratamiento de datos personales deberá evidenciar que las medidas adoptadas e implementadas mitiguen de forma adecuada los riesgos identificados.

Entre otras medidas, se podrán incluir las siguientes;

1) Medidas de anonimización, seudonomización o cifrado de datos personales;
2) Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento de datos personales y el acceso a los datos personales, de forma rápida en caso de incidentes; y
3) Medidas dirigidas a mejorar la resiliencia técnica, física, administrativa, y jurídica.
4) Los responsables y encargados del tratamiento de datos personales, podrán acogerse a estándares internacionales para una adecuada gestión de riesgos enfocada a la protección de derechos y libertades, así como para la implementación y manejo de sistemas de seguridad de la información o a códigos de conducta reconocidos *y* autorizados por la Autoridad de Protección de Datos Personales.

Art. 38.- Medidas de seguridad en el ámbito del sector público.- El mecanismo gubernamental de seguridad de la información deberá incluir las medidas que deban implementarse en cl caso de tratamiento de datos personales para hacer frente a cualquier riesgo, amenaza., vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita en el tratamiento de los daros conforme al principio de seguridad de datos personales.

El mecanismo gubernamental de seguridad de la información abarcará y aplicará a todas las instituciones del sector público, contenidas en el artículo 225 de la Constitución de la República de Ecuador, así como a terceros que presten servicios públicos mediante concesión, u otras figuras legalmente reconocidas. Estas, podrán incorporar medidas adicionales al mecanismo gubernamental de seguridad de la información.

Art. 39.- Protección de datos personales desde el diseño y por defecto.- Se entiende a la protección de datos desde el diseño como el deber del responsable del tratamiento de tener en cuenta, en las primeras fases de concepción y diseño del proyecto, que determinados tipos de tratamientos de datos personales entrañan una serie de riesgos para los derechos de los titulares en atención al estado de la técnica, naturaleza y fines del tratamiento, para lo cual, implementará las medidas técnicas, organizativas y de cualquier otra Índole, con miras a garantizar el cumplimiento de las obligaciones en materia de

protección de datos, en los términos del reglamento.

La protección de datos por defecto hace referencia a que el responsable debe aplicar las medidas técnicas y organizativas adecuadas con miras a que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines del tratamiento, en los términos del reglamento.

Art. 40.- Análisis de riesgo, amenazas y vulnerabilidades.- Para el análisis de riesgos,, amenazas y vulnerabilidades, el responsable y el encargado del tratamiento de los datos personales deberán utilizar una metodología que considere, entre otras;

1) Las particularidades del tratamiento;
2) Las particularidades de las partes involucradas; y,
3) Las categorías y el volumen de datos personales objeto de tratamiento.

Art. 41.- Determinación de medidas de seguridad aplicables.- Para determinar las medidas de seguridad, aceptadas por el estado de la técnica, a las que están obligadas el responsable y el encargado del tratamiento de los datos personales, se deberán tomar en consideración, entre otros:

1) Los resultados del análisis de riesgos, amenazas y vulnerabilidades;
2) La naturaleza de los datos personales;
3) Las características de las partes involucradas; y,
4) Los antecedentes de destrucción de datos personales, la pérdida, alteración, divulgación o impedimento de acceso a los mismos por parte del titular, sean accidentales e intencionales, por acción u omisión, así como los antecedentes de transferencia, comunicación o de acceso no autorizado o exceso de autorización de tales datos.

El responsable y el encargado del tratamiento de datos personales deberán tomar las medidas adecuadas y necesarias, de forma permanente y continua, para evaluar, prevenir, impedir, reducir, mitigar y controlar los riesgos, amenazas y vulnerabilidades, incluidas las que conlleven un alto riesgo para los derechos y libertades del titular, de conformidad con la normativa que emita la Autoridad de Protección de Datos Personales.

Art. 42.- Evaluación de impacto del tratamiento de datos personales.- El responsable realizará una evaluación de impacto del tratamiento de datos personales cuando se haya identificado la probabilidad de que dicho tratamiento, por su naturaleza, contexto o fines, conlleve un alto riesgo para los derechos y libertades del titular o cuando la Autoridad de Protección de Datos Personales lo requiera.

La evaluación de impacto relativa a la protección de los datos será de carácter obligatoria en caso de:

a) Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas naturales;
b) Tratamiento a gran escala de las categorías especiales de datos, o de los datos

personales relativos a condenas e infracciones penales, o
c) Observación sistemática a gran escala de una zona de acceso público.

La Autoridad de Protección de Datos Personales establecerá otros tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos.

La evaluación de impacto deberá efectuarse previo al inicio del tratamiento de datos personales.

Art. 43.- Notificación de vulneración de seguridad.- El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales y la Agencia de Regulación y Control de las Telecomunicaciones, tan pronto sea posible, y a más tardar en el término de cinco (5) días después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la Autoridad de Protección de Datos no tiene lugar en el término de cinco (5) días, deberá ir acompañada de indicación de los motivos de la dilación.

El encargado del tratamiento deberá notificar al responsable cualquier vulneración de la seguridad de datos personales tan pronto sea posible, y a más tardar dentro del término de dos (2) días contados a partir de la fecha en la que tenga conocimiento de ella.

Art. 44.- Acceso a datos personales para atención a emergencias e incidentes informáticos.- Las autoridades públicas competentes, los equipos de respuesta de emergencias informáticas, los equipos de respuesta a incidentes de seguridad informática, los centros de operaciones de seguridad, los prestadores y proveedores de servicios de telecomunicaciones y los proveedores de tecnología y servicios de seguridad, nacionales e internacionales, podrán acceder y efectuar tratamientos sobre los datos personales contenidos en las notificaciones de vulneración a las seguridades, durante el tiempo necesario, exclusivamente para la detección, análisis, protección y respuesta ante cualquier tipo de incidentes así como para adoptar e implementar medidas de seguridad adecuadas y proporcionadas a los riesgos identificados.

Art. 45.- Garantía del secreto de las comunicaciones y seguridad de datos personales.- Para la correcta prestación de los servicios de telecomunicaciones y la apropiada operación de redes de telecomunicaciones, los prestadores de servicios de telecomunicaciones deben garantizar el secreto de las comunicaciones y seguridad de datos personales. Únicamente por orden judicial, los prestadores de servicios de telecomunicaciones podrán utilizar equipos, infraestructuras e instalaciones que permitan grabar los contenidos de las comunicaciones específicas dispuestas por los jueces competentes. Si se evidencia un tratamiento de grabación o interceptación de las comunicaciones no autorizadas por orden judicial se aplicará lo dispuesto en la presente Ley.

Art. 46.- Notificación de vulneración de seguridad al titular.- El responsable del tratamiento deberá notificar sin dilación la vulneración de seguridad de datos personales al titular cuando conlleve un riesgo a sus derechos fundamentales y libertades

individuales, dentro del término de tres días contados a partir de la fecha en la que tuvo conocimiento del riesgo.

No se deberá notificar la vulneración de seguridad de datos personales al titular en los siguientes casos:

1. Cuando el responsable del tratamiento haya adoptado medidas de protección técnicas organizativas o de cualquier otra índole apropiadas aplicadas a los datos personales afectados por la vulneración de seguridad que se pueda demostrar que son efectivas;
2. Cuando el responsable del tratamiento haya tomado medidas que garanticen que el riesgo para los derechos fundamentales y las libertades individuales del titular, no ocurrirá; y,
3. Cuando se requiera un esfuerzo desproporcionado para hacerlo; en cuyo caso, el responsable del tratamiento deberá realizar una comunicación pública a través de cualquier medio en la que se informe de la vulneración de seguridad de datos personales a los titulares.

La procedencia de las excepciones de los numerales 1 y 2 deberá ser calificada por la Autoridad de Protección de Datos, una vez informada esta tan pronto sea posible, y en cualquier caso dentro de los plazos contemplados en el Articulo 43.

La notificación al titular del dato objeto de la vulneración de segundad contendrá lo señalado en el artículo 43 de esta ley.

En caso de que el responsable del tratamiento de los datos personales no cumpliese oportunamente y de modo justificado con la notificación será sancionado conforme al régimen sancionatorio previsto en esta ley.

La notificación oportuna de la violación por parte del responsable cíe tratamiento al titular y la ejecución oportuna de medidas de respuesta, serán consideradas atenuante de la infra (sic).

Capítulo VII
DEL RESPONSABLE, ENCARGO Y DELEGADO DE PROTECCIÓN DE DATOS PERSONALES

Art. 47.- Obligaciones del responsable y encargado del tratamiento de datos personales.- El responsable del tratamiento de datos personales está obligado a:

1) Tratar datos personales en estricto apego a los principios y derechos desarrollados en la presente Ley, en su reglamente, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia;
2) Aplicar e implementar requisitos *y* herramientas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas, a fin de garantizar y demostrar que el tratamiento de daros personales se ha realizado conforme a lo previsto en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de

Protección de Datos Personales, o normativa sobre la materia;
3) Aplicar e implementar procesos de verificación, evaluación, valoración periódica de la eficiencia, eficacia y efectividad de los requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas implementadas;
4) Implementar políticas de protección de datos personales afines al tratamiento de datos personales en cada caso en particular;
5) Utilizar metodologías de análisis y gestión de riesgos adaptadas a las particularidades del tratamiento y de las partes involucradas;
6) Realizar evaluaciones de adecuación al nivel de seguridad previas al tratamiento de datos personales;
7) Tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas;
8) Notificar a la Autoridad de Protección de Datos Personales y al titular de los datos acerca de violaciones a las seguridades implementadas para el tratamiento de datos personales conforme a lo establecido en el procedimiento previsto para el efecto;
9) Implementar la protección de datos personales desde el diseño y por defecto;
10) Suscribir contratos de confidencialidad y manejo adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales;
11) Asegurar que el encargado del tratamiento de datos personales ofrezca mecanismos suficientes para garantizar el derecho a la protección de datos personales conforme a lo establecido en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, normativa sobre la materia y las mejores prácticas a nivel nacional o internacional;
12) Registrar y mantener actualizado el Registro Nacional de Protección de Datos Personales, de conformidad a lo dispuesto en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales;
13) Designar al Delegado de Protección de Datos Personales, en los casos que corresponda;
14) Permitir y contribuir a la realización de auditorias o inspecciones, por parte de un auditor acreditado por la Autoridad de Protección de Datos Personales; y,
15) Los demás establecidos en la presente Ley en su reglamento, en directrices, lineamientos, regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

El encargado de tratamiento de datos personales tendrá las mismas obligaciones que el responsable de tratamiento de datos personales, en lo que sea aplicable, de acuerdo a la presente ley y su reglamento.

Art. 48.- Delegado de protección de datos personales.- Se designará un delegado de protección de datos personales en los siguientes casos:

1) Cuando el tratamiento se lleve a cabo por quienes conforman el sector público de

acuerdo con lo establecido en el artículo 225 de la Constitución de la República;
2) Cuando las actividades del responsable o encargado del tratamiento de datos personales requieran un control permanente y sistematizado por su volumen, naturaleza, alcance o finalidades del tratamiento, conforme se establezca en esta ley, el reglamento a ésta, o en la normativa que dicte al respecto la Autoridad de Protección de Datos Personales;
3) Cuando se refiera al tratamiento a gran escala de categorías especiales de datos, de conformidad con lo establecido en el reglamento de esta ley; y,
4) Cuando el tratamiento no se refiera a datos relacionados con la seguridad nacional y defensa del Estado que adolezcan de reserva ni fuesen secretos, de conformidad con lo establecido en la normativa especializada en la materia.

La Autoridad de Protección de Datos Personales podrá definir nuevas condiciones en las que deba designarse un delegado de protección de datos personales y emitirá, a dicho efecto, las directrices suficientes para su designación.
Art. 49.- Funciones del delegado de protección de datos personales.- El delegado de protección de datos personales tendrá, entre otras, las siguientes funciones y atribuciones:

1) Asesorar al responsable, al personal del responsable y al encargado del tratamiento de datos personales, sobre las disposiciones contenidas en esta ley, el reglamento, las directrices, lineamientos y demás regulaciones emitidas por la Autoridad de Protección de Datos Personales;
2) Supervisar el cumplimiento de las disposiciones contenidas en esta ley, el reglamento, las directrices, lineamientos y demás regulaciones emitidas por la Autoridad de Protección de Datos Personales;
3) Asesorar en el análisis de riesgo, evaluación de impacto y evaluación de medidas de seguridad, y supervisar su aplicación;
4) Cooperar con la Autoridad de Protección de Datos Personales y actuar como punto de contacto con dicha entidad, con relación a las cuestiones referentes al tratamiento de datos personales; y,
5) Las demás que llegase a establecer la Autoridad de Protección de Datos Personales con ocasión de las categorías especiales de datos personales.

En caso de incumplimiento de sus funciones, el delegado de protección de datos personales responderá administrativa, civil y penalmente, de conformidad con la ley.
Art. 50.- Consideraciones especiales para el delegado de protección de datos personales.- Para la ejecución de las funciones del delegado de protección de datos, el responsable y el encargado de tratamiento de datos personales, deberán observar lo siguiente:

1) Garantizar que la participación del delegado de protección de datos personales, en todas las cuestiones relativas a la protección de datos personales, sea apropiada y oportuna;

2) Facilitar el acceso a los datos personales de las operaciones de tratamiento, así como todos los recursos y elementos necesarios para garantizar el correcto y libre desempeño de sus funciones:
3) Capacitar y actualizar en la materia al delegado de protección de datos personales, de conformidad con la normativa técnica que emita la Autoridad de Protección de Datos Personales;
4) No podrán destituir o sancionar al delegado de protección de datos personales por el correcto desempeño de sus funciones;
5) El delegado de protección de datos personales mantendrá relación directa con el más alto nivel ejecutivo y de decisión del responsable y con el encargado;
6) El titular de los datos personales podrá contactar al delegado de protección de datos personales con relación al tratamiento de sus datos personales a fin de ejercer sus derechos; y,
7) El delegado de protección de datos personales estará obligado a mantener la más estricta confidencialidad respecto a la ejecución de sus funciones.

Siempre que no exista conflicto con las responsabilidades establecidas en la préseme ley, su reglamento, directrices, lineamientos y demás regulaciones emitidas por la Autoridad de Protección de Datos Personales, el delegado de protección de datos personales podrá desempeñar otras funciones dispuestas por el responsable o el encargado del tratamiento de datos personales.

Art. 51.- Registro Nacional de protección de datos personales.- El responsable del tratamiento de datos personales deberá reportar y mantener actualizada la información ante la Autoridad de Protección de Datos Personales. sobre lo siguiente:

1) Identificación de la base de datos o del tratamiento;
2) El nombre domicilio legal y datos de contacto del responsable y encargado del tratamiento de datos personales;
3) Características y finalidad del tratamiento de datos personales;
4) Naturaleza de los datos personales tratados;
5) Identificación, nombre, domicilio legal y datos de contacto de los destinatarios de los datos personales, incluyendo encargados y terceros;
6) Modo de interrelacionar la información registrada;
7) Medios utilizados para implementar los principios, derechos y obligaciones contenidas en la presente ley y normativa especializada;
8) Requisitos y herramientas administrativas técnicas y físicas, organizativas y jurídicas implementadas para garantizar la seguridad y protección de datos personales;
9) Tiempo de conservación de los datos.

Capítulo VIII
DE LA RESPONSABILIDAD PROACTIVA

Art. 52.- Autorregulación.- Los responsables y encargados de tratamiento de datos personales podrán, de manera voluntaria, acogerse o adherirse a códigos de conducta, certificaciones, sellos y marcas de protección., cláusulas tipo, sin que esto constituya

eximente de la responsabilidad de cumplir con las disposiciones de la presente ley, su reglamento, directrices lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y demás normativa sobre la materia.

Art. 53.- Códigos de conducta.- La Autoridad de Regulación y Control promoverá la elaboración de códigos de conducta por sectores, industrias, empresas, organizaciones, que tengan como fin el cumplimiento de la normativa vigente en materia de protección de datos.

Los códigos de conducta deberán tomar en cuenta las necesidades específicas de los sectores en los que se efectúe tratamiento de datos personales, así como cumplir con los requisitos que se determinen en la normativa secundaria y con las disposiciones previstas en la, presente Ley, para su aprobación por la Autoridad de Regulación y Control.

Los responsables o encargados de tratamiento de datos personales interesados podrán adherirse e implementar los códigos de conducta aprobados, para lo cual seguirán el procedimiento establecido en el Reglamento a la presente Ley.

Art. 54.- Entidades de Certificación.- En materia de protección de datos personales las Entidades de Certificación, de manera no exclusiva y en concordancia con el artículo 52, podrán.

1) Emitir certificaciones de cumplimiento de la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y demás normativa sobre la materia;
2) Emitir sellos de protección de datos personales;
3) Llevar a cabo auditorías de protección de datos personales, y,
4) Certificar los procesos de transferencias internacionales de datos personales.

Los resultados de las auditorías podrán ser considerados como elementos probatorios dentro de los procesos sancionatorios.

Capítulo IX
TRANSFERENCIA O COMUNICACIÓN INTERNACIONAL DE DATOS PERSONALES

Art. 55.- Transferencia o comunicación internacional de datos personales.- La transferencia o comunicación internacional de datos personales será posible si se sujeta a lo previsto en el presente capítulo, la presente Ley o la normativa especializada en la materia, propendiendo siempre al efectivo ejercicio del derecho a la protección de datos personales.

Art. 56.- Transferencia o comunicación internacional de datos personales a países declarados como nivel adecuado de protección.- Por principio general se podrán transferir o comunicar datos personales a países, organizaciones y personas jurídicas en general que brinden niveles adecuados de protección, y que se ajusten a la obligación de cumplimiento y garantía de estándares reconocidos internacionalmente conforme a los criterios establecidos en el Reglamento a la ley.

Cuando resulte necesario por la naturaleza de la transferencia, la Autoridad de Protección de Datos Personales podrá implementar métodos de control ex post que serán definidos en el Reglamento a la Ley. También establecerá acciones conjuntas entre las autoridades de ambos países con el objeto de prevenir, corregir o mitigar el tratamiento indebido de datos en ambos países.

Para declarar de nivel adecuado de protección a países u organizaciones, la Autoridad de Protección de Datos Personales emitirá resolución motivada, en la que se establezca que la transferencia o comunicación internacional de datos personales cumple niveles adecuados de protección o de garantías adecuadas de protección,, conforme a lo establecido en esta ley y su reglamento.

Art. 57.- Transferencia o comunicación mediante garantías adecuadas.- En caso de realizar una transferencia internacional de datos a un país, organización o territorio económico internacional que no haya sido calificado por la Autoridad de Protección de Datos de tener un nivel adecuado de protección, se podrá realizar la referida transferencia internacional siempre que el responsable o encargado del tratamiento de datos personales ofrezca garantías adecuadas para el titular, para lo cual se deberá observar lo siguiente:

a. Garantizar el cumplimiento de principios, derechos y obligaciones en el tratamiento de datos personales en un estándar igual o mayor a la normativa ecuatoriana vigente.
b. Efectiva tutela del derecho a la protección de datos personales, a través de la disponibilidad permanente de acciones administrativas o judiciales; y,
c. El derecho a solicitar la reparación integral, de ser el caso.

Para que ello ocurra, la transferencia internacional de datos personales se sustentará en un instrumento jurídico que contemple los estándares antes determinados, así como aquellos que establezca la Autoridad de Protección de Datos Personales, el mismo que deberá ser vinculante.

Art. 58.- Normas corporativas vinculantes.- Los responsables o encargados del tratamiento de datos personales podrán presentar a la Autoridad de Protección de Datos Personales, normas corporativas vinculantes, especificas y aplicadas al ámbito de su actividad, las cuales deberán cumplir las siguientes condiciones:

1. Será de obligatorio cumplimiento para el responsable del tratamiento y para la empresa a la que eventualmente transfieran datos personales.
2. Brindar a los titulares los mecanismos adecuados para el ejercicio de sus derechos relacionados al tratamiento de sus datos personales observando las disposiciones de la presente ley;
3. Incluir una enunciación detallada de las empresas filiales que, además del responsable del tratamiento, pertenecen al mismo grupo empresarial. Además, se incluirá la estructura y los datos del contacto del grupo empresarial o joint venture, dedicadas a una actividad económica conjunta y de cada uno de sus miembros.
4. Incluir el detalle de las empresas encargadas del tratamiento de datos personales, las

categorías de datos personales a ser utilizados, así corno el tipo de tratamiento a realizarse y su finalidad;
5. Observar en su contenido todas las disposiciones de la presente ley referentes a principios de tratamiento de datos personales, medidas de seguridad de datos, requisitos respecto a transferencia o comunicación internacional y transferencia o comunicación ulterior a organismos no sujetos a normas corporativas vinculantes;
6. Contener la aceptación por parte del responsable o del encargado del tratamiento de los datos personales, o de cualquier miembro de su grupo empresarial sobre su responsabilidad por cualquier violación de las normas corporativas vinculantes. El responsable o encargado del tratamiento de datos personales no será responsable si demuestra que el acto que originó la violación no le es imputable;
7. Incluir los mecanismos en que se facilita al titular la información clara y completa, respecto a las normas corporativas vinculantes;
8. Incluir las funciones de todo delegado de protección de datos designado de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o del joint venture dedicadas a una actividad económica conjunta bajo un mismo control así como los mecanismos y procesos de supervisión y tramitación de reclamaciones;.
9. Enunciar de forma detallada los mecanismos establecidos en el grupo empresarial o empresas afiliadas que permitan al titular verificar efectivamente el cumplimiento de las normas corporativas vinculantes. Entre estos mecanismos se incluirán auditorías de protección de datos, y aquellos métodos técnicos que brinden acciones correctivas para proteger los derechos del titular. Los resultados de las auditorías serán comunicadas al delegado de protección de datos designado de conformidad con la presente ley, o cualquier otra entidad o persona encargada del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o empresas afiliadas dedicadas a una actividad económica conjunta y al Directorio de la empresa que controla un grupo empresarial, y a disposición de la Autoridad de protección de datos personales:
10. Incluir los mecanismos para cooperar de forma coordinada con la autoridad de protección de datos personales y el responsable del tratamiento de los datos personales; y,
11. Incluir la declaración y compromiso del responsable del tratamiento de los datos personales de promover la protección de datos personales entre sus empleados con formación continua.

La Autoridad de Protección de Datos Personales definirá el formato y los procedimientos para la transferencia o comunicación de datos realizada por parte de los responsables, los encargados y las autoridades de control en lo relativo a la aplicación de las normas corporativas vinculantes a las que se refiere este artículo.

Cualquier cambio a ser realizado a estas normas deberá ser notificado a la autoridad de protección de datos personales y al titular conforme a los mecanismos señalados por el responsable de tratamiento en su solicitud.

Art. 59.- Autorización para transferencia internacional.- Para todos aquellos casos no contemplados en los artículos precedentes, en los que se pretenda realizar una transferencia internacional de datos personales, se requerirá la autorización de la Autoridad de Protección de Datos, para lo cual, se deberá garantizar documentadamente el cumplimiento de la normativa vigente sobre protección de datos de carácter personal, según lo determinado en el Reglamento de aplicación a la presente Ley.

Sin perjuicio de lo anterior la información sobre transferencias internacionales de datos personales deberá ser registradas previamente en el Registro Nacional de Protección de Datos Personales por parte del responsable del tratamiento o, en su caso, del encargado, según el procedimiento establecido en el Reglamento de aplicación a la presente Ley.

Art. 60.- Casos excepcionales de transferencias o comunicaciones internacionales.- Sin perjuicio de lo establecido en los artículos precedentes se podrá realizar? transferencias o comunicaciones internacionales de datos personales, en los siguientes casos;

1. Cuando los datos personales sean requeridos para el cumplimiento de competencias institucionales, de conformidad con la normativa aplicable;
2. Cuando el titular haya otorgado su consentimiento explícito a la transferencia o comunicación propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias o comunicaciones internación a íes, debido a la ausencia de una resolución de nivel adecuado de protección y de garantías adecuadas.
3. Cuando la transferencia internacional tenga como finalidad el cumplimiento de una obligación legal o regulatoria;
4. Cuando la transferencia internacional de datos personales sea necesaria para la ejecución de un contrate entre el titular y el responsable del tratamiento de datos personales, o para la ejecución de medidas de carácter precontractual adoptadas a solicitud del titular;
5. Cuando la transferencia sea necesaria por razones de interés público.
6. Cuando la transferencia internacional sea necesaria para la colaboración judicial internacional.
7. Cuando la transferencia internacional sea necesaria para la cooperación dentro de la investigación de infracciones
8. Cuando la transferencia internacional es necesaria para el cumplimiento de compromisos adquiridos en procesos de cooperación internacional entre Estados;
9. Cuando se realicen transferencias de datos en operaciones bancarias y bursátiles.
10. Cuando la transferencia internacional de datos personales sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones, acciones administrativas o jurisdiccionales y recursos; y,
11. Cuando la transferencia internacional de datos personales sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento.

Art. 61.- Control continuo.- La Autoridad de Protección de Datos Personales en acciones conjuntas con la academia, realizará reportes continuos sobre la realidad internacional en materia de protección de datos personales. Dichos estudios servirán como elemento de

control continuo del nivel adecuado de protección de datos personales de los países u organizaciones que ostenten tal reconocimiento.

En caso de detectarse que un país u organización ya no cumple con un nivel adecuado de protección conforme los principios, derechos y obligaciones desarrollados en la presente Ley, la Autoridad de Protección de Datos Personales procederá a emitir la correspondiente resolución de no adecuación, a partir de la cual no procederán transferencias de datos personales, salvo que operen otros mecanismos de transferencia conforme lo dispuesto en el presente capítulo.

La Autoridad de Protección de Datos Personales publicará en cualquier medio, de forma permanente y debidamente la lista de países, organizaciones, empresas o grupos económicos que garanticen niveles adecuados de protección de datos personales

Capítulo X
DE LOS REQUERIMIENTOS DIRECTOS Y DE LA GESTIÓN DEL PROCEDIMIENTO ADMINISTRATIVO

Art. 62.- Requerimiento directo del titular del dato de carácter personal al responsable del tratamiento.- El titular podrá en cualquier momento, de forma gratuita, por medios físicos o digitales puestos a su disposición por parte del responsable del tratamiento de los datos personales, presentar requerimientos, peticiones, quejas o reclamaciones directamente al responsable del tratamiento, relacionadas con el ejercicio de sus derechos, la aplicación de principios y el cumplimiento de obligaciones por parte del responsable del tratamiento., que tengan relación con él.

Presentado el requerimiento ante el responsable este contará con un término de diez (10) días para contestar afirmativa o negativamente, notificar y ejecutar lo que corresponda.

Art. 63.- Actuaciones previas.- La Autoridad de Protección de Datos Personales podrá iniciar, de oficio o a petición del titular, actuaciones previas con el fin de conocer las circunstancias de] caso concreto o la conveniencia o no de iniciar el procedimiento, para lo cual se estará conforme a las disposiciones del Código Orgánico Administrativo.

Art. 64.- Procedimiento administrativo.- En el caso de que el responsable del tratamiento no conteste el requerimiento, en el término establecido en la presente ley, o éste fuere negado, el titular podrá presentar el correspondiente reclamo administrativo ante la Autoridad de Protección de Datos Personales, para lo cual se deberá estar conforme al procedimiento establecido en el Código Orgánico Administrativo, la presente ley y demás normativa emitida por la Autoridad de Protección de Datos Personales. Sin perjuicio, el titular podrá presentar acciones civiles, penales o constitucionales de las que se crea asistido.

Capítulo XI
MEDIDAS CORRECTIVAS, INFRACCIONES Y RÉGIMEN SANCIONATORIO

Art. 65.- Medidas correctivas.- En caso de incumplimiento de las disposiciones previstas en la presente Ley, su reglamento, directrices y lineamientos y regulaciones emitidas por

la Autoridad de Protección de Datos Personales y normativas sobre la materia, o transgresión a los derechos y principios que componen al derecho a la protección de datos personales, la Autoridad de Protección de Datos Personales dictará medidas correctivas con el objeto de evitar que se siga cometiendo la infracción y que la conducta se produzca nuevamente, sin perjuicio de la aplicación de las correspondientes sanciones administrativas.

Las medidas correctivas podrán consistir, entre otras, en:

1) El cese del tratamiento, bajo determinadas condiciones o plazos;
2) La eliminación de los datos; y
3) La imposición de medidas técnicas, jurídicas, organizativas o administrativas a garantizar un tratamiento adecuado de datos personales.

La Autoridad de Protección de Datos Personales, en el marco de esta Ley, dictará, para cada caso, las medidas correctivas, previo informe de la unidad técnica competente, que permitan corregir, revertir o eliminar las conductas contrarias a la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia.

Art. 66.- Aplicación de medidas correctivas.- La Autoridad de Protección de Datos Personales, en el marco de esta ley, previo informe de la unidad técnica competente, aplicará para cada caso las medidas correctivas citadas en el artículo anterior, que permitan corregir, revertir o eliminar las conductas contrarias a la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

Para la aplicación de las medidas correctivas se seguirán las siguientes reglas:

1. En el caso de que los responsables, encargados de tratamiento de datos personales y organismos de certificación y de ser el caso, a? terceros, se encuentran incursos en el presunto cometimiento de una infracción leve y estos consten dentro del Registro Único de responsables y encargados incumplidos; la Autoridad de Protección de Datos Personales activará directamente el procedimiento administrativo sancionatorio, haciendo constar dentro de la resolución tanto las medidas correctivas aplicables como la sanción correspondiente a la infracción cometida; y,
2. En el caso de que los responsables, encargados del tratamiento de datos personales y organismos de certificación, se encuentren incursos en el presunto cometimiento de una infracción grave; la Autoridad de Protección de Datos Personales; aplicará en primera instancia medidas correctivas. Si las medidas correctivas fueren cumplidas de forma tardía, parcial o defectuosa, la Autoridad de Protección de Datos Personales, aplicará las sanciones que corresponden a las infracciones graves, activando para el efecto el procedimiento administrativo sancionatorio y haciendo constar dentro de la resolución tanto las medidas correctivas aplicables como la sanción correspondiente a la infracción cometida; y,

3. En el caso de que los responsables, encargados del tratamiento de datos personales y organismos de certificación, se encuentren incursos en el presunto cometimiento de una infracción muy grave, la Autoridad de Protección de Datos Personales activará directamente el procedimiento administrativo sancionatorio haciendo constar dentro de la resolución tanto las medidas correctivas aplicables como la sanción correspondiente a la infracción cometida.

Sección I

DE LAS INFRACCIONES DEL RESPONSABLE DE PROTECCIÓN DE DATOS

Art. 67.- Infracciones leves del Responsable de protección de datos.- Se consideran infracciones leves las siguientes:

1. No tramitar, tramitar fuera del término previsto o negar injustificadamente las peticiones o quejas realizadas por el titular;
2. No implementar protección de datos desde el diseño y por defecto;
3. No mantener disponibles políticas de protección de datos personales afines al tratamiento de datos personales;
4. Elegir un encargado del trata.mient.0 de datos personales que no ofrezca garantías suficientes para hacer efectivo el ejercicio del derecho a la protección de datos personales;
5. Incumplir las medidas correctivas dispuestas por la Autoridad de Protección de Datos Personales.

Art. 68.- Infracciones graves del Responsable de protección de datos.- Se consideran infracciones graves las siguientes:

1) No implementar medidas administrativas, técnicas y físicas, organizativas y jurídicas, a fin de garantizar el .tratamiento de datos personales que realice conforme la presente ley, su reglamento, directrices, lineamientos *y* regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia:
2) Utilizar información o datos para fines distintos a los declarados;
3) Ceder o comunica: datos personales sin cumplir con los requisitos y procedimientos establecidos en la presente ley y su reglamento, directrices lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia;
4) No utilizar metodologías de análisis y gestión de riesgos adaptadas a la naturaleza de los datos personales, las particularidades del tratamiento y de las partes involucradas;
5) No realizar evaluaciones de impacto al tratamiento de datos en los casos en que era necesario realizarlas;
6) No implementar medidas técnicas organizativas o de cualquier índole, necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones a la seguridad de datos personales que hayan sido identificadas;
7) No notificar a la Autoridad de Protección de. Datos Personales y al titular, de vulneraciones a la seguridad y protección de datos personales, cuando afecte los derechos fundamentales y libertades individuales de los titulares;

8) No notificar a la Autoridad de Protección de Datos Personales del titular las vulneraciones de seguridad y protección de datos personales, cuando exista afectación a los derechos fundamentales y libertades individuales de los titulares;
9) No suscribir contratos que incluyan cláusulas de confidencialidad y tratamiento adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales.
10) No mantener actualizado el Registro Nacional de protección de datos personales de conformidad a lo dispuesto en la presente lev su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia;
11) No consignar en el Registro Nacional de Protección de paros Personales lo dispuesto en la presente ley y su .reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia:
12) No designar al delegado de protección de datos personales cuando corresponda;
13) No permitir y no contribuir a la realización de auditorías o inspecciones por parte del auditor acreditado por la Autoridad de Protección de Datos Personales; y,
14) Incumplir las medidas correctivas o cumplir de forma tardía, parcial o defectuosa, siempre y cuando hables. precedido por dicha causa la aplicación de una sanción por infracción leve, e incurrir de forma reiterada en faltas leves.

Sección II

DE LAS INFRACCIONES DEL ENCARGADO DE PROTECCIÓN DE DATOS

Art. 69.- Infracciones leves del Encargado de protección de datos.- Se consideran infracciones leves las siguientes:

1) No colaborar con el responsable del tratamiento datos personales, para que este cumpla con su obligación de atender solicitudes que tengan por objeto el ejercicio de los derechos del titular frente al tratamiento de sus datos personales;
2) No facilitar el acceso al responsable del tratamiento de datos personales a toda la información referente al cumplimiento de las obligaciones establecidas en la presente Ley, su reglamento, directrices, lineamientos *y* regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia:
3) No permitir o no contribuir a la realización de auditorias o inspecciones, por parte del responsable del tratamiento de datos personales o de otro auditor autorizado por la Autoridad de Protección de Datos Personales; y,
4) Incumplir las medidas correctivas dispuestas por la Autoridad de Protección de Datos Personales.

Art. 70.- Infracciones graves del Encargado de protección de datos.- Se consideran infracciones graves las siguientes:

1) Realizar tratamientos de datos personales sin observar los principios y derechos desarrollados en la presente Ley y su reglamento, directrices y lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y-normativas sobre la materia;

2) No tratar datos personales de conformidad con lo previsto en el contrato que mantenga con el responsable del tratamiento de datos personales inclusive en lo que respecta a la transferencia o comunicación internacional;
3) No suscribir contratos que. contengan cláusulas de confidencialidad y tratamiento adecuado de datos personales con el personal a cargo del tratamiento de datos personales o quien tenga conocimiento de los datos personales;
4) No implementar mecanismos destinados a mantener la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales;
5) No implementar medidas preventivas y correctivas en la seguridad de los datos personales a fin de evitar vulneraciones;
6) No suprimir los datos personales transferidos o comunicados al responsable del tratamiento de los datos personales, una vez haya culminado su encargo;
7) Proceder a la comunicación de datos personales sin cumplir con los requisitos y procedimientos establecidos en la presente ley, su reglamento directrices lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia;
8) Incumplir las medidas correctivas o cumplirlas de formo, tardía parcial o defectuosa, siempre y cuando hubiese precedido por dicha causa la aplicación de una sanción por infracción leve; y.
9) No notificar al responsable del tratamiento de datos personajes sobre cualquier vulneración de la seguridad de datos personales conforme dispone esta ley o hacerlo con retraso injustificado.

Art. 71.- Sanciones por infracciones leves.- La Autoridad de Protección de Datos Personales impondrá las siguientes sanciones administrativas, en el caso de verificarse el cometimiento de una infracción leve, según las siguientes reglas:

1. Servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones leves establecidas en la presente ley, serán sancionados con una multa de uno (1) a diez (10) salarios básicos unificados del trabajador en general, sin perjuicio de la responsabilidad extracontractual del Estado, la cual se sujetará a las reglas establecidas en la normativa correspondiente;
2. Si el responsable o el encargado del tratamiento de datos personales o de ser el caso un tercero es una entidad de derecho privado o una empresa pública, se aplicará una multa de entre el 0.1% y el 0.7% calculada sobre su volumen de negocio correspondiente al ejercicio economice inmediatamente anterior al de la imposición de la multa. La Autoridad de Protección de Datos Personales establecerá la multa aplicable en función del principio de proporcionalidad, para lo cual deberá verificar los siguientes presupuestos:

a) La intencionalidad, misma que se establecerá en función a la conducta del infractor;
b) Reiteración de la infracción, es decir cuando el responsable, el encargado del tratamiento de datos personales o de ser el caso un tercero, hubiese sido previamente sancionado por dos o más infracciones precedentes, que establezcan sanciones de menor gravedad a la que se pretende aplicar; o cuando hubiesen sido previamente sancionados por una infracción cuya sanción sea de igual o mayor gravedad a la que se pretende

aplicar;
c) La naturaleza del perjuicio ocasionado, es decir, las consecuencias lesivas para el ejercicio del derecho a la protección de datos personales, y,
d) Reincidencia, es decir, cuando la infracción precedente sea de la misma naturaleza de aquella que se pretende sancionar.

Art. 72.- Sanciones por infracciones graves.- La Autoridad de Protección de Datos Personales impondrán las siguientes sanciones administrativas, en el caso de verificarse el cometimiento de una infracción grave, conforme a los presupuestos establecidos en el presente Capítulo:

Los servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones graves establecidas en la presente ley serán sancionados con una multa de entre 10 a 20 salarios básicos unificados del trabajador en general; sin perjuicio de la Responsabilidad Extracontractual del Estado, la cual se sujetará a las reglas establecidas en la normativa correspondiente;

1) Si el responsable, encargado del tratamiento de datos personales o de ser el caso un tercero, es una entidad de derecho privado o una empresa pública se aplicará una multa de entre el 0.7% y el 1% calculada sobre su volumen de negocios, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa. La Autoridad de Protección de Datos Personales establecerá la muirá aplicable en función del principio de proporcionalidad, para lo cual deberá verificar los siguientes presupuestos:

a) La intencionalidad, misma que se establecerá en función a la conducta del infractor;
b) Reiteración de la infracción, es decir, cuando el responsable, encargado del tratamiento de datos personales o de ser el caso, de un tercero hubiese sido previamente sancionado por dos o más infracciones precedentes que establezcan sanciones de menor gravedad a la que se pretende aplicar; o cuando hubiesen sido previamente sancionados por una infracción cuya sanción sea de igual o mayor gravedad a la que se pretende aplicar;
c) La naturaleza del perjuicio ocasionado, es decir, las consecuencias lesivas para el ejercicio del derecho a la protección de datos personales; y,
d) Reincidencia, es decir, cuando la infracción precedente sea de la misma naturaleza de aquella que se pretende sancionar.

En el caso de que. el responsable, encargado del tratamiento de datos personales a un tercero de ser el caso; sea una organización sin domicilio ni representación jurídica en el territorio ecuatoriano, se deberá notificar de la resolución con la cual se establezca la infracción cometida la Autoridad de Protección de Datos Personales, o quien hiciera sus veces, del lugar en donde dicha organización tiene su domicilio principal, a fin de que sea dicho organismo quien sustancia las accione? o procedimientos destinados al cumplimiento de las medidas correctivas y sanciones a las que hubiere lugar.

Art. 73.- Volumen de negocio.- A efectos del régimen sancionatorio de la presente ley, se entiende por volumen de negocio, a la cuantía resultante de la venta de productos y de la prestación de servicios realizados por operadores económicos, durante el último ejercicio

que corresponda a sus actividades, previa deducción del Impuesto al Valor Agregado y de otros impuestos directamente relacionados con la operación económica.

Art. 74.- Medidas provisionales o cautelares.- La Autoridad de Protección de Datos Personales podrá aplicar medidas provisionales de protección o medidas cautelares contempladas en la norma procedimental administrativa.

Capítulo XII
AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES

Art. 75.- Autoridad de protección de datos personales.- La Autoridad de Protección de Datos Personales podrá iniciar, de oficio o a petición del titular, actuaciones previas con el fin de conocer las circunstancias del caso concreto o la conveniencia o no de iniciar el procedimiento, para lo cual se estará conforme a las disposiciones del Código Orgánico Administrativo.

Art. 76.- Funciones atribuciones y facultades.- La Autoridad de Protección de Datos Personales es el órgano de control y vigilancia encargado de garantizar a todos los ciudadanos la protección de sus datos personales, y de realizar todas las acciones necesarias para que se respeten los principios, derechos, garantías y procedimientos previstos en la presente Ley y en su reglamento de aplicación, para lo cual le corresponde las siguientes funciones, atribuciones y facultades;

1) Ejercer la supervisión, control y evaluación de las actividades efectuadas por el responsable y encargado del tratamiento de datos personales;
2) Ejercer la potestad sancionadora respecto de responsables, delegados, encargados y terceros, conforme a lo establecido en la presente Ley;
3) Conocer, sustanciar y resolver los reclamos interpuestos por el titular o aquellos iniciados de oficio, así como aplicar las sanciones correspondientes;
4) Realizar o delegar auditorias técnicas al tratamiento de datos personales:
5) Emitir normativa general o técnica, criterios y demás actos que sean necesarios para el ejercicio de sus competencias y la garantía del ejercicio del derecho a la protección de datos personales;
6) Crear, dirigir y administrar el Registro Nacional de Protección de Datos Personales, así como coordinar las acciones necesarias con entidades del sector público y privado para su efectivo funcionamiento;
7) Promover una coordinación adecuada y eficaz con los encargados de la rendición de cuentas y participar en iniciativas internacionales y regionales para la protección de la protección de los datos personales;
8) Dictar las cláusulas estándar de protección de datos, así como verificar el contenido de las cláusulas o garantías adicionales o específicas:
9) Atender consultas en materia de protección de datos personales;
10) Ejercer el control y emitir las resoluciones de autorización para la transferencia internacional de datos;
11) Ejercer la representación internacional en materia de protección de datos personales:
12) Emitir directrices para el diseño y contenido de la política de tratamiento de datos personales;

13) Establecer directrices para el analiza evaluación y selección de medidas de seguridad de los datos personales;
14) Llevar un registro estadístico sobre vulneraciones a la seguridad de datos personales e identificar posibles medidas de seguridad para cada una de ellas:
15) Publicar periódicamente una guía de la normativa relativa a la protección de datos personales;
16) Promover e incentivar el ejercicio del derecho a la protección de datos personales, así corno la concientización en las personas y la comprensión de los riesgos, normas, garantías y derechos, en relación con el tratamiento y uso de sus datos personales, con especial énfasis en actividades dirigidas a grupos de atención prior liana tales como niñas niños y adolescentes;
17) Controlar y supervisar el ejercicio del derecho a. la protección de datos personales dentro del tratamiento de datos llevado a cabo a través del Sistema Nacional de Registros Públicos; y,
18) Las demás atribuciones establecidas en la. normativa vigente.

Art. 77.- Del titular de la Autoridad de Protección de Datos.- El Superintendente de Protección de Datos será designado de acuerdo a lo establecido en la Constitución de la República, de la terna que remita la Presidente o Presidente de la República, siguiendo criterios de especialidad y méritos se sujetará a escrutinio público y derecho de impugnación ciudadana.

El Superintendente de Protección de Datos deberá ser un profesional del Derecho, de Sistemas de Información, de Comunicación, o de Tecnologías, con título de cuarto nivel y experiencia de al menos 10 años con áreas afines a la materia objeto de regulación de esta ley.

Ejercerá sus funciones por un período de 5 años y únicamente cesará en sus funciones por las causales establecidas en la ley que regula el servicio público que le sean aplicables o por destitución, luego de enjuiciamiento político realizado por la Asamblea Nacional.

DISPOSICIONES GENERALES

Primera.- En lo dispuesto al procedimiento administrativo se estará a lo previsto en el Código Orgánico Administrativo.
Segunda.- En el ámbito del derecho de acceso a la información pública son aplicables las disposiciones de las leyes de la materia.
Tercera.- En e; ámbito de los datos personales registrables, son aplicables las disposiciones de las leyes de la materia.
Cuarta.- La Autoridad de Protección de Datos Personales será responsable de coordinar las acciones necesarias con entidades del sector publico y privado para el efectivo funcionamiento del Registre Nacional de Protección de Datos Personales.
Quinta.- La Autoridad de. Protección de Datos Personales será responsable de presentar informes anuales de evaluación y revisión de la presente Ley, a la ciudadanía.
Sexta.- Créase el Registro Único de Responsables y Encargados Incumplidos, en el cual se llevará un registro de los Responsables y Encargados del Tratamiento de Datos Personales,

que hayan incurrido en una de las infracciones establecidas en la presente Ley; mismo que tendrá fines sociales, estadísticas, preventivos y de capacitación, cuyo funcionamiento estará establecido en el Reglamento de la Ley de Protección de Datos Personales.
Séptima.- El ejercicio de los derechos reconocidos en la presente norma podrá ser exigido por el titular independientemente de la entrada en vigor del régimen sancionatenos
Octava.- Ninguna entidad pública o privada, podrá cobrar valores por servicios de entrega de información sustentada en datos del solicitante de los mismos.
Novena.- Se procurará que en lo referente a los pueblos y nacionalidades indígenas, el tratamiento de sus datos personales sea en sus idiomas y lenguas ancestrales.

DISPOSICIONES TRANSITORIAS

Primera.- Las disposiciones relacionadas con las medidas correctivas y el régimen sancionatorio entrarán en vigencia en dos años contados a partir de la publicación de esta ley en el Registro Oficial, en el transcurso de este tiempo los responsables y encargados del tratamiento, de datos personales se adecuarán a los preceptos establecidos dentro de esas disposiciones, su reglamento de aplicación y demás normativa emitida por la Autoridad de Protección de Datos Personales. El resto de disposiciones establecidas en esta ley entrarán en vigencia conforme se establece en la Disposición Final de esta Ley.
Segunda.- Todo tratamiento realizado previo a la entrada en vigencia de la presente Ley deberá adecuarse a lo previsto en la presente norma dentro del plazo de dos años contados a partir de su publicación en el Registro Oficial.

El incumplimiento de la presente disposición dará lugar a la aplicación del régimen sancionatorio establecido en esta Ley.
Tercera.- Los responsables y encargados del tratamiento de datos personales que hayan implementado los preceptos recogidos dentro de esta Ley antes de plazo señalado en la Disposición Transitoria Primera obtendrán un reconocimiento por buenas prácticas por parte de la Autoridad de Protección de Datos Personales.
Cuarta.- La transferencia internacional de datos personales que hubiere sido realizada antes de la entrada en vigencia de la presente Ley será legítima, sin perjuicio de que el responsable del tratamiento de datos personales deba aplicar lo dispuesto en esta norma para acreditar su responsabilidad proactiva y demostrada.

El responsable de tratamiento deberá adecuar la transferencia internacional de datos personales *a* la presente norma en un plazo no mayor de dos años contados a partir de la publicación de la presente norma en el Registro Oficial.

El incumplimiento de la presente disposición dará lugar a la aplicación del régimen sancionatorio establecido en esta Ley.

DISPOSICIONES REFORMATORIAS

Primera.- De la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el Suplemento del Registro Oficial 557 del 17 de abril de 2002:

1. Suprímese las definiciones de intimidad, datos personales, datos personales autorizados del glosario de términos establecido en la Disposición General Novena.
Segunda.- En la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos publicada en el suplemento del Registro Oficial 162 del 31 de marzo del 2010:

1.- Sustituyese:

a) El término Dirección Nacional de Registro de Datos Públicos por Dirección Nacional de Registros Públicos;
b) El término Sistema Nacional de Registro de Datos Públicos por Sistema Nacional de Registros Públicos;
c) El término Registro de Datos Públicos por Registros Públicos;
d) El término datos de carácter personal por datos personales;
e) El término datos públicos regístrales por la expresión datos públicos y datos personales registrables;
f) El artículo 6, por el siguiente: "**Art. 6.-** Accesibilidad y confidencialidad.- Son confidenciales los datos de carácter personal. El acceso a estos datos, solo será posible cuando quien los requiera se encuentre debidamente legitimado, conforme a los parámetros previstos en la Ley Orgánica de Protección de Datos Personales, su respectivo reglamento y demás normativa emitida por la Autoridad de Protección de Datos Personales.

Al amparo de esta Ley, para acceder a la información sobre el patrimonio de las personas cualquier solicitante deberá justificar y motivar su requerimiento, declarar el uso que hará del mismo y consignar sus datos básicos de identidad, tales como nombres y apellidos completos, número del documento de identidad o ciudadanía, dirección domiciliaria y los demás datos que mediante el respectivo reglamento se determinen. Un uso distinto al declarado dará lugar a la determinación de responsabilidades, sin perjuicio de las acciones legales que el titular de la información pueda ejercer.

La Directora o Director Nacional de Registros Públicos, definirá los demás datos que integran el sistema nacional y el tipo de reserva y accesibilidad.

2.- Incorpórase:

a) En el artículo 31 referente a las atribuciones y facultades de la Dirección Nacional de Registro Públicos antes del numeral 14 lo siguiente:

"14. Controlar y supervisar que las entidades pertenecientes al Sistema Nacional de Registros Públicos incorporen mecanismos de protección de datos personales, así como dar cumplimiento a las disposiciones establecidas en la Ley Orgánica de Protección de Datos Personales, su reglamento de aplicación y demás normativa que la Autoridad de Protección de Datos Personales dicte para el efecto:

15. Tratar datos procedentes del Sistema Nacional de Registros Públicos o de cualquier otra fuente, para realizar procesos de analítica de datos, con el objeto de prestar servicios al sector público, al sector privado y a personas en general, así como generar productos, reportes, informes o estudios, entre otros. Se utilizarán medidas adecuadas que garanticen el derecho a la protección de datos personales y su uso en todas las etapas del tratamiento, como por ejemplo, técnicas de disociación de datos, y,"

3.- Suprímese del numeral 13 del artículo 31 lo siguiente: "y";

4.- Reenumerar el numeral 14 del artículo 31 por numeral "16.;

Tercera.- En el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación publicado en el suplemento del Registro Oficial 899 del 09 de diciembre ríe 2016, sustitúyase la palabra confidencialidad por Protección en el numeral 5 del artículo 67.

Cuarta.- En la Ley Orgánica de Telecomunicaciones, publicada en el tercer suplemento del Registre Oficial 439 del 18 de febrero de 2015:

1.- Suprímase:

a) El inciso segundo, tercer y cuarto del articulo 79;
b) En el primer inciso del artículo 83 lo siguiente “(...) y seguridad de datos personales (…); y,
c) En el inciso primero del artículo 85 lo siguiente "(...) como de seguridad de datos personal (...)"

2.- Sustituyese:

a) El artículo 78 por el siguiente:

"**Art. 78.-** Seguridad de los Datos Personales.- Las y los prestadores de servicios de telecomunicaciones deberán adoptar las medidas técnicas, organizativas y de cualquier otra índole adecuadas para preservar la seguridad de su red con el fin de garantizar la protección de los datos personales de conformidad con lo establecido en la Ley Orgánica de Protección de Datos Personales."

b) El artículo 81 por el siguiente:

"**Art. 81.-** Guías telefónicas o de abonados en general.- Los abonados, clientes o usuarios tienen el derecho a no figurar en guías telefónicas o de abonados. Deberán ser informados, de conformidad con lo establecido en la Ley Orgánica de Protección de Datos Personales, de sus derechos con respecto a la utilización de sus datos personales en las guías telefónicas o de abonados y, en particular, sobre el fin o los fines de dichas guías, así como sobre el derecho que tienen, en forma gratuita, a no ser incluidos, en tales guías."

c) el artículo 82 por el siguiente:

"**Art. 82.-** Uso comercial de datos personales.- Las y los prestadores de servicios no podrán usar datos personajes, información del uso del servicio, información de tráfico o el patrón de consumo de sus abonados clientes o usuarios para la promoción comercial de servicios o productos, a menos que el abonado o usuario al que refieran los datos o tal información, haya dado su consentimiento conforme lo establecido en la Ley Orgánica de Protección de Datos Personales. Los usuarios o abonados dispondrán, de la posibilidad ciara y fácil de retirar su consentimiento para el uso de sus datos y de la información, antes indicada. Tal consentimiento deberá especificar los datos personales o información cuyo uso se autorizan, el tiempo y su objetivo específico.

Sin contar con tal consentimiento y con las mismas características, las y los prestadores de servicios de telecomunicaciones no podrán comercializar, ceder o transferir a terceros los datos personales de sus usuarios, clientes o abonados. Igual requisito se aplicará para la información del uso del servicio, información de tráfico o del patrón de consumo de sus usuarios, clientes y abonados."

d) El artículo 83 por el siguiente:

"**Art. 83.-** Control técnico.- Guando para la realización de las tareas de control técnico, ya sea para verificar el. adecuado uso del espectro radioeléctrico, la correcta prestación de los servicios de telecomunicaciones, el apropiado uso y operación de redes de telecomunicaciones o para comprobar las medidas implementadas para garantizar el secreto de las comunicaciones y seguridad de datos personales, sea necesaria la utilización de equipos, infraestructuras e instalaciones que puedan vulnerar la segundad e integridad de las redes. La Agencia de Regulación y Control de las Telecomunicaciones deberá diseñar y establecer procedimientos que reduzcan al mínimo el riesgo de afectar los contenidos de las comunicaciones.

Cuando, como consecuencia de los controles técnicos efectuados, quede constancia de los contenidos, se deberá coordinar con la Autoridad de Protección de Datos Personales para que;

a) Los soportes en los que éstos aparezcan no sean ni almacenados ni divulgados; y,
b) Los soportes sean inmediatamente destruidos y desechados

Si se evidencia un tratamiento ilegítimo o ilícito de datos personales, se aplicará lo dispuesto en la Ley Orgánica de Protección de Datos Personales."

DISPOSICIONES DEROGATORIAS

Primera.- Derogase el articulo 9 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el suplemento del Registro Oficial 557 del 17 de abril de 2002.

Segunda.- Derogase los artículos 80 y 84 de la Ley Orgánica de Telecomunicaciones, publicada en el tercer suplemento del Registro Oficial 439 del 18 de febrero de 2015.
Tercera.- Derogase el articulo 5 de la. Ley Orgánica del Sistema Nacional de Registro de Datos Públicos publicada en el suplemento del Registro Oficial 162 de 31 de marzo de 2010.
Cuarta.- Quedan así mismo derogadas todas aquellas disposiciones de igual o menor jerarquía que se contrapongan con la presente Ley Orgánica.

DISPOSICIÓN FINAL

La presente Ley entrará en vigencia una vez publicada en el Registro Oficial.

Dado y suscrito, a los diez días del mes de mayo del año dos mil veintiuno.

FUENTES DE LA PRESENTE EDICIÓN DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES

1.- Ley s/n (Quinto Suplemento del Registro Oficial 459, 26-V-2021).