BORRADOR DEL ANTEPROYECTO DE LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES

CAPÍTULO I
DISPOSICIONES DIRECTIVAS

Artículo 1.- Objeto
Artículo 2.- Finalidad
Artículo 3.- Ámbito de aplicación material
Artículo 4.- Ámbito de aplicación territorial
Artículo 5.- Ámbito de exclusión
Artículo 6.- Términos y definiciones

CAPÍTULO II
PRINCIPIOS

Artículo 7.- Principios
Artículo 8.- Legalidad, lealtad y transparencia
Artículo 9.- Legitimidad
Artículo 10.- Proporcionalidad del tratamiento
Artículo 11.- Finalidad
Artículo 12.- Pertinencia y Minimización de datos personales
Artículo 13.- Consentimiento
Artículo 14.- Confidencialidad
Artículo 15.- Calidad
Artículo 16.- Conservación
Artículo 17.- Seguridad y protección de los datos personales
Artículo 18.- Responsabilidad proactiva y demostrada
Artículo 19.- Independencia de control

CAPÍTULO III
DERECHOS

Artículo 20.- Derecho a la transparencia
Artículo 21.- Derecho de Acceso

Artículo 22.- Derecho de Rectificación y Actualización
Artículo 23.- Derecho de eliminación
Artículo 24.- Derecho de oposición
Artículo 25.- Excepciones a los derechos de eliminación y oposición
Artículo 26.- Derecho de anulación
Artículo 27.- Derecho a la portabilidad
Artículo 28.- Derecho a la limitación del tratamiento
Artículo 29.- Derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas
Artículo 30.- Derecho a la educación digital

CAPÍTULO IV
RÉGIMEN ESPECIAL DE DATOS PERSONALES

Artículo 31.- Categorías especiales de datos personales
Artículo 32.- Consentimiento
Artículo 33.- Ejercicio de derechos
Artículo 34.- Datos de personas fallecidas
Artículo 35.- Tratamiento de datos personales necesarios para el archivo de información que constituya patrimonio del Estado, investigación científica, histórica o estadística

CAPITULO V
SEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES

Artículo 36.- Seguridad y protección de datos personales
Artículo 37.- Protección de datos personales desde el diseño y por defecto
Artículo 38.- Análisis de riesgo y determinación de niveles de seguridad aplicables
Artículo 39.- Notificación de vulneración de seguridad
Artículo 40.- Notificación de vulneración de seguridad al titular
Artículo 41.- Delegado de protección de datos personales
Artículo 42.- Funciones del delegado de protección de datos personales
Artículo 43.- Códigos de conducta
Artículo 44.- Certificaciones

CAPÍTULO VI

TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

Artículo 45.- Transferencia internacional de datos personales.-
Artículo 46.- Transferencias internacionales de datos personales a países declarados como nivel adecuado de protección
Artículo 47- Criterios para determinar el nivel adecuado de protección
Artículo 48.- Transferencia mediante garantías adecuadas
Artículo 49.- Normas corporativas vinculantes
Artículo 50.- Casos excepcionales de transferencias internacionales
Artículo 51.- Control continuo

CAPITULO VII
DE LAS OBLIGACIONES

Artículo 52.- Obligaciones del responsable del tratamiento de datos o información
Artículo 53.- Obligaciones del encargado del tratamiento de datos o información

CAPITULO VIII
DEL PROCEDIMIENTO.

Artículo 54- Reclamaciones directas del titular del dato personal al responsable

CAPÍTULO IX
RÉGIMEN SANCIONATORIO

Artículo 55.- Objeto y ámbito de aplicación

Sección 1ª
Del responsable

Artículo 56.- Infracciones leves
Artículo 57.- Infracciones graves

Sección 1ª
Del encargado

BORRADOR

Artículo 58.- Infracciones leves
Artículo 59.- Infracciones graves
Artículo 60.- Sanciones por infracciones leves
Artículo 61.- Sanciones por infracciones graves
Artículo 62.- Medidas provisionales o cautelares

CAPÍTULO X
AUTORIDAD DE CONTROL

Artículo 63.- Autoridad de control
Artículo 64.- Atribuciones
Artículo 65- Registro Nacional de Protección de Datos Personales

BORRADOR

CAPÍTULO I
DISPOSICIONES DIRECTIVAS

Artículo 1.- Objeto.- El objeto de la presente Ley Orgánica es regular el ejercicio del derecho a la protección de datos personales, la autodeterminación informativa y demás derechos digitales en el flujo o circulación de información personal, a través del desarrollo de principios, derechos, obligaciones y mecanismos de tutela.

Artículo 2.- Finalidad.- La finalidad de la presente Ley Orgánica es garantizar derechos fundamentales y libertades individuales; promover el progreso económico y social; impulsar la producción nacional y la cooperación internacional; fomentar la competitividad, la innovación y productividad; elevar la eficiencia de los servicios públicos o privados; mejorar la calidad de vida; así como, contribuir al buen vivir.

Artículo 3.- Ámbito de aplicación material.- La presente Ley Orgánica se aplicará al tratamiento de datos personales contenidos en cualquier tipo de soporte, ya sean totalmente automatizados, parcialmente automatizados o no automatizados y a toda modalidad de uso posterior, por parte de responsables o encargados del tratamiento de datos o información pertenecientes a los sectores público o privado a nivel nacional.

Artículo 4.- Ámbito de aplicación territorial.- Sin perjuicio de la normativa establecida en los convenios y tratados internacionales ratificados por el Estado ecuatoriano que versen sobre esta materia se aplicará la presente Ley Orgánica cuando:

a) El tratamiento de datos personales se realice en cualquier parte del territorio nacional;
b) El responsable o encargado del tratamiento de datos o información se encuentre domiciliado en cualquier parte del territorio nacional; y,
c) El responsable o encargado del tratamiento de datos o información no domiciliado en el territorio nacional que oferte a ecuatorianos bienes o servicios, independientemente de si se requiere su pago o no, o realice actividades relativas al control de su comportamiento.

Artículo 5.- Ámbito de exclusión.- El régimen de protección de datos personales que se establece en la presente Ley Orgánica no será de aplicación para:

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 34 de la presente Ley Orgánica;
c) Datos anonimizados;
d) Fuentes de información periodística 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 y desastres naturales; y, seguridad y defensa del Estado;
f) Cuando se trate de datos personales relativos a la salud, únicamente cuando estos tengan por finalidad evitar poner en riesgo a la población, es decir, para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados;
g) Datos o bases de datos establecidos para la prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales; y,
h) Datos que identifican o hacen identificable a personas jurídicas.

Son accesibles al público y susceptibles de tratamiento los datos personales de comerciantes; representantes y socios de personas jurídicas; servidores públicos en alusión al ejercicio de su profesión, oficio, giro de negocio, competencias, facultades, atribuciones o cargo. Siempre que se trate de: nombres y apellidos; funciones o puestos desempeñados; dirección postal o electrónica; teléfono y número de fax profesionales; así como el histórico y vigente de la declaración patrimonial y de la remuneración para el caso de servidores públicos.

Artículo 6.- Términos y definiciones.- Para los efectos de la aplicación de la presente Ley Orgánica se establecen las siguientes definiciones:

Anonimización: La aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o re-identificación de una persona natural sin esfuerzos desproporcionados.

Base de datos: Conjunto configurado, estructurado o no estructurado de datos, cualquiera que fuere la forma, modalidad de creación, almacenamiento, organización, tipo de soporte, tratamiento, procesamiento y acceso.

Consentimiento informado: Manifestación de voluntad libre, previa, específica, expresa, informada e inequívoca por la que el titular de los datos personales autoriza al responsable del tratamiento de datos o información a tratar los mismos.

Dato biométrico: Dato personal único obtenido a partir de un tratamiento técnico-específico, relativo a las características físicas, fisiológicas o conductuales de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

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; generalmente se analizan a partir de muestras biológicas.

Dato personal: Toda información concerniente a una persona natural identificada o identificable, determinada o determinable, directa o indirectamente, presente o futura, incluidos fragmentos de datos, metadatos y datos inocuos. Cuando en esta Ley Orgánica se

usen los términos dato o información se entenderá que se refieren a aquellos de naturaleza personal.

Datos públicos: Toda información o datos en cualquier formato, contenidos, creados u obtenidos por instituciones públicas o sus delegatarias que se hayan producido con recursos del Estado, en el ejercicio de sus competencias.

Datos personales registrables: Datos personales, que por mandato de la Ley deben estar contenidos en Registros Públicos.

Datos sensibles: Se consideran datos sensibles a aquellos datos personales que gozan de protección reforzada, tales como los relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, estado de salud, datos biométricos, datos de geolocalización y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos humanos o la dignidad e integridad de las personas.

Destinatario: Persona natural o jurídica que ha recibido comunicación de datos personales.

Disociación de datos: Todo tratamiento de datos personales de manera que la información obtenida no pueda ser asociada o vinculada estructuralmente a una persona identificada o identificable.

Elaboración de perfiles: Todo tratamiento de datos que permite evaluar, analizar o predecir aspectos personales de una persona natural para determinar comportamientos o patrones relativos a: rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, ubicación, movimiento físico de una persona, entre otros.

Encargado del tratamiento de datos o información: Persona natural o jurídica, de Derecho público o privado, nacional o internacional que trate datos personales por nombre y a cuenta de un responsable de tratamiento de datos o información. Se considera encargado del tratamiento de datos o información también a la persona natural o jurídica, de Derecho público o privado, nacional o internacional, que dentro de su giro de negocio o para la prestación de servicios se ve inmerso en el tratamiento de datos personales, por cuenta del responsable del tratamiento de datos o información.

Estado de la técnica: Particularidad que permite establecer bases de comparación para determinar si los requisitos y herramientas de carácter administrativo, físico, técnico, organizativo y jurídico analizados son susceptibles de aplicarse en el tratamiento de datos personales.

Filtración: Acción que libera datos personales al público de manera ilegal o ilegítima.

Fuentes accesibles al público: Bases de datos que pueden ser consultadas por cualquier persona natural o jurídica, pública o privada, nacional o internacional cuyo acceso no se encuentre limitado por la normativa vigente o disposición de la autoridad de control

Responsable del tratamiento de datos o información: Persona natural o jurídica, de derecho público o privado, nacional o internacional, que solo o junto con otros, decide sobre el tratamiento de datos personales; esto es, la autenticidad, custodia, finalidad, contenido, debida conservación, uso, destino, procesamiento, entre otros.

Política de tratamiento de datos personales: Documento físico, electrónico o en cualquier formato generado por el responsable del tratamiento de datos o información que debe obligatoriamente ponerse a disposición del titular, a partir del momento en el cual se recaben sus datos personales y debe estar disponible de forma permanente, con el objeto de garantizar el derecho a la transparencia.

Titular: Persona natural a quien le conciernen los datos o información personal.

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

Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, enunciadas de forma enunciativa más no limitativa como: la recogida, obtención, recopilación, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, comunicación por transmisión, transferencia, difusión, procesamiento, almacenamiento, distribución, cesión, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales.

CAPÍTULO II
PRINCIPIOS

Artículo 7.- 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 Orgánica se regirá por los principios de legalidad, lealtad y transparencia; legitimidad; proporcionalidad del tratamiento; finalidad; pertinencia y minimización de datos personales; consentimiento; confidencialidad; calidad; conservación; seguridad y protección de los datos personales; responsabilidad proactiva y demostrada; e, independencia de control.

Artículo 8.- Legalidad, lealtad y transparencia.- Los datos personales deben tratarse con estricto apego y cumplimiento a los principios, derechos y obligaciones establecidas en la presente Ley Orgánica, su reglamento y demás normativa aplicable.

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

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

Artículo 9.- Legitimidad.- El tratamiento solo será legítimo y lícito si se cumple con alguna de las siguientes condiciones:

a) Exista obligación legal aplicable al responsable del tratamiento;
b) Por orden judicial, resolución o mandato motivado de autoridad pública competente;
c) Para el ejercicio de las competencias y facultades establecidas en la Constitución, la Ley y tratados internacionales ratificados por el Ecuador a favor de las entidades pertenecientes al sector público, sus delegatarios y organizaciones de Derecho Internacional Público;
d) Para el cumplimiento de obligaciones contractuales perseguidas por el responsable del tratamiento de datos o información, encargado del tratamiento de datos o información o por un tercero legalmente habilitado;
e) Para la ejecución de medidas precontractuales a petición del titular; siempre que no prevalezcan los intereses o los derechos y libertades de niñas, niños y adolescentes como titulares;
f) Por consentimiento del titular para el tratamiento de sus datos personales para una o varias finalidades específicas; o,
g) Para proteger intereses vitales del interesado o de otra persona natural.

Artículo 10.- Proporcionalidad del tratamiento.- El tratamiento debe ser adecuado, necesario, oportuno, relevante y no excesivo en relación a las finalidades para las cuales han sido recopilados o a la naturaleza de las categorías especiales de datos.

Solo deben tratarse los datos personales si la finalidad del tratamiento no pudiere lograrse razonablemente por otros medios.

Artículo 11.- Finalidad.- Las finalidades del tratamiento deberán ser determinadas, explícitas y legítimas, 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 el principio de legitimidad.

El posterior tratamiento de datos personales necesarios para el archivo de información que constituya patrimonio del Estado, investigación científica, histórica o estadística, que se realice en favor del interés público, no será incompatible con este principio.

Artículo 12.- Pertinencia y Minimización de datos personales.- Los datos personales deben ser adecuados, pertinentes y limitados a lo mínimo necesario para la finalidad del tratamiento.

Artículo 13.- Consentimiento.- Se podrán tratar y ceder datos personales cuando se cuente con la autorización del titular.

Se entenderá por manifestación de voluntad libre a aquella que se encuentre exenta de vicios del consentimiento; la especificidad se refiere a la determinación concreta de los medios y fines del tratamiento; informada aquella que cumple con el principio de transparencia y efectiviza el derecho de información; inequívoca a que no se presenten dudas sobre el alcance de la autorización otorgada por el titular; previa, que el consentimiento se haya dado con anterioridad al tratamiento, ya sea en el momento mismo de la recogida del dato cuando se obtiene directamente del titular y excepcionalmente de forma posterior cuando los datos personales no se obtuvieren de forma directa; expresa, que de manera indubitable, el responsable pueda demostrar que el titular manifestó su voluntad a través de una declaración o acción clara, afirmativa o se deduzca de una acción del titular.

El consentimiento podrá revocarse en cualquier momento sin que sea necesaria una justificación, para lo cual el responsable establecerá mecanismos que garanticen celeridad, eficiencia, eficacia y gratuidad.

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

Artículo 14.- Confidencialidad.- El tratamiento de datos personales debe concebirse sobre la base del debido sigilo y secreto, es decir, no deben tratarse, cederse o comunicarse para un fin distinto para el cual fueron recopilados, sin que se cuente con el consentimiento del titular, mandato de ley u orden judicial. El nivel de confidencialidad dependerá de la naturaleza del dato personal.

Este principio no implica solamente el mantenimiento de la seguridad de los datos personales, sino también la facultad del titular de controlar la forma en la que se tratan sus datos, incluyendo la transferencia o comunicación.

Artículo 15.- Calidad.- Los datos personales que sean objeto de tratamiento deben ser exactos, íntegros, precisos, completos, comprobables, claros de tal forma que no se altere su veracidad y si fuera necesario actualizados.

Artículo 16.- Conservación.- Los datos personales únicamente serán conservados durante el tiempo necesario para cumplir con la finalidad para la cual fueron recopilados, o, hasta cuando estos cumplan con el propósito para el cual fueron tratados; sin que pueda excederse de un plazo máximo de siete (7) años contados a partir de la fecha de su recopilación, salvo que la presente Ley Orgánica y demás normativa aplicable establezca un plazo distinto.

Cumplida la condición establecida en el párrafo precedente, los datos personales deberán suprimirse o ser sometidos a un proceso de anonimización, de ser el caso. Para lo cual, el

responsable implementará métodos y técnicas orientadas a eliminar, anular, borrar, hacer ilegible, destruir o dejar irreconocibles de forma definitiva y segura los datos personales.

Artículo 17.- Seguridad y protección de los datos personales.- Independientemente del tratamiento de los datos se deberán implementar requisitos y herramientas de carácter administrativo, físico, técnico, organizativo y jurídico de seguridad adecuada y necesaria con el objetivo de proteger los datos personales frente al riesgo.

Artículo 18.- Responsabilidad proactiva y demostrada.- El responsable del tratamiento de datos o información 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 Orgánica, para lo cual, además de lo establecido en la normativa aplicable, podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de auto regulación, sistemas de certificación, sellos o marcas 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 o información está obligado a rendir cuentas sobre el tratamiento de datos personales al titular y a la autoridad de control.

El responsable del tratamiento de datos o información deberá evaluar y revisar los mecanismos que adopte para cumplir con el principio de responsabilidad con el objeto de medir su nivel de eficacia en cuanto a la aplicación de la presente Ley Orgánica.

Artículo 19.- Independencia de control.- Para el efectivo ejercicio del derecho a la protección de datos personales, se deberá designar una autoridad independiente, imparcial y autónoma con amplias capacidades de regular, controlar y sancionar a los responsables del tratamiento de datos o información, ya sean personas naturales o jurídicas, de Derecho público o privado, nacional o internacional; para el efecto y aplicación de la presente Ley Orgánica, se considerará como autoridad de control a la Dirección Nacional de Registro de Datos Públicos,

CAPÍTULO III
DERECHOS

Artículo 20.- Derecho a la transparencia.- El titular de datos personales tiene derecho a ser informado de forma previa, ya sea en el momento mismo de la recogida del dato cuando se obtiene directamente del titular y excepcionalmente de forma posterior cuando los datos personales no se obtuvieren de forma directa; expresa; transparente; inteligible; concisa; precisa; sin barreras técnicas; e, inequívoca, por cualquier medio sobre:

a) Los fines del tratamiento;
b) Base legal para el tratamiento;
c) Tipos de tratamiento;
d) Tiempo de conservación;

e) La existencia de una base de datos en donde consten sus datos personales;
f) El origen de los datos personales cuando no se hayan obtenido directamente del titular;
g) Otras finalidades y tratamientos ulteriores;
h) Identidad y contactabilidad del responsable de la base de datos personales o del tratamiento, que incluye: dirección de domicilio legal, número de teléfono y correo electrónico;
i) Identidad y contactabilidad del delegado de protección de datos personales, que incluye: dirección domiciliaria, teléfono y correo electrónico;
j) Las cesiones 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 las mismas;
k) Carácter obligatorio o facultativo de la respuesta y las consecuencias de proporcionar o no sus datos personales;
l) El efecto de suministrar datos personales erróneos o inexactos;
m) La posibilidad de revocar el consentimiento;
n) La existencia y forma en que pueden hacerse efectivos sus derechos de acceso, eliminación, rectificación y actualización, oposición, anulación, portabilidad, limitación del tratamiento, a no ser objeto de una decisión basada únicamente en valoraciones automatizadas y educación digital;
o) Donde y como realizar sus reclamos ante el responsable del tratamiento de datos o información y la autoridad de control; y,
p) La existencia de valoraciones y decisiones automatizadas, incluida la elaboración de perfiles.

Con el objeto de que pueda autorizar el tratamiento, transferencia o comunicación de sus datos personales, esta información deberá ser proporcionada al titular de forma accesible por cualquier medio, incluidas políticas de protección de datos personales; gratuita; suficiente; disponible de forma permanente y redactarse en un lenguaje claro; sencillo; y, de fácil comprensión incluso cuando se trate de contratación electrónica, especialmente en el caso de niñas, niños y adolescentes.

Artículo 21.- Derecho de Acceso.- El titular tiene derecho a conocer y acceder a todos sus datos personales constantes en cualquier base de datos personales, sin necesidad de presentar justificación alguna.

El responsable del tratamiento de datos o información deberá establecer métodos razonables que permitan el acceso a dichos datos, en caso de que fuera necesario restringir dicho acceso deberán especificarse las razones concretas de dicha restricción de acuerdo a lo establecido en la normativa vigente.

Artículo 22.- Derecho de Rectificación y Actualización.- El titular tiene el derecho de solicitar se corrijan o actualicen sus datos inexactos, incompletos, desactualizados, erróneos, falsos, incorrectos o imprecisos.

Es posible que no se autorice la modificación de datos personales cuando estos se requieran legalmente o deban ser retenidos para el cumplimiento de una obligación impuesta por disposición de la ley o por relaciones contractuales entre el responsable del tratamiento de datos o información.

Artículo 23.- Derecho de eliminación.- El titular tiene derecho a solicitar la supresión de sus datos personales, a fin de que estos dejen de ser tratados por el responsable del tratamiento de datos o información, cuando:

a) El tratamiento no cumpla con los principios de legalidad, lealtad, transparencia y legitimidad;
b) El tratamiento no sea necesario o pertinente para el cumplimiento de la finalidad;
c) Los datos personales hayan cumplido con el propósito para el cual fueron recolectados y tratados;
d) Haya vencido el plazo de conservación de los datos personales;
e) El tratamiento afecte derechos fundamentales o libertades individuales; o
f) Haya revocado o no haya otorgado el consentimiento para uno o varios fines específicos, sin necesidad de que medie justificación alguna.

El responsable del tratamiento de datos o información implementará métodos y técnicas orientadas a eliminar, anular, borrar, hacer ilegible, destruir o dejar irreconocibles de forma definitiva y segura.

Artículo 24.- Derecho de oposición.- El titular tiene el derecho a oponerse o negarse al tratamiento de sus datos personales, en especial para fines de mercadotecnia, valoraciones o decisiones automatizas incluida la elaboración de perfiles.

Artículo 25.- Excepciones a los derechos de eliminación y oposición.- No proceden los derechos de eliminación y oposición, en los siguientes casos:

a) Si el solicitante no es el titular de los datos personales o su representante legal no se encuentre debidamente acreditado;
b) Para el cumplimiento de una obligación legal o contractual;
c) Para el cumplimiento de una orden judicial, resolución o mandato motivado de autoridad pública competente;
d) Para la formulación, ejercicio o defensa de reclamos o recursos;
e) Cuando se pueda causar perjuicios a derechos o afectación a intereses legítimos de terceros;
f) Cuando se pueda obstaculizar actuaciones judiciales o administrativas en curso;
g) Para ejercer el derecho a la libertad de expresión y opinión;
h) Para proteger el interés vital del interesado o de otra persona natural;
i) En los casos en que medie el interés público; o,
j) En el tratamiento de datos personales que sean necesarios para el archivo de información que constituya patrimonio del Estado, investigación científica, histórica o estadística.

Siempre y cuando no se vulneren derechos humanos reconocidos en la Constitución de la República o en Instrumentos Internacionales de derechos humanos ratificados o no por el Ecuador.

Artículo 26.- Derecho de anulación.- El titular tiene derecho a solicitar la nulidad ante la Autoridad de control por ilicitud en el acto o el tratamiento de datos personales, bajo las causales señaladas para la nulidad en materia civil, mercantil y administrativa, según sea el caso.

Artículo 27.- Derecho a la portabilidad.- El titular tiene derecho a recibir del responsable del tratamiento de datos o información, sus datos personales en un formato compatible, actualizado, estructurado, común, interoperable y mecánico; con las mismas características, mediante consentimiento para uno o varios fines específicos podrá solicitar la transmisión a otro responsable del tratamiento de datos o información, luego de lo cual procederá su supresión se cuente con el consentimiento del titular, mandato legal u orden judicial que lo impida.

Este derecho solo procederá cuando no afecte derechos y libertades de otros, ni aun cuando se refiera a un conjunto de datos personales determinado que concierna a más de un titular.

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

a) Cuando el titular haya otorgado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos, el traspaso de esta información se hará de responsable del tratamiento de datos o información a responsable del tratamiento de datos o información cuando la operación sea técnicamente posible;
b) Cuando el tratamiento se efectúe por medios automatizados;
c) Cuando se trate de un volumen relevante de información o datos personales; y,
d) Cuando el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos del responsable o encargado del tratamiento de datos o información, o del titular en el ámbito del derecho laboral y seguridad social.

Está transferencia o comunicación debe ser económica y financieramente eficiente, expedita, efectiva y sin trabas.

No procederá este derecho cuando el tratamiento sea necesario para salvaguardar el interés público, en ejercicio de poderes públicos o sea necesario para cumplir una obligación legal aplicable al responsable del tratamiento de datos o información; o, 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 o información 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.

Artículo 28.- Derecho a la limitación del tratamiento.- El titular tendrá derecho a que se use el mínimo de sus datos personales en el tratamiento efectuado por responsables o encargados del tratamiento datos o información; a que sus datos personales no se encuentren disponibles en internet u otros medios de comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido a los titulares o a los autorizados por razones de interés público; a que el tratamiento de datos personales se limite al período que medie entre una solicitud de revisión de legalidad, lealtad, transparencia, legitimidad, acceso, eliminación, rectificación y actualización, oposición, anulación, portabilidad, limitación del tratamiento, a no ser objeto de una decisión basada únicamente en valoraciones automatizadas; hasta su resolución por el responsable o encargado del tratamiento de datos o información; así mismo tendrá derecho a la limitación de sus datos personales cuando estos sean innecesarios para el responsable o encargado del tratamiento de datos o información, pero los necesite para formular un reclamo.

Artículo 29.- Derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas.- El titular tiene derecho a no soportar valoraciones que sean producto de procesos automatizados, incluida la elaboración de perfiles, que produzcan efectos jurídicos en él o que atenten contra sus derechos y libertades fundamentales, para lo cual podrá:

a) Solicitar una explicación motivada sobre la decisión tomada por el responsable o encargado del tratamiento de datos o información;
b) Exponer su punto de vista;
c) Conocer los criterios de valoración sobre el programa automatizado; y/o,
d) Impugnar la decisión.

No se aplicará este derecho cuando la decisión es necesaria para la celebración o ejecución de un contrato entre el titular y el responsable o encargado del tratamiento de datos o información; o cuando está autorizada por la normativa aplicable, orden judicial, resolución o mandato motivado de autoridad pública competente, para lo cual se deberá establecer medidas adecuadas para salvaguardar los derechos fundamentales y libertades del titular; o se base en el consentimiento del titular.

Artículo 30.- Derecho a la educación digital.- Las personas tienen derecho al acceso y disponibilidad del conocimiento, aprendizaje, preparación, estudio, formación, capacitación, enseñanza e instrucción relacionados al uso y manejo 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.

Las entidades educativas deberán potenciar el enfoque de derechos antes mencionados de manera transversal en el currículo nacional en todos los niveles educativos. Se deberán emprender proyectos orientados a la prevención de situaciones de riesgo derivadas de la

inadecuada utilización de las tecnologías de la información y comunicación, con especial atención a las situaciones de violencia en la red.

El cuerpo docente deberá ser formado y capacitado en competencias digitales para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior.

Los planes de estudio de los títulos universitarios, en especial aquellos que habiliten el desempeño profesional, en especial para la formación de niñas, niños y adolescentes, garantizarán el conocimiento en el uso y seguridad de los medios digitales y en el efectivo ejercicio de los derechos fundamentales en Internet.

CAPÍTULO IV
RÉGIMEN ESPECIAL DE DATOS PERSONALES

Artículo 31.- Categorías especiales de datos personales.- Para el tratamiento de datos sensibles, datos de niñas, niños y adolescentes, datos crediticios y datos necesarios para el archivo de información que constituya patrimonio del Estado, investigación científica, histórica o estadística, se aplicará lo dispuesto en el presente capítulo.

Artículo 32.- Consentimiento.- Además de los requisitos del consentimiento previstos en el artículo 13, se requiere de la manifestación de la voluntad explícita del titular para el tratamiento de datos sensibles, datos crediticios y de datos personales de adolescentes entre 16 a 18 años.

Para el caso de adolescentes entre 12 y 16 años, así como de niñas y niños es necesario contar con el consentimiento explícito de su representante legal.

Se entiende por consentimiento explícito a aquel que de manera indubitable, el responsable o encargado del tratamiento de datos o información, pueda demostrar que el titular otorgó su autorización a través de una declaración o acción clara y afirmativa.

El titular puede ejercer su derecho a la autodeterminación informativa aunque ya no sea niña, niño o adolescente.

El responsable o encargado del tratamiento de datos o información, deberá informar al titular o al representante legal, del carácter facultativo de sus respuestas, consecuencias y los derechos que le asisten, respecto de datos sensibles y de datos de niñas, niños y adolescentes.

El responsable o encargado del tratamiento de datos o información está en obligación de verificar si el representante legal ha otorgado su consentimiento explícito para el tratamiento de datos sensibles, datos crediticios y en especial, datos de niñas, niños y adolescentes.

No se podrán tratar datos sensibles o datos de niñas, niños y adolescentes, en lo referente al artículo 29 inciso final, a menos que se cuente con autorización explícita del titular o para salvaguardar el interés público.

Artículo 33.- 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 relacionada al uso y tratamiento responsable, adecuado y seguro de datos personales de niñas, niños y adolescentes, tanto a sus titulares como a sus representantes legales.

Los adolescentes de entre 12 y 16 años, así como las niñas y niños, para el ejercicio de sus derechos necesitarán de su representante legal. Los adolescentes de entre 16 a 18 años, podrán ejercitarlos de forma directa ante la Autoridad de control o ante el responsable de la base de datos personales y del tratamiento.

Artículo 34.- Datos de personas fallecidas.- Los titulares de derechos sucesorios del fallecido podrán dirigirse al responsable de la base de datos personales o del tratamiento con el objeto de solicitar el acceso, rectificación o eliminación de los datos personales del causante.

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

En caso de fallecimiento de niñas, niños, adolescentes o personas con discapacidad, estas facultades podrán ejercerse también por sus representantes legales.

Artículo 35.- Tratamiento de datos personales necesarios para el archivo de información que constituya patrimonio del Estado, investigación científica, histórica o estadística.- Para el tratamiento de datos personales necesarios para el archivo de información que constituya patrimonio del Estado catalogados como tal por la ley de la materia; la investigación científica; histórica; o, estadística se atenderá a lo previsto a la normativa aplicable, y subsidiariamente a lo previsto en la presente Ley Orgánica y su Reglamento.

CAPITULO V
SEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES

Artículo 36.- Seguridad y protección de datos personales.- El responsable o encargado del tratamiento de datos o información, según sea el caso, deberá sujetarse al principio de seguridad y protección de datos personales, conforme lo dispuesto en el artículo 17 de la presente Ley Orgánica; para lo cual deberá tomar en cuenta el estado de la técnica, mejores prácticas de la industria en seguridad y protección de datos personales y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento de datos,

así como identificar la probabilidad de riesgos y el nivel de impacto de estos que puedan afectar los derechos fundamentales y libertades individuales.

El responsable o encargado del tratamiento de datos o información, deberá implementar un proceso de verificación, evaluación y valoración periódica de la eficiencia, eficacia y efectividad de los requisitos implementados y herramientas de carácter administrativo, físico, técnico, organizativo y jurídico para garantizar la seguridad del tratamiento de datos o información.

El responsable o encargado del tratamiento de datos o información deberá garantizar que los requisitos y herramientas adoptadas para la mitigación de riesgos establezcan un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

La anonimización, encriptación, cifrado o codificación de datos personales;

La capacidad de garantizar la confidencialidad, integridad, disponibilidad permanentes de los sistemas y servicios del tratamiento de datos o información y el acceso a los datos personales, de forma rápida en caso de incidente físico o técnico; y,

La capacidad de garantizar la resiliencia técnica, física, administrativa, organizativa, y jurídica.

La demostración de los requisitos y herramientas previamente referidos se podrá acreditar a través de la adhesión a un código de conducta o mecanismos de certificación.

Los responsables y encargados del tratamiento de datos o información, podrán acogerse a estándares internacionales para medición y gestión de riesgos, 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 control .

Artículo 37.- Protección de datos personales desde el diseño y por defecto.- El responsable del tratamiento de datos o información implementará los requisitos y herramientas administrativas, físicas, técnicas, organizativas y jurídicas apropiadas con miras a garantizar que, desde el diseño y por defecto, solo sean objeto de tratamiento los datos personales, que sean necesarios para cada una de las finalidades.

Está obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales requisitos y herramientas garantizarán en particular que, desde el diseño y por defecto, los datos personales no sean accesibles sin la intervención de la persona, a un número indeterminado de personas naturales.

Artículo 38.- Análisis de riesgo y determinación de niveles de seguridad aplicables.- Para el análisis de riesgos, el responsable y el encargado del tratamiento de datos o información deberá utilizar una metodología de análisis y gestión de riesgos, adaptada a las particularidades del tratamiento y de las partes involucradas.

Para determinar el nivel de seguridad aplicable, se deberán tomar en cuenta los resultados del análisis de riesgos que presente el tratamiento, la naturaleza de los datos personales y las características de las partes involucradas; en particular, como consecuencia de la

destrucción, pérdida o alteración, accidental o ilícita, de datos personales, la transferencia o comunicación o acceso no autorizados a dichos datos.

Previo al tratamiento de datos personales, el responsable o el encargado del tratamiento de datos o información deberá tomar las medidas técnicas, físicas, administrativas, organizacionales, y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulnerabilidades identificadas.

Artículo 39.- Notificación de vulneración de seguridad.- En caso de violación a las seguridades implementadas y establecidas o de filtración de datos personales el responsable del tratamiento de datos o información deberá notificar a la Autoridad de control hasta 72 horas después de tener constancia de ella.

El encargado deberá notificar al responsable del tratamiento de datos o información la violación a las seguridades establecidas o de filtración de datos personales en un plazo no mayor a 24 horas después de tener constancia de ella.

En caso de retraso del responsable o del encargado del tratamiento de datos o información en la notificación de vulneración de seguridad sin que intermedie la debida justificación, se aplicarán las sanciones correspondientes conforme a lo establecido en la presente Ley Orgánica, su Reglamento y demás normativa aplicable.

Artículo 40.- Notificación de vulneración de seguridad al titular.- Si de las consecuencias de la violación o filtración de datos personales se determina un riesgo a los derechos de su titular, el responsable del tratamiento deberá notificar al titular de los datos personales dentro del mismo plazo de notificación a la Autoridad de control.

No se deberá notificar al titular si se cumple alguna de las siguientes condiciones:

El responsable o encargado del tratamiento de datos o información ha adoptado requisitos y herramientas de protección técnicas, físicas, administrativas, organizativas y jurídicas apropiadas;

El responsable o encargado del tratamiento de datos o información, ha adoptado medidas que garanticen que no exista la probabilidad de que se materialice el riesgo para el derecho del titular; y,

Suponga un esfuerzo desproporcionado, en este supuesto se emitirá una comunicación pública o una medida análoga que garantice el conocimiento de la vulneración por parte del titular o titulares.

Artículo 41.- Delegado de protección de datos personales.- El responsable y encargado del tratamiento de datos o información designarán un delegado de protección de datos personales cuando:

a) El tratamiento se lleve a cabo por una entidad del sector público;
b) Las actividades del responsable o encargado de tratamiento de datos o información requieran de un control permanente y sistematizado debido a la naturaleza, alcance y/o finalidades del tratamiento;
c) El tratamiento se refiera a categorías especiales de datos, de acuerdo a lo establecido en el Capítulo IV de la presente Ley; y,
d) El tratamiento se refiera a datos relacionados con la seguridad y defensa del Estado.

Artículo 42.- Funciones del delegado de protección de datos personales.- El delegado de protección de datos personales tendrá, entre otras, las siguientes funciones y atribuciones:

a) Informar y asesorar al responsable y encargado del tratamiento de datos o información así como al personal relacionado al tratamiento de datos personales, respecto a las disposiciones contenidas en esta Ley Orgánica, su Reglamento y en la demás normativa aplicable;
b) Supervisar el cumplimiento de las disposiciones contenidas en esta Ley Orgánica, su Reglamento y en la demás normativa aplicable;
c) Asesorar en el análisis de riesgo y evaluación de nivel de seguridad; y,
d) Cooperar con la Autoridad de control y actuar como punto de contacto con dicha entidad en relación a las cuestiones referentes al tratamiento de datos o información.

En caso de incumplimiento de sus funciones, responderá administrativa, civil y penalmente.

Artículo 43.- Códigos de conducta.- La Autoridad de control, aprobará los códigos de conducta que deberán ser presentados e implementados por los responsables y encargados del tratamiento de datos o información, para lo cual se deberá tomar en cuenta las necesidades específicas de los sectores en los que se efectúe tratamiento de datos personales.

La autoridad de control, supervisará y controlará la implementación de los códigos de conducta y su cumplimiento.

Artículo 44.- Certificaciones.- La Autoridad de control, autorizará el funcionamiento de entidades certificadoras para la emisión de sellos o marcas de protección de datos personales y elaborará el modelo de gestión para dicha finalidad.

CAPÍTULO VI
TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

Artículo 45.- Transferencia internacional de datos personales.- La transferencia internacional de datos personales será posible si se sujeta a lo previsto en el presente capítulo propendiendo siempre el efectivo ejercicio del derecho a la protección de datos personales.

En dichas transferencias o incluso cuando existan posteriores, tanto el responsable como el encargado del tratamiento de datos o información deberán regirse a las condiciones detalladas en la presente Ley o la normativa especializada en la materia.

Artículo 46.- Transferencias internacionales de datos personales a países declarados como nivel adecuado de protección.- Por principio general se podrán transferir datos personales a países, organizaciones o territorios económicos que brinden niveles adecuados de protección.

Artículo 47- Criterios para determinar el nivel adecuado de protección.- Para declarar de nivel adecuado a países, organizaciones o territorios económicos internacionales, la autoridad de control emitirá resolución motivada respecto a si un país, organización o territorio económico internacional garantiza un nivel de adecuado de protección, en la cual se verificará la existencia de los siguientes presupuestos:

a) Normativa que promueva y garantice el ejercicio de derechos fundamentales y libertades individuales;
b) Autoridad de control independiente;
c) La existencia de normativa especial de protección de datos personales, así como el funcionamiento efectivo de una autoridad estatal independiente que garantice y promueva la efectiva tutela del derecho a la protección de datos personales.
d) Acuerdos o instrumentos internacionales vinculantes ratificados por un tercer país, organización o territorio económico que generen obligaciones respecto al tratamiento y trasferencia de datos personales, siempre que estos establezcan un estándar igual o mayor a la normativa ecuatoriana vigente, en favor del titular más allá de su origen o nacionalidad.
e) Legislación específica en materia seguridad nacional y defensa del Estado. Será analizado también el nivel de acceso de las autoridades públicas a los datos personales de sus ciudadanos.

La resolución de nivel adecuado de protección deberá contemplar mecanismos de revisión periódica, al menos cada cinco años, para garantizar el derecho a la protección de datos personales de los ecuatorianos. 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 o territorios económicos internacionales.

Artículo 48.- Transferencia mediante garantías adecuadas.- Este mecanismo de transferencia transfronteriza de datos opera cuando no existe una resolución de nivel adecuado, en su lugar el responsable o encargado ha tomado medidas para compensar la falta de protección de datos en un tercer país, organización o territorio económico internacional mediante garantías adecuadas para el titular, como:

f) Observancia de principios, derechos y obligaciones en el tratamiento de datos personales siempre que estos cumplan con un estándar igual o mayor a la normativa ecuatoriana vigente.

a) Efectiva tutela del derecho a la protección de datos personales, a través de la disponibilidad permanente de acciones administrativas o judiciales.
b) El derecho a solicitar la reparación integral, de ser el caso.

Para la consecución de este mecanismo se requiere de un instrumento jurídico vinculante y exigible entre autoridades y responsables del tratamiento de datos o información como: normas corporativas vinculantes, clausulas tipo de protección de datos, clausulas o garantías adicionales, códigos de conducta aprobados o mecanismos de certificación, sellos o marcas de protección de datos personales.

Artículo 49.- Normas corporativas vinculantes.- Los responsables o encargados del tratamiento de datos o información podrán presentar a la Autoridad de control normas corporativas vinculantes, específicas y aplicadas al ámbito de su actividad, en las cuales, para su aprobación, deberán cumplir las siguientes condiciones:

a) Deberán ser de obligatorio cumplimiento para la empresa signataria, la totalidad del grupo empresarial al que esta pertenezca, sus empresas asociadas y cualquier otra empresa a la que eventualmente transfieran datos personales, incluidos sus empleados que pudiesen tener acceso a los mismos;
b) Deberán brindar a los titulares los derechos exigibles por el tratamiento de sus datos personales, observando y manteniendo la compatibilidad con todo el articulado de esta Ley.
c) Deberán incluir una enunciación detallada de las empresas filiales que, además de la signataria, pertenecen al mismo grupo empresarial. La estructura y los datos de contacto del grupo empresarial o joint venture dedicadas a una actividad económica conjunta y de cada uno de sus miembros;
d) Incluir el detalle de las empresas encargadas del tratamiento de datos o información, las categorías de datos personales a ser utilizados, así como el tipo de tratamiento a realizarse y su finalidad;
e) Enunciar de forma expresa el carácter jurídicamente vinculante de tales normas a nivel nacional e internacional;
f) Deberá observar en su contenido todas las disposiciones de la presente ley referentes a principios de tratamiento de datos personales, mediadas de seguridad de datos, requisitos respecto a transferencias internacionales, conforme a los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes;
g) Deberá contener los derechos del titular en relación con el tratamiento de sus datos y mecanismos efectivos para ejercerlos directamente frente al responsable del tratamiento de datos o información, o a presentar reclamaciones ante la autoridad de control competente y de ser procedente, el derecho a una indemnización por violación de las normas corporativas vinculantes;
h) Deberá contener la aceptación por parte del responsable o del encargado del tratamiento de los datos o información por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de su grupo empresarial. El responsable o encargado del tratamiento de datos o información no será responsable si éste demuestra que el acto que originó los daños y perjuicios no le es imputable.

i) Incluir los mecanismos en que se facilita al titular la información clara y completa, respecto a las normas corporativas vinculantes y sus efectos jurídicos;
j) Incluir las funciones de todo delegado de protección de datos designado o 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;
k) Detallarlos procedimientos de reclamación previos o en vía administrativa o judiciales;
l) Enunciar de forma detallada los mecanismos establecidos en el grupo empresarial o empresas afiliadas que permitan al titular verificar efectivamente del cumplimiento de las normas corporativas vinculantes. Entre estos mecanismos se incluirá auditorías continuas de protección de datos y aquellos métodos técnicos que brinden acciones correctivas para proteger los derechos del titular. Los resultados de las auditorias deberán ser publicados y de acceso público, así mismo, se pondrán a disposición de la Autoridad de control ;
m) Incluir los mecanismos para cooperar de forma coordinada con la Autoridad de control y el responsable del tratamiento de los datos o información; e,
n) Incluir la declaración y compromiso del responsable del tratamiento de los datos o información de promover la protección de datos personales entre sus empleados con formación continua.

La Autoridad de control podrá definir el formato y los procedimientos para la transmisión 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 previamente aprobado por la Autoridad de control y deberá notificarse posteriormente a los interesados inmersos. Se deberá establecer claramente los mecanismos a ser utilizados para tales notificaciones.

Artículo 50.- Casos excepcionales de transferencias internacionales.- En aquellos casos donde no se apliquen los artículos 46 y 47, la Autoridad de control podrá autorizar transferencias internacionales de datos personales:

a) A países, organizaciones o territorios económicos internacionales que brinden garantías adecuadas para la protección de datos de sus ciudadanos sin que necesariamente exista una ley específica o autoridad de control. En estos casos será necesaria la suscripción de un instrumento jurídicamente vinculante entre las partes que promueva la protección de datos personales por ser compatible con los preceptos de esta Ley;
b) A las empresas o grupos económicos que implementen normas corporativas vinculantes de conformidad con el artículo 47; en estos casos se nombrará como ente de control a la Autoridad de control y se aplicará en casos de controversias la normativa ecuatoriana. Las empresas deberán nombrar a un representante o Agente

en el Ecuador para que los titulares de los datos puedan hacer exigibles sus derechos;

c) A países, organizaciones, territorios económicos o empresas que hayan sido certificadas como nivel adecuado mediante mecanismos compatibles con la normativa ecuatoriana, en estos casos se exigirá a los responsables o encargados del tratamiento de datos o información las respectivas garantías de los derechos de los interesados en casos de transferencias ulteriores de datos a otros territorios;
d) Cuando el titular haya otorgado su consentimiento explícito a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias, debido a la ausencia de una resolución de nivel adecuado de protección y de garantías adecuadas;
e) Cuando la transferencia internacional de datos personales sea necesaria para la ejecución de una obligación contractual entre el titular y el responsable del tratamiento de datos o información, o para la ejecución de medidas de carácter precontractual adoptadas a solicitud del titular;
f) Cuando la transferencia internacional de datos personales sea necesaria para la celebración o ejecución de un contrato, en interés del titular entre el responsable del tratamiento de datos o información y otra persona natural o jurídica;
g) Cuando la transferencia sea necesaria por razones de interés público;
h) Cuando la transferencia internacional sea necesaria para la colaboración judicial internacional;
i) Transferencias bancarias y bursátiles.
j) 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,
k) 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.

Artículo 51.- Control continuo.- La autoridad de control 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, organizaciones o territorios económicos internacionales que ostenten tal reconocimiento.

En caso de detectarse que un país, organización o territorio económico internacional ya no cumple con un nivel de adecuado de protección conforme los principios, derechos y obligaciones desarrollados de la presente ley, la Autoridad de control procederá a emitir la correspondiente resolución de no adecuación, fecha a partir de la cual no proceden transferencias de datos personales salvo que opere otros mecanismos de transferencia conforme lo dispuesto en el presente capítulo.

La autoridad de control publicará periódicamente en su página web, una lista de países, organizaciones, territorios económicos internacionales, empresas o grupos económicos que garanticen niveles adecuados de protección de datos personales.

CAPITULO VII
DE LAS OBLIGACIONES

Artículo 52.- Obligaciones del responsable del tratamiento de datos o información.- El responsable del tratamiento está obligado a:

1. Tratar datos personales en estricto apego a los principios y derechos desarrollados en esta ley, en el reglamento y en directrices, lineamientos y regulaciones emitidas por la Autoridad de control , o normativa que verse 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 datos o información se ha realizado conforme a los previsto en la presente Ley y en la normativa especializada en la materia;
3. Aplicar e implementar procesos de verificación, evaluación y 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 o información en cada caso en particular;
5. Adherirse a códigos de conducta, o a mecanismos de certificación, sellos o marcas de protección de datos personales aprobados por la Autoridad de control ;
6. Utilizar metodologías de análisis y gestión de riesgos adaptadas a las particularidades del tratamiento y de las partes involucradas;
7. Realizar evaluaciones de adecuación al nivel de seguridad previas al tratamiento de datos o información.
8. Tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas;
9. Notificar a la Autoridad de control y al titular de violaciones a las seguridades implementadas para el tratamiento de datos e información conforme en lo establecido al procedimiento establecido para el efecto;
10. Implementar la protección de datos desde el diseño y por defecto;
11. Suscribir contratos de confidencialidad y manejo adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos o información o que tenga conocimiento de los datos personales;
12. Elegir y designar el encargado del tratamiento de datos o información que ofrezca garantías suficientes para garantizar el derecho a la protección de datos personales conforme lo establecido en esta ley, la normativa especializada en la materia y las mejores prácticas a nivel nacional o internacional.
13. Registrar y mantener actualizado el Registro Nacional de Protección de Datos Personales de conformidad a lo dispuesto en la normativa especializada;
14. Designar al Delegado a la Protección de Datos Personales; y,
15. Los demás establecidos en la presente Ley y normativa especializada.

Artículo 53.- Obligaciones del encargado del tratamiento de datos o información.- El encargado del tratamiento de datos o información está obligado a:

a) Tratar datos personales en estricto apego a los principios y derechos desarrollados en esta ley, en el reglamento y en directrices, lineamientos y regulaciones emitidas por la Autoridad de control , o normativa que verse sobre la materia;
b) Tratar datos personales únicamente siguiendo lo previsto en el contrato que mantenga con el responsable del tratamiento de datos o información , inclusive en lo que respecta a la transferencia internacional de datos, salvo que esté obligado a hacerlo bajo obligación legal u orden judicial, de ser este el caso deberá informar al responsable del tratamiento de datos o información;
c) Suscribir contratos de confidencialidad y manejo adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos o información, o que tenga conocimiento de los datos personales;
d) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales;
e) Implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales a efecto de evitar vulneraciones;
f) Asistir al responsable para que éste 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;
g) Asistir al responsable a garantizar el cumplimiento de las obligaciones previstas en esta ley y en la normativa especializada en la materia;
h) Devolver y suprimir los datos personales entregados al responsable del tratamiento de los datos o información una vez haya culminado su encargo;
i) Facilitar el acceso al responsable del tratamiento de datos o información de toda la información referente al cumplimiento de las obligaciones establecidas en la presente ley y normativa especializada en la materia;
j) Permitir y contribuir a la realización de auditorías incluidas inspecciones, por parte del responsable del tratamiento de datos o información o de otro auditor autorizado por éste;
k) Cumplir el código de conducta o a un mecanismo de certificación, sellos o marcos aprobado para demostrar la existencia de garantías suficientes para la protección de datos personales; y,
l) Los demás establecidos en la presente Ley y normativa especializada.

CAPITULO VIII
DEL PROCEDIMIENTO.

Artículo 54- Reclamaciones directas del titular del dato personal al responsable.- El titular de los datos personales podrá, en cualquier momento, de forma gratuita y por medios digitales puestos a su disposición por parte del responsable del tratamiento de los datos o información presentar reclamaciones sobre el contenido de los derechos, principios y obligaciones para hacer efectiva de forma directa sus peticiones, en especial aquellas relacionadas al acceso, rectificación, supresión, oposición, limitaciones al tratamiento,

portabilidad, notificaciones sobre violaciones a la seguridad, transferencia internacional a terceros países.

Presentada la reclamación ante el responsable, este contará con un plazo de cinco días para contestar y notificar en debida forma sobre su respuesta afirmativa o negativa, y ejecutar lo que se le haya solicitado. En el caso de que el responsable no dé contestación en el plazo señalado o esta sea negativa, el titular podrá iniciar las acciones administrativas previstas en el Código Orgánico Administrativo, acogiéndose a los procedimientos y plazos previstos en él; así como podrá presentar acciones civiles, penales incluida la constitucional de *habeas data* de las que se crea asistido.

CAPÍTULO IX
RÉGIMEN SANCIONATORIO

Artículo 55.- Objeto y ámbito de aplicación.- Los responsables o encargados del tratamiento de datos o información están sujetos al régimen sancionatorio establecido en el presente Capítulo.

La Resolución a través de la cual se imponga un sanción derivada del incumplimiento de las obligaciones establecidas en la presente Ley, deberán incluir las medidas que se deberán adoptadas para cesar o corregir los efectos de la infracción cometida.

En el caso de entidades pertenecientes al sector público, dicha resolución deberá ser comunicada a la máxima autoridad de la institución responsable del tratamiento de datos o información con la finalidad de que se inicien los procedimientos sancionatorios correspondientes conforme lo determinado en la ley pertinente.

Sección 1ª

Del responsable

Artículo 56.- Infracciones leves.- Se consideran infracciones leves las siguientes:

a) No tramitar y resolver de manera injustificada las peticiones o reclamos realizados por el titular.
b) No notificar a la autoridad de control y al titular las vulneraciones a la seguridad y protección de datos personales cuando no exista afectación a los derechos fundamentales y libertades individuales de los titulares;
c) No mantener disponible políticas de protección de datos personales afines al tratamiento de datos o información;
d) No mantener actualizado el Registro Nacional de Protección de Datos Personales de conformidad a lo dispuesto en el reglamento a la presente ley y demás normativa especializada

Artículo 57.- Infracciones graves.- Se consideran infracciones graves las siguientes:

a) No aplicar e implementar requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas a fin de garantizar que el tratamiento de datos o información se realice conforme la presente ley, su respectivo reglamento y normativa especializada;
b) Utilizar información o datos para fines distintos a los declarados.
c) No implementar políticas de protección de datos personales afines al tratamiento de datos o información;
d) Reincidir en no mantener disponible políticas de protección de datos personales;
e) No cumplir lo dispuesto en códigos de conducta aprobados por la Autoridad de control ;
f) Proceder a la comunicación de datos personales, sin cumplir con los requisitos y procedimientos establecidos en la presente Ley, su reglamento y normativa especializada;
g) 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;
h) No implementar requisitos y herramientas administrativas, técnicas, físicas, organizativas, y jurídicas necesarios para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas;
i) No realizar evaluaciones de adecuación al nivel de seguridad previas al tratamiento de datos o información;
j) No notificar a la Autoridad de control y al titular las vulneraciones a la seguridad y protección de datos personales cuando afecta los derechos fundamentales y libertades individuales de los titulares;
k) No implementar protección de datos desde el diseño y por defecto;
l) No suscribir contratos de confidencialidad y manejo adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos o información o que tenga conocimiento de los datos personales;
m) Elegir al encargado del tratamiento de datos o información que no ofrezca garantías suficientes para hacer efectivo el ejercicio del derecho a la protección de datos personales;
n) No registrar el Registro Nacional de Protección de Datos Personales de conformidad a lo dispuesto en el reglamento a la presente ley y demás normativa especializada;
o) Reincidir en no mantener actualizado el Registro Nacional de Protección de Datos Personales de conformidad a lo dispuesto en el reglamento a la presente ley y demás normativa especializada;
p) No designar al Delegado de Protección de Datos Personales; e,
q) Incumplir con las normas de seguridad establecidas por la Autoridad de control para el mantenimiento de bases de datos.

Sección 1ª

Del encargado

Artículo 58.- Infracciones leves.- Se consideran infracciones leves las siguientes:

a) No asistir al responsable para que éste 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;
b) No facilitar el acceso al responsable del tratamiento de datos o información a toda la información referente al cumplimiento de las obligaciones establecidas en la presente ley y normativa especializada en la materia;
c) No permitir y contribuir a la realización de auditorías incluidas inspecciones, por parte del responsable del tratamiento de datos o información o de otro auditor autorizado por éste;

Artículo 59.- Infracciones graves.- Se consideran infracciones graves las siguientes:

d) No tratar datos personales en estricto apego a los principios y derechos desarrollados en esta ley, en el reglamento y en directrices, lineamientos y regulaciones emitidas por la Autoridad de control , o normativa que verse sobre la materia;
e) No tratar datos personales de conformidad con lo previsto en el contrato que mantenga con el responsable del tratamiento de datos o información , inclusive en lo que respecta a la transferencia internacional;
f) No suscribir contratos de confidencialidad y manejo adecuado de datos personales con el personal a cargo del tratamiento de datos o información, o que tenga conocimiento de los datos personales;
g) No garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales;
h) No implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad al tratamiento de los datos personales a efecto de evitar vulneraciones;
i) Reincidir en no asistir al responsable para que éste 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;
j) Reincidir en no facilitar el acceso al responsable del tratamiento de datos o información a toda la información referente al cumplimiento de las obligaciones establecidas en la presente ley y normativa especializada en la materia;
k) Reincidir en no permitir y contribuir a la realización de auditorías incluidas inspecciones, por parte del responsable del tratamiento de datos o información o de otro auditor autorizado por éste;
l) No suprimir los datos personales entregados al responsable del tratamiento de los datos o información una vez haya culminado su encargo;
m) Incumplir el código de conducta aprobados por la Autoridad de control ; y,
n) Los demás establecidos en la presente Ley y normativa especializada.

Artículo 60.- Sanciones por infracciones leves.- La Autoridad de control impondrá las siguientes sanciones administrativas en el caso de verificarse el cometimiento de una infracción leve conforme a los presupuestos establecidos en el presente Capítulo:

1. Si el responsable o encargado del tratamiento de los datos o información es una entidad perteneciente al sector público se aplicarán las siguientes sanciones:

    a) Una multa equivalente al cinco por ciento de la doceava parte del presupuesto anual de la institución; o,
    b) En caso reincidencia se aplicará una multa del diez por ciento de la doceava parte de su presupuesto anual de la institución.

2. Si el responsable o encargado del tratamiento de datos o información es un entidad de derecho privado se aplicarán las siguientes sanciones:

    a) Con una multa de entre 0,03 y 0,04 calculada sobre el total de ingresos del responsable de tratamiento de datos personales correspondientes a su última declaración de impuesto a la renta o facturación anual; o,
    b) En caso de reincidencia, con sanción pecuniaria de entre 0,05 y 0,06 calculada sobre el total de ingresos del responsable de tratamiento de datos personales correspondientes a su última declaración de Impuesto a la Renta.

Artículo 61.- Sanciones por infracciones graves.- La autoridad de control impondrá las siguientes sanciones administrativas en el caso de verificarse el cometimiento de una infracción grave conforme a los presupuestos establecidos en el presente Capítulo:

1. Si el responsable o encargado del tratamiento de los datos o información es una entidad perteneciente al sector público se aplicarán las siguientes sanciones:

    a) Una multa equivalente al veinte por ciento de la doceava parte del presupuesto anual de la institución; o,
    b) En caso reincidencia se aplicará una multa del cuarenta por ciento de la doceava parte de su presupuesto anual de la institución.

3. Si el responsable o encargado del tratamiento de datos o información es un entidad de derecho privado se aplicarán las siguientes sanciones:

    a) Con una multa de entre 0,07 y 0,08 calculada sobre el total de ingresos del responsable de tratamiento de datos personales, correspondientes a su última declaración de impuesto a la renta; o,
    b) En caso de reincidencia, con sanción pecuniaria de entre 0,1 y 0,2 calculada sobre el total de ingresos del responsable de tratamiento de datos personales, correspondientes a su última declaración de Impuesto a la Renta.

Artículo 62.- Medidas provisionales o cautelares.- En aquellos casos en el que el cometimiento de una infracción repercuta o afecte de manera directa al derecho a la protección de datos personales, la autoridad de control, aplicará, además de las medidas provisionales de protección o medidas cautelares contempladas en el Código Orgánico

Administrativo, la cesación inmediata en la utilización o cesión ilícita de los información o datos hasta la finalización del procedimiento sancionatorio.

CAPÍTULO X
AUTORIDAD DE CONTROL

Artículo 63.- Autoridad de control.- Para los fines de la presente Ley Orgánica la Dirección Nacional de Registro de Datos Públicos ejercerá las funciones y atribuciones de órgano de control.

Artículo 64.- Atribuciones.- Corresponden a la autoridad de control las siguientes atribuciones:

a) Ejercer la supervisión, control y evaluación preventiva de las actividades efectuadas por el responsable y encargado del tratamiento de datos o información y de las entidades certificadoras;
b) Emitir la normativa y demás actos que sean necesarios para el ejercicio de sus competencias y garantizar el ejercicio del derecho a la protección de datos personales;
c) Autorizar el funcionamiento de entidades certificadoras para la emisión de sellos o marcas de protección de datos personales;
d) Dejar sin efecto la autorización de funcionamiento de las entidades certificadoras o la emisión de sellos o marcas de protección de datos personales conforme a los presupuestos establecidos en la normativa emitida para dicha finalidad y elaborar el modelo de gestión correspondiente;
e) Aprobar los Códigos de Conducta presentados por los responsables o encargados del tratamiento de datos o información o dejar sin efecto los mismos conforme a los presupuestos establecidos en la normativa emitida para dicha finalidad y elaborar el modelo de gestión correspondiente;
f) Ordenar al responsable y encargado del tratamiento de datos o información facilitar los datos personales e información que requiera para el ejercicio de sus funciones;
g) Conocer, tramitar y resolver las peticiones, reclamos, recursos y denuncias interpuestas ante la autoridad de control , así como de aquellos procedimientos administrativos iniciados de oficio;
h) Atender consultas en materia de protección de datos personales;
i) Promover e incentivar el ejercicio del derecho a la protección de datos personales;
j) Disponer a los responsables y encargados del tratamiento de datos o información la adopción de las medidas necesarias para el adecuado tratamiento de datos de conformidad a lo establecido en esta Ley y demás normativa especializada;
k) Ejercer la potestad sancionatoria conforme a los términos establecidos en esta Ley;
l) Solicitar datos e información al responsable o encargado del tratamiento de datos o información sobre la gestión para el adecuado tratamiento de datos personales para el cumplimiento de sus funciones de control y demás atribuciones establecidas en esta Ley y normativa especializada;

m) Ejercer el control y emitir las resoluciones de autorización para la transferencia internacional de datos;
n) Requerir a las instituciones que considere necesario la implementación de acciones adecuadas para garantizar la plena y efectiva aplicación de la presente Ley y normativa especializada.
o) Suscribir acuerdos, convenios o tratados de cooperación internacional en materia de protección de datos personales o actuar en coordinación con las dependencias competentes en la negociación de tratados, acuerdos o convenios internacionales en materia de protección de datos personales;
p) Crear, dirigir y administrar el Registro Nacional de Protección de Datos Personales; y,
q) Las demás atribuciones señaladas en la Constitución y ley.

Artículo 65- Registro Nacional de Protección de Datos Personales.-El responsable del tratamiento o información deberá reportar a la autoridad de control, lo siguiente:

a) Identificación de la base de datos o del tratamiento;
b) El nombre, domicilio legal y datos de contactabilidad del responsable y encargado del tratamiento de datos o información;
c) Características y finalidad del tratamiento de datos o información;
d) Naturaleza de los datos personales tratados;
e) Identificación, nombre, domicilio legal y datos de contactabilidad de los destinatarios;
f) Modo de interrelacionar la información registrada;
g) Medios utilizados para implementar los principios, derechos y obligaciones contenidas en la presente ley y normativa especializada;
h) Requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas implementadas para garantizar la seguridad y protección de datos personales;
i) Tiempo de conservación de los datos;
j) Constancia de la existencia de códigos de conducta;
k) Constancia de disponibilidad de certificaciones, sellos y marcas de protección de datos personales;

Este registro deberá mantenerse actualizado en todo momento, de esta manera se controlará que ningún responsable o encargado del tratamiento de datos o información trate datos personales con fines y características distintas a las declarados en el registro o contratarías a la ley y normativa especializada.

NOTA: ESTE ES UN TEXTO BORRADOR - NO SE HAN INCLUIDO LAS DISPOSICIONES GENERALES, TRANSITORIAS Y REGULATORIAS PERTINENTES.