LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES

Exposición de Motivos:

Es de conocimiento general el espíritu cambiante de la sociedad en que vivimos, las nuevas tendencias y comportamientos componen un sinfín de mecanismos que enmarcan caminos y definen horizontes. El individuo en sí mismo pertenece a un conglobado de oportunidades que siembra libertades, pero no siempre las materializa, esto en virtud de elementos que ajenos a los fines se apropia de ellos y los modifican.

El legislador en esta posición y en términos aristotélicos vendría a ser la justicia animada, en donde el justo medio de un todo revelará una sociedad fructífera, que no esté viciada por extremos equiparables a una inequidad que dista de lo justo que en sí mismo debe ser permanente y acceder a todos los espacios para adjudicarse como tal.

En este contexto es imperante mencionar que el espacio en el que actualmente el individuo se desarrolla no se limita a sus expectativas, sino más bien, en sintonía con la evolución previamente mencionada, el sujeto es símbolo de conservación, labra estrategias que le permiten afianzarse a un terreno sólido y en el camino sobrevivir ante la vulneración de sus libertades, ya que como es conocido, todo aquel mecanismo que las genere será el mismo que las limitará.

Trasladándolo al escenario actual, la colectividad ha experimentado cambios que por su irrevocable importancia han dejado precedentes en la historia, esto es por ejemplo un relativismo ideológico, nuevas formas de agrupación familiar, aumento en la esperanza de vida y en paralelo disminución de la tasa de natalidad y en particular la omnipresencia de la tecnología.

Es así que el individuo aun víctima de las dificultades que con ello advienen, recolecta los aspectos positivos y disfruta de los avances en todo ámbito posible, en el caso puntual, la región digital que de la mano con el perfeccionamiento tecnológico extienden las posibilidades de un nuevo mundo, colaborando así no solo con la efectivización de procesos sino también con el desarrollo económico, facilitando el vivir cotidiano creando redes de distribución de la información y generando en función a ello réditos económicos.

Es de admitir que, las personas se desenvuelven en una sociedad altamente conectada, esto permite que la provisión de distintos servicios y la comunicación, se realicen desde cualquier parte del mundo y en tiempo real. Las tecnologías de la información y comunicación (TIC) han impactado sustancialmente en la vida de las personas, tanto es así, que se han convertido en herramientas y procesos indispensables e ineludibles para la satisfacción de necesidades básicas de los seres humanos.

Su versatilidad permite que estas logren adaptarse a las necesidades y requerimientos de forma personalizada, es por eso que el ser humano las acopla en todas sus actividades manteniendo con ellas una relación incluso cercana a la dependencia. Como consecuencia de ello se ha generado la omnipresencia de las mismas, en la totalidad de las áreas en las que los individuos se desenvuelven (salud, comercio, educación, migración, cooperación internacional, respeto y garantía de derechos, cultura, entre otros).

Es indudable que las TIC representan un sin número de beneficios que tienen como objetivo mejorar la calidad de vida de los seres humanos; sin embargo, también se ha de reconocer que el mismo potencial ha sido invertido para configurar un espacio lleno de múltiples riesgos para las personas.

Esto en virtud de que los individuos no son conscientes del valor de sus datos; considerando que, usados de manera adecuada, pueden generar una serie de ventajas, no solo para su titular, sino también para los proveedores de bienes o servicios públicos o privados que los procesan; pero cuando se tratan de forma irresponsable o abusiva pueden llegar a afectar gravemente la dignidad e integridad de los seres humanos,

es así que, su recopilación, procesamiento y comunicación inadecuada puede significar una vulneración a derechos fundamentales como la vida, la salud, el acceso a servicios públicos, la integridad física, psicológica o sexual, entre muchos otros; lesiones que se han podido evidenciar a nivel mundial y que incluso ya se han familiarizado con la realidad ecuatoriana.

La casi arbitraria libertad con la que se mueve la información acaece desconcierto social por la ausencia de mecanismos de protección que controlen su tratamiento, esto en virtud de que gran parte de esta sujeta datos personales, que utilizados o tratados inadecuadamente pueden, por ejemplo, alterar elecciones presidenciales, determinar quién recibe servicios de salud o alimenticios, ser una herramienta para la delincuencia organizada (trata de personas, narcotráfico o terrorismo). Situaciones que parecen lejanas a nuestra realidad; sin embargo, estas circunstancias se vivencian actualmente incluso en nuestro país, donde se han evidenciado robos, ataques o exposiciones ilegítimas de bases de datos de carácter público o privado, que han generado perjuicios sociales y económicos.

En lo que respecta al siglo pasado la relación instituida entre el Estado y el individuo en cuanto a identificación mutua ha sido realmente escasa; el ambiente percibido en tal época se contenía en cajas de información registrada a mano que en virtud del tiempo se volvía frágil, quebrando consigo toda relación existente.

Actualmente el Estado constituye en sí una de las mayores fuentes de información en razón de la posesión de grandes bases de datos necesarias para la consecución de sus fines administrativos, convirtiéndolo en un efectivizador de procesos que atraviesa la delgada línea entre su posición garantista de derechos humanos y la susceptibilidad de vulnerarlos.

A lo largo de la historia, el ser humano ha sido testigo de grandes vulneraciones a la dignidad, debido al procesamiento de información con fines ajenos al interés general; eventos históricos como la Segunda Guerra Mundial no habrían dejado tantas víctimas, si aquellos que abusaron del poder no hubieran tenido en sus manos información que les permitiera aniquilar a millones de personas.

Hito histórico que parece ajeno a nuestra realidad territorial y actual, pero ejemplos como el proyecto SAFARI en la Francia de 1974 o el Plan Cóndor cultivado por los regímenes dictatoriales del Cono Sur que desencadenaron los "Archivos del terror" de Paraguay en 1992, evidencian lo peligroso que puede ser para el ser humano, no ser consciente del valor de su información.

Con la influencia actual de las tecnologías de la información y comunicación, y los procesos de analítica de datos, es cada vez más necesario entender su trascendencia; en el Ecuador, constantemente se suscitan circunstancias de afectación a derechos, debido al tratamiento inadecuado de datos personales, es muy común encontrar noticias que anuncian el robo de bases de datos, la modificación de las mismas para la obtención de beneficios ilegales, incluso, un intento de incidir en su derecho a elegir por la emisión de noticias falsas.

Es imperante, denotar que las transgresiones no solo se suscitan en el ámbito público, sino que también ocurren a nivel privado, con mayor frecuencia de la que el individuo percibe; en el Ecuador, cualquier abonado a servicios móviles, recibe innumerables llamadas para el ofrecimiento de planes celulares, de seguros y tarjetas de crédito, sin conocer cómo empresas con las que nunca han tenido relaciones obtienen su información y que a pesar de su incomodidad no pueden dejar de ser parte de estas redes.

Así mismo, son innumerables las denuncias por el inicio de procesos que tienen el objeto de deudas que en la mayoría de los casos son inexistentes o la denegación de acceso a servicios por criterios sin fundamento y en algunos casos discriminatorio.

Los datos en la actualidad se consideran activos digitales con gran valor económico, incluso equiparable al del dinero; los sujetos se enfrentan a una realidad en donde su información forma parte de un mercado negro, del que nadie habla pero que es innegable.

Para enfrentar estas dificultades y aprovechar el potencial de las TIC para el desarrollo sostenible, generar confianza en línea y garantizar las oportunidades que brindan los adelantos tecnológicos, cada uno de los países, sobre la base de su estructura normativa propia, ha optado por desarrollar mecanismos de protección de las personas y sus datos.

Hay pocos Estados que no han desarrollado normativa alguna sobre la materia, o la que tienen es incompleta, dispersa o contradictoria; estos son los que mayor desventaja presentan no solo frente a los riesgos y peligros que trae consigo el manejo de datos personales, sino ante la imposibilidad de usarlos como insumos clave para su desarrollo económico y social, lo cual evidencia la posibilidad real de quedar aún más rezagados.

En ese contexto, es indispensable dar certidumbre a usuarios, empresas, organizaciones y Estados, sobre todo en este momento en el cual la economía mundial se desplaza más hacia un espacio de información masiva, hiperconectada, en tiempo real, de flujo incesante proveniente de internet de las cosas, automatizada con algoritmos de inteligencia artificial cada vez más sofisticados, y de la réplica incesante mediante tecnologías de registros distribuidos. Todo esto, unido a que los datos no tienen fronteras y que las plataformas y servicios son de libre disposición y se almacenan en centros de datos de todo el mundo, obliga a los países a realizar marcos jurídicos compatibles en distintos niveles: nacional, regional y mundial que faciliten el intercambio y al mismo tiempo respeten y protejan los derechos humanos.

Por otro lado, en lo que respecta al contexto internacional, el Consejo de Derechos Humanos de la Asamblea General de Naciones Unidas, en Resolución 28/16 "Profundamente preocupado por los efectos negativos que pueden tener para el ejercicio y el goce de los derechos humanos la vigilancia y la interceptación de las comunicaciones, incluidas la vigilancia y la interceptación extraterritoriales de las comunicaciones y la recopilación de datos personales, en particular cuando se llevan a cabo a gran escala" nombra por primera vez al Relator especial sobre el derecho a la privacidad en la era digital con la finalidad de que, entre otras, presente informes que incluya "observaciones importantes" sobre cómo garantizar este derecho fundamental, así como denuncias sobre posibles violaciones.
En el mismo sentido, el 25 de mayo de 2018, entró en vigencia el Reglamento General Europeo de Protección de Datos Personales, su aplicación afecta a todos los países del mundo, ya que únicamente permite e incentiva que países que cuenten con niveles adecuados de protección puedan tratar datos de ciudadanos europeos.

Adicionalmente, es importante mencionar que en el año 2016 se suscribió el Protocolo de Adhesión de Ecuador al Acuerdo Comercial Multipartes con la Unión Europea, con el objetivo de buscar mejores condiciones para el intercambio de bienes y servicios entre los países miembros de la UE y el Estado ecuatoriano; este acuerdo, sin embargo, se ha visto afectado dado que para el intercambio de bienes o servicios, en la mayoría de los casos, se requiere que exista el flujo transfronterizo de datos personales, y al no tener normativa amparada por un ente controlador especializado en la materia, no le es posible al país ofrecer un nivel adecuado de protección, lo que desalienta el comercio y genera que se prefieran destinos como Colombia, Perú y los demás países suscriptores del acuerdo, que si cuentan con Ley de Protección de Datos Personales.

En virtud de estos antecedentes, y dada la urgencia de legislación especializada que se encargue de regular el tratamiento de datos personales, es necesario contar con una Ley, que salvaguarde los derechos, promueva la actividad económica, comercial, de innovación tecnológica, social, cultural, entre otras y que delimite los parámetros para un tratamiento adecuado en el ámbito público y privado.

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, los 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 de forma 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, deberes y oportunidades.*";

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

Que, el numeral 6 del artículo 11 de la Carta Magna determina que "*Todos los principios y derechos son inalienables, indivisibles, interdependientes y de igual jerarquía.*";

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 numeral 9 del artículo 11 de la Constitución de la República prescribe que "*El más alto deber del Estado consiste en respetar y hacer respetar los derechos garantizados en la Constitución. El Estado, sus delegatarios, concesionarios y toda persona que actúe en ejercicio de una potestad pública, estarán obligados a reparar las violaciones a los derechos de los particulares por la falta o deficiencia en la prestación de los servicios públicos, o por las acciones u omisiones de sus funcionarias y funcionarios, y empleadas y empleados públicos en el desempeño de sus cargos*. ";

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 y 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 las 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 y 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 25 del artículo 66 de la Norma Suprema prevé que "*Se reconoce y garantizará a las personas: 25. El derecho a acceder a bienes y servicios públicos y privados de calidad, con eficiencia, eficacia y buen trato, así como a recibir información adecuada y verás sobre su contenido y características.*";

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 a 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 numeral 2 del artículo 133 de la Constitución de la República preceptúa que "*Las leyes serán orgánicas y ordinarias*. Serán leyes orgánicas: 2. Las que regulan el ejercicio de los derechos y garantías constitucionales.";

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 275 de la Norma Suprema preceptúa que "*El régimen de desarrollo es el conjunto organizado, sostenible y dinámico de los sistemas económicos, políticos, socioculturales y ambientales, que garantizaran la realización del buen vivir, del sumak kawsay. El Estado planificará el desarrollo del país para garantizar el ejercicio de los derechos, la consecución de los objetivos del régimen de desarrollo y los principios consagrados en la Constitución. La planificación propiciará la equidad social y territorial, promoverá la concertación, y será participativa, descentralizada, desconcentrada y transparente. El buen vivir requerirá que las personas, comunidades, pueblos y nacionalidades gocen efectivamente de sus derechos, ejerzan responsabilidades en el marco de la interculturalidad, del respeto a sus diversidades, y de la convivencia armónica con la naturaleza*.";

Que, el numeral 1 y 5 del artículo 276 de la Carta Magna prescriben que "*El régimen de desarrollo tendrá los siguientes objetivos: 1. Mejorar la calidad y esperanza de vida, y aumentar las capacidades y potencialidades de la población en el marco de los principios y derechos que establece la Constitución. 5. Garantizar la soberanía nacional, promover la integración latinoamericana e impulsar una inserción estratégica en el contexto internacional, que contribuya a la paz y a un sistema democrático y equitativo mundial.*";

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 283 de la Carta Magna dispone que "*El sistema económico es social y solidario; reconoce al ser humano como sujeto y fin; propende a una relación dinámica y equilibrada entre sociedad, Estado y mercado, en armonía con la naturaleza; y tiene por objetivo garantizar la producción y reproducción de las condiciones materiales e inmateriales que posibiliten el buen vivir.*";

Que, el artículo 285 de la Norma Suprema prescribe que "*El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad: 3. Desarrollar tecnologías e innovaciones que impulsen la*

producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir.";

Que, el numeral 1 del 387 de la Constitución de la República establece que "*Será responsabilidad del Estado: 1. Facilitar e impulsar la incorporación a la sociedad del conocimiento para alcanzar los objetivos del régimen de desarrollo.*";

Que, el artículo 416 de la Carta Maga preceptúa que "*Las relaciones del Ecuador con la comunidad internacional responderán a los intereses del pueblo ecuatoriano, al que le rendirán cuenta sus responsables y ejecutores, y en consecuencia: 1. Proclama la independencia e igualdad jurídica de los Estados, la convivencia pacífica y la autodeterminación de los pueblos, así como la cooperación, la integración y la solidaridad. 7. Exige el respeto de los derechos humanos, en particular de los derechos de las personas migrantes, y propicia su pleno ejercicio mediante el cumplimiento de las obligaciones asumidas con la suscripción de instrumentos internacionales de derechos humanos.*";

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 humano se aplicarán los principios pro ser humano, de no restricción de derechos, de aplicabilidad directa y de cláusula abierta establecidos 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, el artículo 426 de la Norma Suprema establece que "*Todas las personas, autoridades e instituciones están sujetas a la Constitución. (…). Los derechos consagrados en la Constitución y los instrumentos internacionales de derechos humanos serán de inmediato cumplimiento y aplicación. (…).*";

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*.";

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, el Objetivo 1 del Eje 1: Derechos para todos durante toda la vida, del Plan Nacional de Desarrollo 2017-2021-Toda una Vida apunta a "*Garantizar una vida digna con iguales oportunidades para todas las personas.*";

Que, el Objetivo 5 del Eje 2: Economía al servicio de la sociedad, del plan Nacional de Desarrollo 2017-2021-Toda una Vida, persigue "*Impulsar la productividad y competitividad para el crecimiento económico y sostenible de manera redistributiva y solidaria*.";

Que, el Objetivo 7 del Eje 3: Más sociedad, mejor Estado; del plan Nacional de Desarrollo 2017-2021-Toda una Vida, busca "*Incentivar una sociedad participativa, con un Estado cercano al servicio de la ciudadanía*.";

Que, el Objetivo 8 del Eje 3: Más sociedad, mejor Estado; del plan Nacional de Desarrollo 2017-2021-Toda una Vida, pretende "*Promover la transparencia y la corresponsabilidad para una nueva ética social*";

Que, el Objetivo 9 del Eje 3: Más sociedad, mejor Estado; del plan Nacional de Desarrollo 2017-2021-Toda una Vida, aspira a "*Garantizar la soberanía y la paz, y posicionar estratégicamente al país en la región y el mundo*.";

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, el Eje 6 del Plan de la Sociedad de la Información y del Conocimiento 2018-2021, busca "*Promover la protección de datos personales con enfoque de Gobierno, de empresa y para el ciudadano*.";

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 Ecuador Digital, fomenta un Ecuador Eficiente y Ciberseguro, para lo cual, ha establecido que la Protección de Datos Personales es un eje esencial para alcanzarlo, en este sentido, determina como objetivo "*Concientizar a las decenas de miles de usuarios de los portales web del gobierno central acerca de cómo están siendo usados sus datos personales.*".

Que, la Estrategia Ecuador Digital, para alcanzar un Ecuador Eficiente y Ciberseguro, propone, como objetivo dentro del eje de Protección de Datos Personales, "*Poner freno al uso inapropiado de la información personal tanto en el ámbito público como privado*.".

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.*";

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
DISPOSICIONES DIRECTIVAS

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

Artículo 2. Finalidad: La finalidad de la presente Ley es procurar el adecuado tratamiento y flujo de datos personales para garantizar los derechos fundamentales y las 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 y/o privados; y, mejorar la calidad de vida.

Artículo 3. Ámbito de aplicación material: La presente Ley 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 personales.

La presente ley no será aplicable a:

1. El tratamiento de datos personales utilizados en actividades familiares o domésticas;
2. Datos anónimos; y,
3. Datos que identifican o hacen identificable a personas jurídicas.

Son accesibles al público y susceptibles de tratamiento los datos personales de contacto de comerciantes; representantes y socios de personas jurídicas; así como los de servidores públicos siempre y cuando se refieran al ejercicio de su profesión, oficio, giro de negocio, competencias, facultades, atribuciones o cargo.

El histórico y vigente de la declaración patrimonial y de la remuneración para el caso de servidores públicos, por la naturaleza de su cargo, se considerará accesible al público y susceptible de tratamiento.

Artículo 4. 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. El responsable o encargado del tratamiento de datos personales que no se encuentre domiciliado en el Ecuador y oferte bienes o servicios a personas localizadas en el territorio nacional, independientemente de si se requiere su pago o no;

4. El responsable o encargado del tratamiento de datos personales que no se encuentre domiciliado en el Ecuador y realice actividades relativas a la recogida de datos personales de personas localizadas en el territorio nacional; y,
5. Al responsable o encargado del tratamiento de datos personales no domiciliado en el territorio nacional que le resulte aplicable la legislación nacional, en virtud de la celebración de un contrato o del derecho internacional público.

Artículo 5. Términos y definiciones: Para los efectos de la aplicación de la presente Ley 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: 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 personales 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, 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; generalmente se analizan a partir de muestras biológicas.

Dato personal: Dato que identifica o hace identificable a una persona natural, directa o indirectamente, en el presente o futuro. Los datos inocuos, metadatos o fragmentos de datos que identifiquen o hagan identificable a un ser humano, forman parte de este concepto.

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

Datos personales registrables: Datos personales que conforme al ordenamiento jurídico deben estar contenidos en Registros Públicos.

Datos sensibles: Se consideran datos sensibles los 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 humanos o la dignidad e integridad de las personas. La Autoridad de Protección de Datos Personales podrá determinar otras categorías de datos sensibles.

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

Disociación de datos: Todo tratamiento de datos personales destinado a que éstos no puedan ser asociados o vinculados a una persona identificada o identificable.

Elaboración de perfiles: Todo tratamiento de datos personales que permite evaluar, analizar o predecir aspectos 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 personales: Persona que trate datos personales por nombre y a cuenta de un responsable de tratamiento de datos personales.

Estado de la técnica: Estado último de cualquier particularidad que permita establecer bases de comparación para determinar si los requisitos o herramientas de carácter administrativo, físico, técnico, organizativo, jurídico u otros constituyen niveles adecuados de protección en el tratamiento de datos personales.

Filtración: Es un incidente ilegal o no autorizado que involucra la visualización, acceso, extracción o divulgación de datos personales por un individuo, aplicación, servicio u otros.

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 Protección de Datos Personales.

Política de tratamiento de datos personales: Documento físico, electrónico o en cualquier formato generado por el responsable del tratamiento de datos personales 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, cuyo contenido será definido por la Autoridad de Protección de Datos Personales.

Responsable del tratamiento de datos personales**:** Persona natural o jurídica, pública o privada, que 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.

Tercero: Persona que no ostenta la calidad de responsable o encargado de tratamiento; titular; o, Autoridad de Protección de Datos Personales, conforme al alcance establecido en la presente Ley.

Titular: Persona natural cuyos datos son objeto de tratamiento.

Transferencia o comunicación: Manifestación, declaración, publicación, 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 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, tales como: la recogida, recopilación, obtención, 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.

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

Artículo 6. Sujetos intervinientes: Son parte del sistema de protección de datos personales, lo siguientes sujetos:

1. Titular;
2. Responsable del tratamiento;
3. Encargado del tratamiento;
4. Tercero;
5. Destinatario;
6. Autoridad de protección de datos;
7. Entidades certificadoras; y,
8. Delegado de protección de datos personales.

Artículo 7. Normas aplicables al ejercicio de derechos: El ejercicio de los derechos a la protección de datos personales, se canalizará a través del responsable del tratamiento, Autoridad de Protección de Datos Personales y/o jueces competentes, de conformidad con el procedimiento establecido en la presente ley.

CAPÍTULO II
PRINCIPIOS

Artículo 8. 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 juridicidad, lealtad y transparencia; legitimidad; finalidad; pertinencia y minimización de datos personales; proporcionalidad del tratamiento; consentimiento; confidencialidad; calidad; conservación; seguridad de datos personales; responsabilidad proactiva y demostrada; aplicación favorable al titular; e, independencia de control.

Artículo 9. Juridicidad, lealtad y transparencia: 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.

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, su reglamento y demás normativa atinente a la materia.

Artículo 10. Legitimidad: El tratamiento solo será legítimo y lícito si se cumple con alguna de las siguientes condiciones:

1. Exista obligación en el ordenamiento jurídico aplicable al responsable del tratamiento;
2. Por orden judicial, resolución o mandato motivado de autoridad pública competente;
3. Para el ejercicio de las competencias y facultades establecidas en la Constitución, la Ley, instrumentos internacionales ratificados por el Ecuador y demás normativa aplicable a favor de las entidades pertenecientes al sector público, sus delegatarios y organizaciones de Derecho Internacional Público;
4. 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;

5. Para la ejecución de medidas precontractuales a petición del titular, excepto cuando prevalezcan los intereses o los derechos y libertades de niñas, niños y adolescentes como titulares;
6. Por consentimiento del titular para el tratamiento de sus datos personales para una o varias finalidades específicas; o,
7. Para proteger intereses vitales, del interesado o de otra persona natural, como por ejemplo su vida, salud o integridad.

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.

Artículo 12. Pertinencia y Minimización de datos personales: Los datos personales deben ser pertinentes y limitados a lo mínimo necesario para su finalidad.

Artículo 13. Proporcionalidad del tratamiento: El tratamiento debe ser adecuado, necesario, oportuno, relevante y no excesivo en relación a las finalidades para las cuales han sido recogidos o a la naturaleza de las categorías especiales de datos.

Artículo 14. Consentimiento: Se podrán tratar y comunicar datos personales cuando se cuente con la manifestación de la voluntad del titular de hacerlo.

El consentimiento será válido, cuando la manifestación de la voluntad sea: *libre*, es decir, que se encuentre exenta de vicios del consentimiento; *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 a la transparencia; *inequívoca*, 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 del tratamiento de datos personales establecerá mecanismos que garanticen celeridad, eficiencia, eficacia y gratuidad, así como un procedimiento igual de sencillo que el que fue llevado para recabar el consentimiento.

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

Artículo 15. Confidencialidad: El tratamiento de datos personales debe concebirse sobre la base del debido sigilo y secreto, es decir, no deben tratarse o comunicarse para un fin distinto para el cual fueron recogidos, sin que se cuente con el consentimiento del titular o concurra una de las causales que habiliten el tratamiento conforme al principio de legitimidad. 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 16. Calidad: 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.

La Autoridad de Protección de Datos Personales definirá los casos en los cuales se deberán actualizar los datos personales y su periodicidad.

Artículo 17. Conservación: Los datos personales serán conservados conforme a los siguientes presupuestos:

1. Durante el tiempo consentido, determinado en el ordenamiento jurídico o establecido en orden judicial, resolución o mandato motivado de autoridad pública competente; o,
2. Hasta cuando cumplan con la finalidad para la cual fueron recogidos o tratados.

Cumplido uno de los presupuestos establecidos, 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.

El posterior tratamiento de datos personales únicamente se realizará para la investigación científica, histórica o estadística, que se realice en favor del interés público, siempre y cuando se establezcan las garantías de seguridad y protección de datos personales oportunas, así como las demás que contemple la presente Ley, su Reglamento de Aplicación o las Resoluciones de la Autoridad de Protección de Datos Personales, para salvaguardar los derechos contemplados en esta norma.

Artículo 18. Seguridad de datos personales: Los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas y necesarias, sean éstas técnicas, organizativas o de cualquier otra índole, para proteger los datos personales frente a cualquier riesgo, amenaza, vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita, atendiendo a la naturaleza de los datos de carácter personal, al ámbito y el contexto.

Artículo 19. 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 corregulación, 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.

***Artículo 20. 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.

Artículo 21. Independencia de control: Para el efectivo ejercicio del derecho a la protección de datos personales, el Estado ejercerá un control independiente, imparcial y autónomo, así como su regulación y sanción.

Artículo 22. Normativa especializada: Los datos personales cuyo tratamiento se encuentre regulado en normativa especializada en materia de ejercicio de la libertad de expresión, 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 de juridicidad, lealtad y transparencia; legitimidad; finalidad; confidencialidad; conservación, seguridad de datos personales; responsabilidad proactiva y demostrada, en los casos que corresponda; y, de aplicación favorable.

CAPÍTULO III
DERECHOS

Artículo 23. Derecho a la lealtad, transparencia e información: El titular de datos personales tiene derecho a ser informado de forma leal y transparente por cualquier medio sobre:

1. Los fines del tratamiento;
2. Base legal para el tratamiento;
3. Tipos de tratamiento;
4. Tiempo de conservación;
5. La existencia de una base de datos en donde consten 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 incluye: dirección de domicilio legal, número de teléfono y correo electrónico;
9. Identidad y datos de contacto del delegado de protección de datos personales, que incluye: dirección domiciliaria, 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;
11. Carácter obligatorio o facultativo de la respuesta y las consecuencias de proporcionar o no sus datos personales;
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 fueran obtenidos 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.

Excepcionalmente, el titular deberá ser informado de forma posterior, dentro del mes siguiente, cuando los datos personales no se obtuvieren de forma directa; expresa; transparente; inteligible; concisa; precisa; sin barreras técnicas; e, inequívoca.

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; gratuitos; suficientes; disponibles de forma permanente y redactarse en un lenguaje claro; sencillo; y, de fácil comprensión incluso cuando se trate de contratación electrónica.

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 artículo será proporcionada a su representante legal conforme a lo dispuesto en el inciso precedente.

***Artículo 24. Derecho de Acceso*:** El titular tiene derecho a conocer y a obtener 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.

En caso de que fuera necesario restringir o negar dicho acceso, deberán especificarse las razones concretas de dicha restricción o negativa de acuerdo a lo establecido en la normativa vigente.

***Artículo 25. 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.

***Artículo 26. 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 personales, cuando:

1. El tratamiento no cumpla con los principios de juridicidad, lealtad, transparencia y legitimidad;
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; o
6. 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 personales implementará métodos y técnicas orientadas a eliminar, anular, borrar, hacer ilegible, destruir o dejar irreconocibles de forma definitiva y segura, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales.

Artículo 27. Derecho al olvido digital: El titular tiene el derecho a solicitar al juez competente, obtener sin dilación indebida del responsable del tratamiento la supresión de sus datos personales que estén siendo tratados en el entorno digital, cuando concurra alguna de las circunstancias siguientes:

1. Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados;
2. El interesado retire el consentimiento en que se basa el tratamiento o solicite su supresión;
3. El interesado se oponga al tratamiento, y no prevalezcan otros motivos legítimos para el tratamiento;

4. Los datos personales hayan sido tratados ilícitamente;
5. Los datos personales sean de carácter obsoleto;
6. Los datos personales no tengan valor histórico o científico;
7. Los datos personales no sean de relevancia pública; o,
8. Los datos personales sean inadecuados, inexactos, impertinentes o excesivos con relación a los fines y al tiempo transcurrido.

Lo anterior no se aplicará cuando el tratamiento sea necesario por cualquiera de las siguientes causas:

1. Para ejercer el derecho a la libertad de expresión e información;
2. Para el cumplimiento de una obligación legal que requiera el tratamiento de datos por parte del responsable del tratamiento;
3. Por razones de interés público en el ámbito de la salud pública;
4. Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos; o,
5. Para la formulación, el ejercicio o la defensa de reclamaciones.

Para la aplicación del presente artículo, se estará a las siguientes definiciones:

Datos personales tratados en el entorno digital: Datos personales que son tratados en redes de computadoras públicas o privadas (Internet o Intranet). Se entiende por redes privadas aquellas que no están abiertas al acceso de todo público pero que si son usadas por una colectividad de usuarios autorizados.

Datos personales de carácter obsoleto: Datos personales que ya no están en uso, son antiguos, anticuados o han dejado de tener vigencia o relevancia para los fines del tratamiento.

Datos personales que no tengan valor histórico o científico: Datos personales que no son útiles, necesarios o de valor significativo para la ciencia o la historia política o social de Ecuador.

Datos personales que no sean de relevancia pública: Datos personales que el público en general no necesita o no tiene interés justificado en conocer.

***Artículo 28. 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 29. Derecho de anulación: El titular tiene derecho a solicitar la nulidad por ilicitud en el acto o por el tratamiento de datos personales ante autoridad jurisdiccional, bajo las causales señaladas para la nulidad en materia civil, mercantil y administrativa, según sea el caso.

***Artículo 30. Derecho a la portabilidad*:** El titular tiene derecho a recibir del responsable del tratamiento, sus datos personales en un formato compatible, actualizado, estructurado, común, interoperable y de lectura mecánica, preservando sus características; y/o transmitirlos a otros responsables.

El titular podrá solicitar la transferencia o comunicación de sus datos personales a otro responsable del tratamiento. Luego de completada la transferencia, el responsable que transfiere dichos datos procederá a su eliminación.

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;
2. Que el tratamiento se efectúe por medios automatizados;
3. Que se trate de un volumen relevante de datos personales; 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, efectiva 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.

***Artículo 31. Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y/o portabilidad*:** No proceden los derechos de rectificación, actualización, eliminación, oposición, anulación y/o 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. Para el cumplimiento de una obligación legal o contractual;
3. Para el cumplimiento de una orden judicial, resolución o mandato motivado de autoridad pública competente;
4. 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;
6. Cuando se pueda obstaculizar actuaciones judiciales o administrativas en curso debidamente notificadas;
7. Para ejercer el derecho a la libertad de expresión y opinión;
8. Para proteger el interés vital del interesado o de otra persona natural;
9. En los casos en que medie el interés público; o,
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.

***Artículo 32. 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 de datos personales; 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 juridicidad, lealtad, transparencia, legitimidad, acceso, eliminación, rectificación y actualización, oposición, anulación, portabilidad, limitación del tratamiento o, de no ser objeto de una decisión basada únicamente en valoraciones automatizadas; hasta su resolución por el responsable o encargado del tratamiento de datos personales.

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 limitación se extenderá hasta la resolución del procedimiento administrativo.

El responsable del tratamiento de datos personales conservará únicamente los datos personales que sean necesarios para la formulación de un reclamo, una vez cumplido el plazo o condición del tratamiento.

***Artículo 33. Derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas*:** El titular tiene derecho a no ser sometido a una decisión basada únicamente en 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:

1. Solicitar una explicación motivada sobre la decisión tomada por el responsable o encargado del tratamiento de datos personales;
2. Presentar observaciones;
3. Solicitar los criterios de valoración sobre el programa automatizado; y/o,
4. Impugnar la decisión ante el responsable o encargado de 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 pública 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 del titular.

Artículo 34. 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.

Artículo 35. 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.

El órgano rector de la educación, en coordinación con la Autoridad de Protección de Datos, emitirá las directrices para que las entidades educativas garanticen 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 relacionado con 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.

***Artículo 36. 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, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales.

Los adolescentes mayores a doce (12) años y menores de dieciséis (16) años, así como las niñas y niños, para el ejercicio de sus derechos necesitarán de su representante legal. Los adolescentes mayores a dieciséis (16) 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 y del tratamiento.

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

Artículo 37. Excepción por normativa especializada: No proceden los derechos establecidos en esta ley, para los datos personales cuyo tratamiento se encuentre regulado en normativa especializada en materia de ejercicio de la libertad de expresión, 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. En estos casos, los titulares podrán ejercer los derechos previstos en dicha normativa especializada.

CAPÍTULO IV
CATEGORÍAS ESPECIALES DE DATOS PERSONALES

***Artículo 38. Categorías especiales de datos personales*:** Se aplicará lo dispuesto en el presente capítulo al tratamiento de datos sensibles, datos de niñas, niños y adolescentes, datos crediticios, datos de salud y datos necesarios para el archivo de información que constituya patrimonio del Estado, investigación científica, histórica o estadística.

Artículo 39. Consentimiento relativo a categorías especiales de datos: 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 mayores a dieciséis (16) años y menores de dieciocho (18) años.

Para el caso de adolescentes mayores a doce (12) años y menores de dieciséis (16) años, así como de niñas y niños, es necesario contar con el consentimiento explícito y verificable de su representante legal. La Autoridad de Protección de Datos Personales definirá los parámetros de verificación del consentimiento.

Se entiende por consentimiento explícito aquel que puede ser demostrado de manera indubitable por el responsable o encargado del tratamiento de datos personales, en relación a la autorización otorgada por el titular a través de una declaración o acción clara y afirmativa.

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

Artículo 40. Lealtad, transparencia e información de categorías especiales de datos: Además de la información establecida en el derecho a la lealtad, transparencia e información, el responsable o encargado del tratamiento de datos personales, deberá informar al titular o al representante legal, del carácter facultativo de sus respuestas, consecuencias y los derechos que le asisten al titular, respecto de datos sensibles y de datos de niñas, niños y adolescentes.

Artículo 41. Derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas en categorías especiales de datos: Además de los presupuestos establecidos en el derecho a no ser objeto

de una decisión basada únicamente en valoraciones automatizadas, no se podrán tratar datos sensibles o datos de niñas, niños y adolescentes, a menos que se cuente con autorización explícita del titular o representante legal; o, cuando dicho tratamiento esté destinado a salvaguardar el interés público.

Artículo 42. Datos de personas fallecidas: Los titulares de derechos sucesorios del fallecido, 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.

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 éste; y, en su caso su rectificación, actualización o eliminación.

En caso de fallecimiento de niñas, niños, adolescentes o personas a las que la Ley reconoce como incapaces, las facultades de acceso, rectificación y actualización o eliminación, podrán ejercerse por quién hubiese sido su último representante legal.

El ejercicio de este derecho estará regulado en el Reglamento a la presente Ley.

***Artículo 43. 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 sujetará a lo previsto a la normativa aplicable, y subsidiariamente a lo dispuesto en la presente Ley, su Reglamento y demás normativa dictada por la Autoridad de Protección de Datos Personales.

***Artículo 44. Datos crediticios*:** 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.

Artículo 45. Datos relativos a la salud: Las instituciones y centros sanitarios públicos y privados, así como los profesionales correspondientes, podrán tratar datos personales relativos a la salud de sus pacientes, de acuerdo 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.

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

Artículo 46. 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 y, además, se cuente con el consentimiento del titular.

Artículo 47. Acceso a datos personales por parte de terceros: El acceso de un tercero a datos personales, no se considerará transferencia o comunicación, siempre que sea necesario para la prestación de un servicio al responsable del tratamiento de datos personales. El tercero que ha accedido legítimamente a datos personales en estas condiciones, será considerado encargado de tratamiento.

El tratamiento de datos personales realizado por terceros deberá estar regulado por un contrato, en donde se establezca de manera clara y precisa que el encargado del tratamiento de datos personales únicamente tratará los mismos conforme las instrucciones del responsable y que no los aplicará o utilizará para

finalidades diferentes a las que figuren 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.

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

Artículo 48. 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 bases 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 normativa vigente;
4. Cuando la comunicación se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos, siempre y cuando dichos datos se encuentren debidamente disociados; y,
5. Cuando la comunicación de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre salud.

Cuando, sea requerido el consentimiento del titular para que sus datos personales sean comunicados a un tercero, éste 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 disociación.

Artículo 49. Falta de consentimiento para la transferencia o comunicación de datos personales: Se entenderá que no hubo consentimiento para la transferencia o comunicación de datos personales cuando el responsable del tratamiento no haya entregado información suficiente al titular, que le permita conocer la finalidad a que se destinarán sus datos o el tipo de actividad del tercero a quien se pretende transferir o comunicar dichos datos.

CAPÍTULO VI
SEGURIDAD DE DATOS PERSONALES

***Artículo 50. 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 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 y el nivel de impacto que estos representen a los derechos fundamentales y libertades individuales.

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 demostrar 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, encriptación, cifrado o codificación 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, organizativa, y jurídica.

Los responsables y encargados del tratamiento de datos personales, podrán acogerse a estándares 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 Protección de Datos Personales.

***Artículo 51. Medidas de seguridad en el ámbito del sector público*:** El mecanismo gubernamental de seguridad de la información incluirá las medidas que deban implementarse en el 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 datos conforme al principio de seguridad de datos personales.

El alcance de aplicación del mecanismo gubernamental de seguridad de la información, que incluya las disposiciones establecidas en el primer párrafo del presente artículo, abarcará a todos los miembros del sector público, conforme a lo detallado en el artículo 225 de la Constitución de la República del Ecuador.

Las instituciones mencionadas en el párrafo precedente podrán incorporar medidas adicionales a las establecidas en el mecanismo gubernamental de seguridad de la información, atendiendo a la naturaleza de sus atribuciones y funciones.

Artículo 52. Protección de datos personales desde el diseño y por defecto: El responsable y el encargado implementarán las medidas técnicas, organizativas y de cualquier otra índole con miras a garantizar que los procesos y medios de tratamiento protejan los datos personales desde su diseño, así como sus configuraciones se encuentren por defecto en cumplimiento de las disposiciones de la presente Ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

***Artículo 53. Análisis de riesgo y determinación de medidas de seguridad aplicables*:** Para el análisis de riesgos, amenazas y vulnerabilidades, el responsable y el encargado del tratamiento de datos personales deberán utilizar una metodología que considere, entre otros:

1. Las particularidades del tratamiento;
2. Las particularidades de las partes involucradas; y,
3. El tipo y volumen de datos personales objeto del tratamiento.

Para determinar las medidas de seguridad necesarias y adecuadas, se deberán tomar en cuenta, 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, pérdida, alteración, divulgación o impedimento de acceso al titular a los mismos, sean éstas accidentales o intencionales, por acción u omisión, así como los de transferencia, comunicación, o acceso no autorizados o en exceso de autorización a dichos 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 técnica emitida por la Autoridad de Protección de Datos Personales.

Artículo 54. Evaluación de impacto del tratamiento de datos personales: El responsable realizará una evaluación de impacto del tratamiento de datos personales cuando se ha identificado la probabilidad de que dicho tratamiento, por su naturaleza, contexto o fines, conlleva un alto riesgo para los derechos y libertades del titular.

La evaluación de impacto del tratamiento de datos personales podrá analizar un conjunto de tratamientos equivalentes que conlleven altos riesgos similares.

La evaluación de impacto deberá efectuarse previo al inicio del tratamiento de datos personales mencionado en el presente artículo.

***Artículo 55. 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, dentro del término de tres (3) días a partir del conocimiento de dicha vulneración.

El encargado de tratamiento deberá notificar al responsable la vulneración de la seguridad de datos personales en un término no mayor a dos (2) días después de tener conocimiento de ella.

En caso de retraso del responsable o del encargado del tratamiento de datos personales 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.

En la notificación deberá constar lo siguiente:

1. La descripción de la naturaleza de la vulneración de la seguridad de los datos personales;
2. Las categorías y el número aproximado de titulares afectados;
3. Las categorías y el número aproximado de registros o campos de datos personales afectados;
4. El nombre y los datos de contacto del delegado de protección de datos, o a falta de este, de cualquier otro punto de contacto;
5. La descripción de las posibles consecuencias de la vulneración de la seguridad de los datos personales;
6. La descripción de las medidas adoptadas, implementadas o propuestas por el responsable para remediar la vulneración de la seguridad de los datos personales; y,
7. De ser el caso, las medidas adoptadas e implementadas para mitigar los posibles efectos negativos de la vulneración de la seguridad de datos personales.

Una vez tomado conocimiento de la vulneración de las seguridades de datos personales, el responsable deberá efectuar el análisis de riesgo sobre los derechos de libertad de sus titulares.

La notificación de las vulneraciones de seguridad de datos personales tendrá como objeto principal que la Autoridad de Protección de Datos Personales lleve un registro estadístico sobre vulneraciones e identificar posibles medidas de seguridad para cada una de ellas, así como identificar sectores o instituciones más vulnerables y promover nuevas regulaciones que busquen mejorar las seguridades exigibles a los responsables de tratamiento y otorgar seguridad jurídica en el tratamiento de datos personales.

La Autoridad de Protección de Datos Personales sólo podrá sancionar al responsable o encargado del tratamiento, cuando la vulneración de seguridad de datos personales ha sido producto de incumplimientos a las medidas de seguridad adecuadas. En tal caso, la notificación oportuna de la violación por parte del responsable de tratamiento, tanto a la autoridad como al titular, así como las medidas de respuesta adoptadas, serán considerados como un atenuante de la infracción.

En caso de no cumplimiento del término para la notificación, el responsable del tratamiento deberá justificar la dilación, caso contrario, se procederá conforme al régimen sancionatorio establecido para el efecto.

***Artículo 56. 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 y alcance necesarios para, de forma exclusiva, su detección, análisis, protección y respuesta ante incidentes, así como para adoptar e implementar medidas de seguridad adecuadas y proporcionadas a los riesgos identificados.

***Artículo 57. Notificación de vulneración de seguridad al titular*:** El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a su titular, cuando conlleve un riesgo a sus derechos de libertad, de forma inmediata o hasta dentro de un término de tres (3) días, contados a partir de tener conocimiento del riesgo.

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

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 su seguridad;
2. Cuando el responsable del tratamiento haya tomado medidas que garanticen que ya no se concrete el riesgo para los derechos de libertad del titular; y,
3. Cuando se requiera un esfuerzo desproporcionado, para lo cual se realizará una comunicación pública, a través de cualquier medio, en la que se informe a los titulares.

La notificación al titular del dato contendrá lo señalado en el artículo precedente.

En caso de no cumplimiento del término para la notificación, el responsable del tratamiento deberá justificar la dilación, caso contrario, se procederá conforme al régimen sancionatorio establecido para el efecto.

***Artículo 58. Delegado de protección de datos personales*:** Se designará un delegado de protección de datos personales cuando:

1. 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. Las actividades del responsable o encargado de tratamiento de datos personales requieran de un control permanente y sistematizado debido a su volumen, naturaleza, alcance y/o finalidades del tratamiento;
3. Se refiera a tratamientos de gran volumen de categorías especiales de datos; y,
4. El tratamiento se refiera a datos relacionados con la seguridad nacional y defensa del Estado no regulado por normativa especializada.

La Autoridad de Protección de Datos Personales podrá definir nuevas condiciones para la necesidad de contar con un Delegado de Protección de Datos Personales, así como emitir directrices para su designación.

***Artículo 59. Consideraciones especiales para el delegado de protección de datos personales*:** Para la ejecución de sus funciones como delegado de protección de datos personales, se deberá considerar lo siguiente:

1. Corresponde al responsable y al encargado 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. Es responsabilidad del responsable y del encargado facilitar el acceso a los datos personales y a las operaciones de tratamiento, así como todos los recursos y elementos necesarios para garantizar el correcto y libre desempeño de sus funciones;
3. Corresponde al responsable y al encargado capacitar y actualizar los conocimientos del delegado de protección de datos personales en la materia, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales;
4. El responsable y el encargado no podrán destituir o sancionar al delegado de protección de datos personales por el desempeño de sus funciones;
5. El delegado de protección de datos personales mantendrá relación directa con el más alto nivel jerárquico del responsable o encargado;
6. El titular podrá contactar al delegado de protección de datos personales en relación al tratamiento de sus datos personales y al ejercicio de sus derechos;
7. El delegado de protección de datos personales estará obligado a mantener la más estricta confidencialidad respecto a la ejecución de sus funciones; y,
8. Siempre que no exista conflicto con sus responsabilidades establecidas en la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y demás normativa sobre la materia, el delegado de protección de datos personales podrá desempeñar otras funciones dispuestas por el responsable o el encargado.

Artículo 60. Funciones del delegado de protección de datos personales: El delegado de protección de datos personales tendrá, entre otras, las siguientes funciones y atribuciones:

1. Informar y asesorar al responsable y encargado del tratamiento de datos personales, así como al personal relacionado al tratamiento de datos personales, respecto a las disposiciones contenidas en esta ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y demás normativa sobre la materia;
2. Supervisar el cumplimiento de las disposiciones contenidas en esta ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y demás normativa sobre la materia;
3. Asesorar en el análisis de riesgo, evaluación de impacto y evaluación de medidas de seguridad, así como supervisar su aplicación; y,
4. Cooperar con la Autoridad de Protección de Datos Personales y actuar como punto de contacto con dicha entidad en relación a las cuestiones referentes al tratamiento.

La Autoridad de Protección de Datos Personales podrá definir otras funciones, atribuciones y responsabilidades para el delegado de protección de datos personales, atendiendo a la naturaleza de los datos de carácter personal, al ámbito, el contexto y finalidades del tratamiento.

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

CAPÍTULO VII
DE LA RESPONSABILIDAD PROACTIVA

Artículo 61. Aplicación del principio de responsabilidad proactiva: Los responsables y encargados de tratamiento de datos personales podrán, de manera voluntaria, acogerse o adherirse a códigos de protección, estándares, certificaciones, sellos y mejores prácticas para dar cumplimiento al principio de responsabilidad proactiva, 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.

La Autoridad de Protección de Datos Personales aprobará los contenidos de códigos de protección; evaluará, controlará, autorizará, sancionará y revocará, cuando sea procedente, las autorizaciones otorgadas a entidades certificadoras para su funcionamiento, así como evaluará, controlará y, de ser el caso, revocará las certificaciones y sellos otorgados por dichas entidades; y, además avalará estándares y mejores prácticas.

***Artículo 62. Atribuciones de las Entidades de Certificación*:** En materia de protección de datos personales, las Entidades de Certificación, 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.

***Artículo 63. Reconocimiento y revocatoria como Entidad Certificadora*:** La Autoridad de Protección de Datos Personales emitirá las directrices para la constitución y autorización de funcionamiento de las Entidades Certificadoras, y para su evaluación continua y permanente.

La Autoridad de Protección de Datos Personales, mediante resolución motivada, podrá revocar, de ser el caso, la autorización de funcionamiento como Entidad Certificadora en cualquier momento.

CAPÍTULO VIII
TRANSFERENCIA O COMUNICACIÓN INTERNACIONAL DE DATOS PERSONALES

***Artículo 64. 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.

***Artículo 65. Criterios para declarar el nivel adecuado de protección*:** Para declarar de nivel adecuado de protección a países u organizaciones, la Autoridad de Protección de Datos Personales emitirá resolución motivada, en la cual se verificará la existencia de los siguientes presupuestos:

1. Que cuente con normativa que promueva y garantice el ejercicio de derechos fundamentales y libertades individuales;
2. Que cuente con una autoridad estatal independiente que garantice y promueva la efectiva tutela del derecho a la protección de datos personales;
3. Que cuente con normativa especializada en materia de protección de datos personales;
4. Que sea parte de Acuerdos o instrumentos internacionales vinculantes ratificados por un tercer país u organización que generen obligaciones respecto al tratamiento y trasferencia o comunicación de datos personales, siempre que estos establezcan un estándar igual o mayor de protección en favor del titular, más allá de su origen o nacionalidad; y,
5. Que posea legislación específica en materia seguridad nacional y defensa del Estado, que establezca mecanismos de control y verificación del 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. 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.

***Artículo 66. 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 u organizaciones que brinden niveles adecuados de protección, conforme a los criterios establecidos en el artículo precedente.

***Artículo 67. Transferencia o comunicación mediante garantías adecuadas**:* Este mecanismo de transferencia o comunicación transfronteriza de datos personales opera cuando no existe una resolución de nivel adecuado de protección, en su lugar el responsable o encargado del tratamiento de datos personales deberá tomar medidas para compensar la falta de protección de datos en un tercer país u organización mediante garantías adecuadas para el titular, debiendo cumplir al menos con las siguientes:

1. Observancia de principios, derechos y obligaciones en el tratamiento de datos personales siempre que estos cumplan con un estándar igual o mayor de protección;
2. Efectiva tutela del derecho a la protección de datos personales, a través de la disponibilidad permanente de acciones administrativas o judiciales; y,
3. El derecho a solicitar la reparación integral, de ser el caso.

Para la consecución de este mecanismo se requiere de instrumentos jurídicos vinculantes y exigibles entre autoridades y responsables del tratamiento de datos personales tales como: normas corporativas vinculantes, cláusulas estándar de protección de datos, cláusulas o garantías adicionales o específicas, códigos de protección, mecanismos de certificación, sellos de protección de datos personales aprobados.

Corresponde a la Autoridad de Protección de Datos Personales dictar el contenido de las cláusulas estándar de protección de datos, así como la verificación de cláusulas o garantías adicionales o específicas acordadas entre las partes.

La Autoridad de Protección de Datos Personales aprobará códigos de protección, mecanismos de certificación y sellos de protección de datos personales.

Para el cumplimiento de lo previsto en el presente artículo, se considerarán los derechos, garantías y principios de la presente ley, como requisitos y condiciones mínimas para la transferencia o comunicación internacional.

***Artículo 68. 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, específicas y aplicadas al ámbito de su actividad, en las cuales, para su aprobación, deberán cumplir las siguientes condiciones:

1. Ser de obligatorio cumplimiento para el responsable de tratamiento, la totalidad del grupo empresarial al que ésta pertenezca, sus empresas asociadas y cualquier otra 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 constantes en 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 de 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 como el tipo de tratamiento a realizarse y su finalidad;
5. Enunciar de forma expresa el carácter jurídicamente vinculante de tales normas a nivel nacional e internacional;
6. 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;
7. 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 éste demuestra que el acto que originó los daños y perjuicios no le es imputable.
8. Incluir los mecanismos en que se facilita al titular la información clara y completa, respecto a las normas corporativas vinculantes y sus efectos jurídicos;
9. 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;
10. Detallar los procesos o procedimientos en vía administrativa o judicial que le asistan;
11. 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 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 auditorías serán de acceso público, debidamente publicados y se pondrán a disposición de la Autoridad de Protección de Datos Personales en la periodicidad establecida en el reglamento a la presente ley;
12. 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,
13. 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 previamente aprobado por la Autoridad de Protección de Datos Personales y notificado al titular conforme a los mecanismos señalados por el responsable de tratamiento en su solicitud de aprobación.

***Artículo 69. Casos excepcionales de transferencias o comunicaciones internacionales*:** En aquellos casos donde no se cumpla con los criterios de niveles adecuados de protección o de garantías adecuadas de protección, la Autoridad de Protección de Datos Personales podrá autorizar transferencias o comunicaciones internacionales de datos personales, en los siguientes casos:

1. A países u organismos internacionales que brinden garantías adecuadas para la protección de datos personales sin que necesariamente exista una ley específica o Autoridad de Protección de Datos Personales, para lo cual será necesaria la suscripción de un convenio o tratado internacional;
2. Cuando los datos personales sean requeridos para el cumplimiento de competencias institucionales, de conformidad con la normativa aplicable;
3. Cuando el titular haya otorgado su consentimiento explícito a la transferencia o comunicación propuesta, tras haber sido informado de las finalidades del tratamiento y posibles riesgos para él de dichas transferencias o comunicaciones internacionales, debido a la ausencia de una resolución de nivel adecuado de protección y de garantías adecuadas;
4. Cuando la transferencia internacional tenga como finalidad el cumplimiento de una obligación legal o regulatoria;
5. 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 personales, o para la ejecución de medidas de carácter precontractual adoptadas a solicitud del titular;
6. 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 personales y otra persona natural o jurídica;
7. Cuando la transferencia sea necesaria por razones de interés público;
8. Cuando la transferencia internacional sea necesaria para la colaboración judicial internacional;
9. Cuando la transferencia internacional sea necesaria para la cooperación dentro de la investigación de infracciones;
10. Cuando la transferencia internacional es necesaria para el cumplimiento de compromisos adquiridos en procesos de cooperación internacional entre Estados;
11. Transferencias bancarias y bursátiles;
12. 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,
13. 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 70. 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 actualizado, una lista de países, organizaciones, empresas o grupos económicos que garanticen niveles adecuados de protección de datos personales.

CAPITULO IX
DE LAS OBLIGACIONES

***Artículo 71. Obligaciones del responsable del tratamiento de datos personales*:** El responsable del tratamiento está obligado a:

1. Tratar datos personales en estricto apego a los principios y derechos desarrollados 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;
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 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 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 personales en cada caso en particular;
5. Adherirse a códigos de protección, mecanismos de certificación o sellos de protección de datos personales aprobados por la Autoridad de Protección de Datos Personales;
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 personales;
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 Protección de Datos Personales y al titular de violaciones a las seguridades implementadas para el tratamiento de datos personales conforme a lo establecido en el procedimiento previsto para el efecto;
10. Implementar la protección de datos personales 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 personales o que tenga conocimiento de los datos personales;
12. Elegir y designar el encargado del tratamiento de datos personales que ofrezca mecanismos suficientes para garantizar el derecho a la protección de datos personales conforme 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;
13. 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;
14. Designar al Delegado de Protección de Datos Personales;
15. Permitir y contribuir a la realización de auditorías o inspecciones, por parte de un auditor acreditado por la Autoridad de Protección de Datos Personales; y,

16. Los demás establecidos en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

***Artículo 72. Obligaciones del encargado del tratamiento de datos personales*:** El encargado 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 reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;
2. Tratar datos personales de conformidad a 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, salvo que esté obligado a hacerlo en función al principio de legitimidad; de ser este el caso, deberá informar al responsable del tratamiento de datos personales;
3. Suscribir contratos de confidencialidad y manejo adecuado de datos personales con el personal a cargo del tratamiento de datos personales, o con quién tenga conocimiento de los datos personales;
4. Garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales;
5. 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;
6. 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;
7. Asistir al responsable para garantizar el cumplimiento de las obligaciones previstas en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;
8. Transferir o comunicar los datos personales entregados al responsable del tratamiento y suprimirlos, una vez que haya culminado su encargo;
9. Facilitar el acceso al responsable del tratamiento de datos personales de toda la información referente al cumplimiento de las obligaciones establecidas en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;
10. Permitir y contribuir a la realización de auditorías o inspecciones, por parte del responsable del tratamiento de datos personales o de un auditor autorizado por éste o por la Autoridad de Protección de Datos Personales;
11. Cumplir el código de protección, mecanismos de certificación o sellos aprobados para demostrar la existencia de garantías suficientes para la protección de datos personales; y,
12. Las demás establecidas en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

CAPITULO X
DE LAS QUEJAS DIRECTAS Y DE LA GESTÍON DEL PROCEDIMIENTO ADMINISTRATIVO

***Artículo 73. Queja directa del titular del dato personal al responsable del tratamiento de datos personales*:** El titular de los datos personales podrá, en cualquier momento, de forma gratuita y por medios físicos o digitales puestos a su disposición por parte del responsable del tratamiento de los datos personales, presentar quejas sobre el contenido de los derechos, principios y obligaciones para hacer efectivas de forma directa sus peticiones, en especial aquellas relacionadas al acceso, rectificación o actualización, eliminación, oposición, limitaciones al tratamiento, portabilidad, notificaciones sobre violaciones a la seguridad, transferencia internacional a terceros países, entre otros.

Presentada la queja ante el responsable, este contará con un término de cinco (5) días para contestar y notificar en debida forma sobre su respuesta afirmativa o negativa, y ejecutar lo que se le haya solicitado.

***Artículo 74. Del inicio del procedimiento administrativo*:** 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.

***Artículo 75. Reclamo administrativo ante la Autoridad de Protección de Datos Personales*:** En el caso de que el responsable del tratamiento no conteste a la queja en el término establecido en la presente ley, o, ésta fuere negativa, el titular podrá presentar el correspondiente reclamo administrativo ante la Autoridad de Protección de Datos Personales, para lo cual se estará 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 de lo antes expuesto, el titular podrá presentar acciones civiles, penales y constitucionales a las que se crea asistido.

CAPÍTULO XI
MEDIDAS CORRECTIVAS, INFRACCIONES Y RÉGIMEN SANCIONATORIO

***Artículo 76. Objeto y ámbito de aplicación*:** Los responsables, encargados del tratamiento de datos personales y de ser el caso terceros, están sujetos a medidas correctivas, infracciones y al régimen sancionatorio establecido en el presente Capítulo.

En el caso de entidades pertenecientes al sector público, las resoluciones que determinen medidas correctivas o aplicación de régimen sancionatorio, deberán ser comunicada a la máxima autoridad de la institución responsable del tratamiento de datos personales con la finalidad de que se inicien los procedimientos disciplinarios en contra de los servidores o funcionarios, por cuya acción u omisión se hubiese incurrido en alguna de las infracciones establecidas en la presente ley, sin perjuicio de la responsabilidad civil, administrativa y/o penal a la que hubiere lugar.

Artículo 77. Medidas correctivas: En caso de incumplimiento de las obligaciones previstas en la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa 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 reestablecer el derecho vulnerado y evitar 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; y,
2. La imposición de medidas técnicas, jurídicas, organizativas o administrativas tendientes a garantizar un tratamiento adecuado de datos personales.

Artículo 78. Implementación: La Autoridad de Protección de Datos Personales, en el marco de esta ley, implementará para cada caso las medidas correctivas, previo informe de la unidad técnica competente, que permita 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. Para el caso de infracciones leves se aplicará a los responsables, encargados del tratamiento de datos personales y de ser el caso terceros, únicamente medidas correctivas; en el caso de incumplimiento de dichas medidas correctivas o que éstas fueren cumplidas de forma tardía, parcial o defectuosa, la Autoridad de Protección de Datos Personales, aplicará las sanciones que corresponden a las infracciones leves establecidas en la presente ley;
2. En el caso de que los responsables, encargados del tratamiento de datos personales y de ser el caso terceros, se encuentren incursos en el presunto cometimiento de una infracción leve y éstos 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,
3. En el caso de que los responsables, encargados del tratamiento de datos personales y de ser el caso terceros, se encuentren incursos en el presunto cometimiento de una infracción 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 1a
Del responsable

Artículo 79. Infracciones leves: Se consideran infracciones leves las siguientes:

1. No tramitar, tramitar fuera del plazo previsto o negar injustificadamente las peticiones o quejas realizadas por el titular;
2. No notificar a la Autoridad de Protección de Datos Personales y al titular las vulneraciones de seguridad y protección de datos personales cuando no exista afectación a los derechos fundamentales y libertades individuales de los titulares;
3. No mantener disponibles políticas de protección de datos personales afines al tratamiento de datos personales;
4. No mantener actualizado el Registro Nacional de Protección de Datos Personales de conformidad a lo dispuesto en la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia; y,
5. Incumplir las medidas correctivas dispuestas por la Autoridad de Protección de Datos Personales.

Artículo 80. Infracciones graves: Se consideran infracciones graves las siguientes:

1. No implementar requisitos, mecanismos o herramientas administrativas, técnicas, físicas, organizativas y jurídicas a fin de garantizar que el tratamiento de datos personales se realice conforme la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;
2. Utilizar información o datos para fines distintos a los declarados;
3. No cumplir lo dispuesto en códigos de protección, mecanismos de certificación, sellos de protección, cláusulas estándar de protección de datos, cláusulas o garantías adicionales o específicas y normas vinculantes;
4. 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 normativa sobre la materia;

5. 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;
6. No realizar evaluaciones de impacto al tratamiento de datos;
7. 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 los datos personales que hayan sido identificadas;
8. No notificar a la Autoridad de Protección de Datos Personales y al titular las vulneraciones a la seguridad y protección de datos personales cuando afecte los derechos fundamentales y libertades individuales de los titulares;
9. No implementar protección de datos desde el diseño y por defecto;
10. No 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. Elegir al encargado del tratamiento de datos personales que no ofrezca garantías suficientes para hacer efectivo el ejercicio del derecho a la protección de datos personales;
12. No consignar en el Registro Nacional de Protección de Datos Personales lo dispuesto en la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;
13. No designar al Delegado de Protección de Datos Personales;
14. No permitir o no contribuir a la realización de auditorías o inspecciones, por parte del auditor acreditado por la Autoridad de Protección de Datos Personales; y,
15. El incumplimiento de las medidas correctivas o el cumplimiento de éstas de forma tardía, parcial o defectuosa; siempre y cuando hubiese precedido por dicha causa la aplicación de una sanción por infracción leve.

Sección 2ª
Del encargado

Artículo 81. Infracciones leves: Se consideran infracciones leves las siguientes:

1. 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;
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 auditorías o inspecciones, por parte del responsable del tratamiento de datos personales o de otro auditor autorizado por éste o por la Autoridad de Protección de Datos Personales; y,
4. Incumplir las medidas correctivas dispuestas por la Autoridad de Protección de Datos Personales.

***Artículo 82. Infracciones graves*:** Se consideran infracciones graves las siguientes:

1. No tratar datos personales en estricto apego a los principios y derechos desarrollados en la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa 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 de confidencialidad y manejo adecuado de datos personales con el personal a cargo del tratamiento de datos personales, o quién 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 efecto 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. No cumplir lo dispuesto en códigos de protección, mecanismos de certificación, sellos de protección, cláusulas estándar de protección de datos, cláusulas o garantías adicionales o específicas y normas vinculantes;
8. 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 normativa sobre la materia; y,
9. El incumplimiento de las medidas correctivas o el cumplimiento de éstas de forma tardía, parcial o defectuosa; siempre y cuando hubiese precedido por dicha causa la aplicación de una sanción por infracción leve.

***Artículo 83. 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. Los 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, encargado del tratamiento de datos personales y/o de ser el caso un tercero, es una entidad de Derecho Privado o una Empresa Pública se aplicará una multa de entre el 3% y el 9% calculada sobre su volumen de negocio, correspondiente al ejercicio económico 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, encargado del tratamiento de datos personales y/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.

***Artículo 84. Sanciones por infracciones graves*:** La Autoridad de Protección de Datos Personales 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. 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 sancionado con una multa de entre diez (10) a veinte (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.

2. Si el responsable, encargado del tratamiento de datos personales y/o de ser el caso un tercero, es una entidad de Derecho Privado o una Empresa Pública se aplicará una multa de entre el 10% y el 17% calculada sobre su volumen de negocio, correspondiente al ejercicio económico 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, encargado del tratamiento de datos personales y/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.

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

***Artículo 85. Sanciones por infracciones graves*:** La Autoridad de Protección de Datos Personales 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. 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 sancionado 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.
2. Si el responsable, encargado del tratamiento de datos personales y/o de ser el caso un tercero, es una entidad de Derecho Privado o una Empresa Pública se aplicará una multa de entre el 10% y el 17% calculada sobre su volumen de negocio, correspondiente al ejercicio económico 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, encargado del tratamiento de datos personales y/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.

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

***Artículo 86. 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 sobre el valor agregado y de otros impuestos directamente relacionados con la operación económica.

Artículo 87. 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 XI
AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES

Artículo 88. Autoridad de Protección de Datos Personales: La Autoridad de Protección de Datos Personales será una entidad de derecho público dependiente de la Función Ejecutiva con personería jurídica y gozará de autonomía administrativa y financiera.

Artículo 89. Funciones, atribuciones y facultades: Corresponden a la Autoridad de Protección de Datos Personales 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 y de las entidades certificadoras, de conformidad a lo establecido en la presente Ley, su reglamento de aplicación y demás normativa emitida por la Autoridad de Protección de Datos Personales;
2. Conocer sobre los proyectos de normas de carácter general o técnico que se desarrollen en materia de protección de datos personales;
3. Emitir normativa general o técnica, criterios y demás actos que sean necesarios para el ejercicio de sus competencias y garantizar el ejercicio del derecho a la protección de datos personales;
4. Promover proyectos de ley o reformas en materia de protección de datos personales;
5. Autorizar y revocar la autorización de funcionamiento de entidades certificadoras, conforme a los presupuestos establecidos en la normativa emitida para dicha finalidad y elaborar el modelo de gestión correspondiente;
6. Revisar, aprobar, rechazar, revocar y exigir la modificación de códigos de protección, mecanismos de certificación o sellos de protección de datos personales, conforme a los presupuestos establecidos en la normativa emitida para dicha finalidad y elaborar el modelo de gestión correspondiente;
7. Revocar las certificaciones o sellos de protección en materia de datos personales, conforme a los presupuestos establecidos en la normativa emitida para dicha finalidad y elaborar el modelo de gestión correspondiente;

8. Promover una coordinación adecuada y eficaz con entidades de certificación o agentes privados encargados de la rendición de cuentas, y participar en iniciativas internacionales y regionales para la protección de la protección de los datos personales;
9. Dictar las cláusulas estándar de protección de datos, así como verificar el contenido de las cláusulas o garantías adicionales o específicas;
10. Conocer, sustanciar y resolver los reclamos interpuestos por el titular o aquellos iniciados de oficio; así como aplicar las sanciones correspondientes;
11. Atender consultas en materia de protección de datos personales;
12. Promover e incentivar el ejercicio del derecho a la protección de datos personales;
13. Ejercer el control y emitir las resoluciones de autorización para la transferencia internacional de datos;
14. Coordinar con otros organismos del sector público y privado los esfuerzos para formular y aplicar planes y políticas destinados a fortalecer la protección de datos personales;
15. Ejercer la representación internacional en materia de protección de datos personales;
16. Coordinar, promover y ejecutar programas de cooperación con organismos internacionales análogos en materia de protección de datos personales, así como con unidades nacionales relacionadas, dentro del marco de sus competencias; y ejecutar acciones conjuntas a través de convenios de cooperación nacional o internacional;
17. Prestar asistencia en asuntos relacionados con la protección de datos personales a petición de un organismo nacional o internacional, de una entidad pública o privada;
18. Emitir directrices para el diseño y contenido de la política de tratamiento de datos personales;
19. Establecer directrices para el análisis, evaluación y selección de medidas de seguridad de los datos personales;
20. Llevar un registro estadístico sobre vulneraciones a la seguridad de datos personales e identificar posibles medidas de seguridad para cada una de ellas;
21. Solicitar información sobre su gestión a responsables, encargados y entidades de certificación para el cumplimiento de sus funciones de control y demás atribuciones establecidas en la presente ley;
22. Realizar o delegar auditorías técnicas al tratamiento de datos personales de conformidad a lo establecido en la presente Ley, su reglamento de aplicación y demás normativa emitida por la Autoridad de Protección de Datos Personales;
23. Solicitar y recabar información para el análisis y elaboración de estudios en materia de protección de datos personales;
24. Publicar periódicamente una guía de la normativa relativa a la protección de datos personales;
25. Ejercer la potestad sancionadora respecto de responsables, encargados, terceros y entidades de certificación, conforme a lo establecido en la presente ley;
26. 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;
27. Promover la concientización en las personas y la compresión 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 prioritaria, tales como niñas, niños y adolescentes;
28. Compartir con organismos internacionales análogos en materia de protección de datos personales, así como con entidades nacionales e internacionales de control o fiscalización de índole administrativa o judicial: (i) informes, (ii) información; o (iii) datos personales relacionados a procesos de investigación, en el marco de sus competencias y de conformidad con la normativa aplicable, sin que dicha transferencia constituya una vulneración al principio de confidencialidad al constituir parte de la cadena de custodia, con la finalidad exclusiva de realizar el análisis, investigación y toma de acciones legales, judiciales y las demás que fueren pertinentes, pudiendo ser además utilizada como instrumento probatorio;
29. 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,

30. Las demás atribuciones establecidas en la normativa vigente.

Artículo 90. Registro Nacional de Protección de Datos Personales: El responsable del tratamiento de datos personales deberá reportar a la Autoridad de Protección de Datos, lo siguiente:

1. Identificación de la base de datos o del tratamiento;
2. El nombre, domicilio legal y datos de contactabilidad 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 contactabilidad de los destinatarios;
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, físicas, organizativas y jurídicas implementadas para garantizar la seguridad y protección de datos personales;
9. Tiempo de conservación de los datos;
10. Transferencias internacionales;
11. Constancia de la existencia de códigos de conducta; y,
12. 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 personales, los trate con fines y características distintas a las declaradas en el registro o contrarias a la ley y normativa especializada en la materia.

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 el 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 público y privado para el efectivo funcionamiento del Registro Nacional de Protección de Datos Personales.

Quinta: La Autoridad de Protección de Datos Personales será responsable de presentar informes bianuales 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, estadísticos, 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 sancionatorio.

DISPOSICIONES TRANSITORIAS

Primera: Las medidas correctivas y el régimen sancionatorio se aplicarán dentro de dos años contados a partir de la entrada en vigencia de la presente Ley, sin perjuicio de que en el transcurso de este tiempo los responsables y encargados del tratamiento se adecuen a los preceptos establecidos dentro de esta norma, su reglamento de aplicación y demás normativa emitida por la Autoridad de Protección de Datos Personales.

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 del plazo señalado en la Disposición Final 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. Suprímase las definiciones de intimidad, datos personales, datos personales autorizados del glosario de términos establecido en la Disposición General Novena.

2. Sustitúyase el texto del artículo 32 por el siguiente: "Art. 32.- Protección de datos por parte de las entidades de certificación de información acreditadas.- Las entidades de certificación de información garantizarán la protección de los datos personales conforme a los presupuestos establecidos en la Ley Orgánica de Protección de Datos Personales, su reglamento de aplicación y demás normativa emitida por la Autoridad de Protección de Datos Personales".

Segunda: Suprímase el inciso segundo del artículo 21 del Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicado en el Registro Oficial 735 del 31 de diciembre de 2002.

Tercera: 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. Sustitúyase:

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 dato público registral 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, sólo 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. Incorpórese:

a) En el artículo 31 referente a las atribuciones y facultades de la Dirección Nacional de Registros Públicos antes del numeral 14 el 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. Suprímase del numeral 13 del artículo 31 lo siguiente: "y,".

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

Cuarta: En el Reglamento a la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos publicado en el suplemento del Registro Oficial 718 del 23 de marzo del 2016:

Sustitúyase:

1. El término Dirección Nacional de Registros de Datos Públicos por Dirección Nacional de Registros Públicos;

2. El término Sistema Nacional de Registro de Datos Públicos por Sistema Nacional de Registros Públicos;

3. El término Registro de Datos Públicos por Registros Públicos;

4. El término datos de carácter personal por datos personales; y

5. El término dato público registral por la expresión datos públicos y datos personales registrables.

Incorpórese:

En la Disposición General Séptima el siguiente inciso final: "La definición de términos relacionados con el derecho a la protección de datos personales estará conforme a lo establecido en la ley de la materia."

Quinta: 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 de 2016, sustitúyase la palabra confidencialidad por protección en el numeral 5 del artículo 67.

Sexta: En la Ley Orgánica de Telecomunicaciones, publicada en el tercer suplemento del Registro Oficial 439 del 18 de febrero de 2015:

1. Suprímase:
   a) El inciso, segundo, tercer y cuarto del artículo 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 personales (…)"

2. Sustitúyase:

   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 personales, 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 se 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 clara 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: Cuando 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 seguridad 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.

Séptima: En el Reglamento a la Ley Orgánica de Telecomunicaciones, publicado en el suplemento del Registro Oficial 676 del 25 de enero de 2016 sustitúyase:

1. El artículo 120, por el siguiente:

Art. 120. Protección de datos personales: Los prestadores de servicios del régimen general de telecomunicaciones tienen prohibido ejecutar u omitir acciones que violen la garantía de protección de datos personales, como por ejemplo, provocar la destrucción, la pérdida, la alteración, la revelación o el acceso no autorizado de datos personales, transmitidos, almacenados o tratados en la prestación de servicios de telecomunicaciones, conforme el alcance, los procedimientos o protocolos previstos en la Ley Orgánica de Protección de Datos Personales, su Reglamento y las resoluciones emitidas por la

Autoridad de Protección de Datos Personales, para el efecto. La violación de esta garantía dará lugar a la imposición de las sanciones previstas en el ordenamiento jurídico.

2. El artículo 121, por el siguiente:

Art. 121. Uso comercial: Los datos personales que los usuarios proporcionen a los prestadores de servicios del régimen general de telecomunicaciones no podrán ser usados para la promoción comercial de servicios o productos, inclusive de la propia operadora; salvo consentimiento del usuario, de conformidad con lo establecido en la Ley Orgánica de Protección de Datos Personales.

Para tal fin, los prestadores de servicios deberán solicitar a sus usuarios su consentimiento, conforme lo establece la Ley Orgánica de Protección de Datos Personales, en un instrumento separado y distinto al contrato de prestación de servicios a través de medios físicos o electrónicos, para que la prestadora de servicios del régimen general de telecomunicaciones pueda utilizar comercialmente sus datos personales. Dicho instrumento debe contener lo determinado en la Ley Orgánica de Protección de Datos Personales, su Reglamento o las resoluciones que su Autoridad de Protección de Datos Personales, dicte para el efecto. Sin perjuicio de lo anterior se considerarán públicos los datos contenidos en las guías telefónicas de telefonía fija, no obstante lo cual los abonados tendrán derecho a que se excluyan gratuitamente sus datos personales de dichas guías.

La ARCOTEL establecerá los mecanismos y emitirá las regulaciones correspondientes a fin de precautelar el secreto de las comunicaciones y de la información que se trasmite a través de redes de telecomunicaciones, así como la seguridad de las redes.

Octava: Sustitúyase del Capítulo III, del Título XIII, del Libro I, de la Resolución No. SB-2017-810, de 31 de Octubre 2017, que Codifica las Normas de la Superintendencia de Bancos:

El artículo 14, literal b por el siguiente: Las entidades financieras al tratar datos personales deberán apegarse a lo previsto en la Ley Orgánica de Protección de Datos Personales, su respectivo reglamento y la normativa especializada emanada por la Autoridad de Protección de Datos Personales que dicte para el efecto.

DISPOSICIONES DEROGATORIAS

Primera: Deróguese el artículo 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: Deróguese 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: Deróguese el artículo 5 de 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.

Cuarta: Deróguense los artículos 11 y 12 y los numerales 2, 3, 4, 5, 8, 10, 11, y 12 de la Disposición General Séptima del Reglamento a la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos publicado en el suplemento del Registro Oficial 718 del 23 de marzo del 2016.

Quinta: Quedan así mismo derogadas todas aquellas disposiciones de igual o menor jerarquía que se contrapongan con la presente Ley Orgánica.