

LEY ORGÁNICA DE PROTECCION DE DATOS PERSONALES

SUPLEMENTO REGISTRO OFICIAL No. 459 DE 26 DE MAYO DE 2021

La Asamblea Nacional del Ecuador, en sesión virtual No. 707 del 10 de mayo de 2021, aprobó el proyecto de Ley. Dicho proyecto fue sancionado por el ex Presidente de la República del Ecuador, el 21 de mayo de 2021.

Esta ley orgánica, ha sido motivada para el cumplimiento del derecho a la protección de datos personales garantizado en la Constitución de la República del Ecuador; en uno de los ejes de la Estrategia acordada en el año 2016 de la red Iberoamericana de Datos Personales 2020; en los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, aprobados el 20 de junio de 2017; en la propuesta de declaración de principios de privacidad y protección de datos personales en las Américas, adoptado por el Comité Jurídico de la Organización de Estados Americanos; en el Proyecto de Ley Modelo sobre Protección de datos Personales, desarrollado por la Organización de Estados Americanos el 27 de marzo de 2015; en el Libro Blanco de la Sociedad de la Información y del Conocimiento 2018; en 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*"; en el principio de Legalidad de la Carta Iberoamericana de Gobierno Electrónico del año 2007, con el objetivo de precautelar el derecho que tienen los ciudadanos a relacionarse electrónicamente con el Estado; y, en 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"

Contiene aspectos relevantes como los exponemos a continuación:

OBJETO Y FINALIDAD

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

AMBITO

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

- a) Personas naturales que utilicen estos datos en la realización de actividades familiares o domésticas;
- b) Personas fallecidas, sin perjuicio de lo establecido en el artículo 28 de la presente Ley;
- c) Datos anonimizados, en tanto no sea posible identificar a su titular. Tan pronto los datos dejen de estar disociados o de ser anónimos, su tratamiento estará sujeto al cumplimiento de las obligaciones de esta ley, especialmente la de contar con una base de licitud para continuar tratando los datos de manera no anonimizada o disociada;
- d) Actividades periodísticas y otros contenidos editoriales;

- e) Datos personales cuyo tratamiento se encuentre regulado en normativa especializada de igual o mayor jerarquía en materia de gestión de riesgos por desastres naturales; y, seguridad y defensa del Estado, en cualquiera de estos casos deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y a los principios de esta ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad;
- f) Datos o bases de datos establecidos para la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, llevado a cabo por los organismos estatales competentes en cumplimiento de sus funciones legales. En cualquiera de estos casos deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y a los principios de esta ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad; y
- g) Datos que identifican o hacen identificable a personas jurídicas.

Son accesibles al público y susceptibles de tratamiento los datos personales referentes al contacto de profesionales y los datos de comerciantes, representantes y socios y accionistas de personas jurídicas y servidores públicos, siempre y cuando se refieran al ejercicio de su profesión, oficio, giro de negocio, competencias, facultades, atribuciones o cargo y se trate de nombres y apellidos, funciones o puestos desempeñados, dirección postal o electrónica, y, número de teléfono profesional. En el caso de los servidores públicos, además serán de acceso público y susceptibles de tratamiento de datos, el histórico y vigente de la declaración patrimonial y de su remuneración.

Art. 3.- Ámbito de aplicación territorial. - Sin perjuicio de la normativa establecida en los instrumentos internacionales ratificados por el Estado ecuatoriano que versen sobre esta materia, se aplicará la presente Ley cuando;

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

TERMINOS Y DEFINICIONES PRINCIPALES

La ley contempla definiciones para su aplicación, entre ellas:

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

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

Datos sensibles: Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud,

datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.

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

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

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

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

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

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

Titular: Persona natural cuyos datos son objeto de tratamiento.

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

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

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

INTEGRANTES DEL SISTEMA DE PROTECCIÓN DE DATOS PERSONALES

<p>Son parte del sistema de protección de datos personales, los siguientes:</p> <ol style="list-style-type: none"> 1) Titular; 2) Responsable del tratamiento; 3) Encargado del tratamiento, 4) Destinatario; 5) Autoridad de Protección de Datos Personales; y, 6) Delegado de protección de datos personales.
<p>NORMAS APLICABLES AL EJERCICIO DE DERECHOS</p>
<p>El ejercicio de los derechos previstos en esta Ley se canalizará a través del responsable del tratamiento, Autoridad de Protección de Datos Personales o jueces competentes, de conformidad con el procedimiento establecido en la presente Ley y su respectivo Reglamento de aplicación. El Reglamento a esta Ley u otra norma secundaria no podrán limitar al ejercicio de los derechos.</p>
<p>TRATAMIENTO LEGÍTIMO DE DATOS DE PERSONAS</p>
<p>El tratamiento será legítimo y lícito si se cumple con alguna de las condiciones previstas en la Ley entre ellas:</p> <ol style="list-style-type: none"> 1) Por consentimiento del titular para el tratamiento de sus datos personales, para una o varias finalidades específicas; 2) Que sea realizado por el responsable del tratamiento en cumplimiento de una obligación legal; 3) Que sea realizado por el responsable del tratamiento, por orden judicial, debiendo observarse los principios de la presente ley; 4) Que el tratamiento de datos personales se sustente en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, derivados de una competencia atribuida por una norma con rango de ley, sujeto al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta ley y a los criterios de legalidad, proporcionalidad y necesidad; 5) Para la ejecución de medidas precontractuales a petición del titular o para el cumplimiento de obligaciones contractuales perseguidas por el responsable del tratamiento de datos personales, encargado del tratamiento de datos personales o por un tercero legalmente habilitado; 6) Para proteger intereses vitales, del interesado o de otra persona natural, como su vida, salud o integridad, 7) Para tratamiento de datos personales que consten en bases de datos de acceso público; u, 8) Para satisfacer un interés legítimo del responsable de tratamiento o de tercero, siempre que no prevalezca el interés o derechos fundamentales de los titulares al amparo de lo dispuesto en esta norma.
<p>CONSENTIMIENTO</p>
<p>Se podrán tratar y comunicar datos personales cuando se cuente con la manifestación de la voluntad del titular para hacerlo. El consentimiento será válido, cuando la manifestación de la voluntad sea:</p>

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

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

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

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

INTERÉS LEGÍTIMO

Cuando el tratamiento de datos personales tiene como fundamento el interés legítimo:

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

PRINCIPIOS

Sin perjuicio de otros principios establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, la presente Ley se regirá por los principios de:

- a) Juridicidad
- b) Lealtad
- c) Transparencia
- d) Finalidad
- e) Pertinencia y minimización de datos personales
- f) Proporcionalidad del tratamiento
- g) Confidencialidad
- h) Calidad y exactitud
- g) Conservación
- j) Seguridad de datos personales
- k) Responsabilidad proactiva y demostrada
- l) Aplicación favorable al titular
- m) Independencia del control

DERECHOS
<p>Normativa especializada</p> <p>Derecho a la información</p> <p>Derecho de acceso</p> <p>Derecho de rectificación y actualización</p> <p>Derecho de eliminación</p> <p>Derecho de oposición</p> <p>Derecho a la portabilidad</p> <p>Derecho a la suspensión del tratamiento</p> <p>Derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas</p> <p>Derecho de niñas, niños y adolescentes a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas</p> <p>Derecho de consulta</p> <p>Derecho a la educación digital</p>
EXCEPCIONES A LOS DERECHOS DE RECTIFICACIÓN, ACTUALIZACIÓN, ELIMINACIÓN, OPOSICIÓN, ANULACIÓN Y PORTABILIDAD.
<p>Se fija en la ley orgánica, excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad. No proceden los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad.</p>
EJERCICIO DE DERECHOS
<p>El Estado, entidades educativas, organizaciones de la sociedad civil, proveedores de servicios de la sociedad de la información y el conocimiento, y otros entes relacionados, dentro del ámbito de sus relaciones, están obligados a proveer información y capacitación relacionadas con el uso y tratamiento responsable, adecuado y seguro de datos personales de niñas, niños y adolescentes, tanto a sus titulares como a sus representantes legales, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales.</p> <p>Los adolescentes mayores de doce (12) años y menores de quince (15) años, así como las niñas y niños, para el ejercicio de sus derechos necesitarán de su representante legal. Los adolescentes mayores de quince (15) años y menores de dieciocho (18) años, podrán ejercerlos de forma directa ante la Autoridad de Protección de Datos Personales o ante el responsable de la base de datos personales del tratamiento.</p> <p>Los derechos del titular son irrenunciables. Será nula toda estipulación en contrario</p>
CATEGORIAS
<p>Se considerarán categorías especiales de datos personales, los siguientes:</p> <p>a) Datos sensibles;</p> <p>b) Datos de niñas, niños y adolescentes;</p> <p>c) Datos de salud; y,</p> <p>d) Datos de personas con discapacidad y de sus sustitutos, relativos a la discapacidad.</p>
TRATAMIENTO DE DATOS SENSIBLES

Queda prohibido el tratamiento de datos personales sensibles salvo que concurra alguna de las siguientes circunstancias:

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

DATOS PERSONALES DE PERSONAS FALLECIDAS

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

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

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

DATOS CREDITICIOS

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

La protección de datos personales crediticios se sujetará a lo previsto en la presente ley, en la

legislación especializada sobre la materia y demás normativa dictada por la Autoridad de Protección de Datos Personales.

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

DATOS RELATIVOS A LA SALUD

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

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

TRATAMIENTO DE DATOS RELATIVOS A LA SALUD

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

TRANSFERENCIA O COMUNICACIÓN Y ACCESO A DATOS PERSONALES POR TERCEROS

Los datos personales podrán transferirse o comunicarse a terceros cuando se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del responsable y del destinatario, cuando la transferencia se encuentre configurada dentro de una de las causales de legitimidad establecidas en esta Ley, y se cuente, además, con el consentimiento del titular.

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

ACCESO DE DATOS PERSONALES POR PARTE DEL ENCARGADO

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

El tratamiento de datos personales realizado por el encargado deberá estar regulado por un contrato, en el que se establezca de manera clara y precisa que el encargado del tratamiento

de datos personales tratará únicamente los mismos conforme las instrucciones del responsable y que no los utilizará para finalidades diferentes a las señaladas en el contrato, ni que los transferirá o comunicará ni siquiera para su conservación a otras personas.

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

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

ACCESO DE DATOS PERSONALES POR PARTE DE TERCEROS

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

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

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

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

EXCEPCIONES DE CONSENTIMIENTO PARA LA TRANSFERENCIA O COMUNICACIÓN DE DATOS PERSONALES

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

- 1) Cuando los datos han sido recogidos de fuentes accesibles al público;
- 2) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica entre el responsable de tratamiento y el titular, cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con base de datos. En este caso la transferencia o comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique;
- 3) Cuando los datos personales deban proporcionarse a autoridades administrativas o judiciales en virtud de solicitudes y órdenes amparadas en competencias atribuidas en la norma vigente;
- 4) Cuando la comunicación se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando dichos datos se encuentren debidamente dissociados o a lo menos anonimizados, y,
- 5) Cuando la comunicación de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que implique intereses vitales de su titular y este se encontrare impedido de otorgar su consentimiento.

6) Cuando la comunicación de datos de carácter personal relativos a la salud sea necesaria para realizar los estudios epidemiológicos de interés público, dando cumplimiento a los estándares internacionales en la materia de derechos humanos, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad. El tratamiento deberá ser de preferencia anonimizado, y en todo caso agregado» una vez pasada la urgencia de interés público.

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

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

SEGURIDAD DE DATOS PERSONALES

Seguridad de datos personales. - El responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos,

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

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

MEDIDAS DE SEGURIDAD EN EL ÁMBITO DEL SECTOR PÚBLICO

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

PROTECCION DE DATOS PERSONALES DESDE EL DISEÑO Y POR DEFECTO

Se entiende a la protección de datos desde el diseño como el deber del responsable del tratamiento de tener en cuenta, en las primeras fases de concepción y diseño del proyecto, que determinados tipos de tratamientos de datos personales entrañan una serie de riesgos

para los derechos de los titulares en atención al estado de la técnica, naturaleza y fines del tratamiento, para lo cual, implementará las medidas técnicas, organizativas y de cualquier otra índole, con miras a garantizar el cumplimiento de las obligaciones en materia de protección de datos, en los términos del reglamento.

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

ANÁLISIS DE RIESGO, AMENAZAS Y VULNERABILIDADES

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

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

DETERMINACION DE MEDIDAS DE SEGURIDAD APLICABLES

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

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

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

EVALUACION DE IMPACTO DEL TRATAMIENTO DE DATOS PERSONALES

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

NOTIFICACION DE VULNERACION DE SEGURIDAD

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

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

ACCESO DE DATOS PERSONALES PARA ATENCIÓN DE EMERGENCIAS E INCIDENTES INFORMÁTICOS

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

GARANTÍA DEL SECRETO DE LAS COMUNICACIONES Y SEGURIDAD DE DATOS PERSONALES

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

NOTIFICACIÓN DE VULNERACIÓN DE SEGURIDAD AL TITULAR

El responsable del tratamiento deberá notificar sin dilación la vulneración de seguridad de datos personales al titular cuando conlleve un riesgo a sus derechos fundamentales y libertades individuales, dentro del término de tres días contados a partir de la fecha en la que tuvo conocimiento del riesgo.

OBLIGACIONES DEL RESPONSABLE Y ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES

El responsable del tratamiento de datos personales está obligado a:

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

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

DELEGADO DE PROTECCION DE DATOS PERSONALES

Se designará un delegado de protección de datos personales en los siguientes casos:

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

La Autoridad de Protección de Datos Personales podrá definir nuevas condiciones en las que deba designarse un delegado de protección de datos personales y emitirá, a dicho efecto, las directrices suficientes para su designación.

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

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

En caso de incumplimiento de sus funciones, el delegado de protección de datos personales responderá administrativa, civil y penalmente, de conformidad con la ley.

REGISTRO NACIONAL DE PROTECCIÓN DE DATOS PERSONALES

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

- 1) Identificación de la base de datos o del tratamiento;
- 2) El nombre domicilio legal y datos de contacto del responsable y encargado del tratamiento de datos personales;
- 3) Características y finalidad del tratamiento de datos personales;
- 4) Naturaleza de los datos personales tratados;
- 5) Identificación, nombre, domicilio legal y datos de contacto de los destinatarios de los datos personales, incluyendo encargados y terceros;

- 6) Modo de interrelacionar la información registrada;
- 7) Medios utilizados para implementar los principios, derechos y obligaciones contenidas en la presente ley y normativa especializada;
- 8) Requisitos y herramientas administrativas técnicas y físicas, organizativas y jurídicas implementadas para garantizar la seguridad y protección de datos personales;
- 9) Tiempo de conservación de los datos,

DE LA RESPONSABILIDAD PROACTIVA

Autorregulación
Códigos de conducta
Entidades de Certificación

TRANSFERENCIA O COMUNICACIÓN INTERNACIONAL DE DATOS PERSONALES

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,

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

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, las cuales deberán cumplir las condiciones determinadas en la ley orgánica.

AUTORIZACIÓN PARA TRANSFERENCIA INTERNACIONAL

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

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

CASOS EXCEPCIONALES DE TRANSFERENCIAS O COMUNICACIONES INTERNACIONALES

La ley orgánica prevé excepciones para realizar transferencias o comunicaciones internacionales de datos personales.

CONTROL CONTÍNUO

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] a presente Ley, la Autoridad de Protección de Datos Personales procederá a emitir la correspondiente resolución de no adecuación, a partir de la cual no procederán transferencias de datos personales, salvo que operen otros mecanismos de transferencia conforme lo dispuesto en el presente capítulo.

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

DE LOS REQUERIMIENTOS DIRECTOS Y DE LA GESTIÓN DEL PROCEDIMIENTO ADMINISTRATIVO

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

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

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

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

MEDIDAS CORRECTIVAS, INFRACCIONES Y RÉGIMEN SANCIONATORIO

En caso de incumplimiento de las disposiciones previstas en la presente Ley, su reglamento, directrices y lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia, o transgresión a los derechos y principios que componen al derecho a la protección de datos personales, la Autoridad de Protección de Datos Personales dictará medidas correctivas con el objeto de evitar que se siga cometiendo la infracción y que la conducta se produzca nuevamente, sin perjuicio de la aplicación de las correspondientes sanciones administrativas.

Las medidas correctivas podrán consistir, entre otras, en:

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

DE LAS INFRACCIONES DEL RESPONSABLE DE PROTECCIÓN DE DATOS

Se consideran infracciones leves las siguientes:

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

Se consideran infracciones graves las siguientes:

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

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

DE LAS INFRACIONES DEL ENCARGADO DE PROTECCIÓN DE DATOS

Se consideran infracciones leves las siguientes:

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

Se consideran infracciones graves las siguientes:

- 1) Realizar tratamientos de datos personales sin observar los principios y derechos desarrollados en la presente Ley y su reglamento, directrices y lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y-normativas sobre la materia;
- 2) No tratar datos personales de conformidad con lo previsto en el contrato que mantenga con el responsable del tratamiento de datos personales inclusive en lo que respecta a la transferencia o comunicación internacional;
- 3) No suscribir contratos que. contengan cláusulas de confidencialidad y tratamiento adecuado de datos personales con el personal a cargo del tratamiento de datos personales o quien tenga conocimiento de los datos personales;

- 4) No implementar mecanismos destinados a mantener la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales;
- 5) No implementar medidas preventivas y correctivas en la seguridad de los datos personales a fin de evitar vulneraciones;
- 6) No suprimir los datos personales transferidos o comunicados al responsable del tratamiento de los datos personales, una vez haya culminado su encargo;
- 7) Proceder a la comunicación de datos personales sin cumplir con los requisitos y procedimientos establecidos en la presente ley, su reglamento directrices lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia;
- 8) Incumplir las medidas correctivas o cumplirlas de forma, tardía parcial o defectuosa, siempre y cuando hubiese precedido por dicha causa la aplicación de una sanción por infracción leve; y.
- 9) No notificar al responsable del tratamiento de datos personales sobre cualquier vulneración de la seguridad de datos personales conforme dispone esta ley o hacerlo con retraso injustificado.

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

1. Servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones leves establecidas en la presente ley, serán sancionados con una multa de uno (1) a diez (10) salarios básicos unificados del trabajador en general, sin perjuicio de la responsabilidad extracontractual del Estado, la cual se sujetará a las reglas establecidas en la normativa correspondiente;
2. Si el responsable o el encargado del tratamiento de datos personales o de ser el caso un tercero es una entidad de derecho privado o una empresa pública, se aplicará una multa de entre el 0.1% y el 0.7% calculada sobre su volumen de negocio correspondiente al ejercicio 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, el encargado del tratamiento de datos personales o de ser el caso un tercero, hubiese sido previamente sancionado por dos o más infracciones precedentes, que establezcan sanciones de menor gravedad a la que se pretende aplicar; o cuando hubiesen sido previamente sancionados por una infracción cuya sanción sea de igual o mayor gravedad a la que se pretende aplicar;
 - c) La naturaleza del perjuicio ocasionado, es decir, las consecuencias lesivas para el ejercicio del derecho a la protección de datos personales, y,
 - d) Reincidencia, es decir, cuando la infracción precedente sea de la misma naturaleza de aquella que se pretende sancionar.

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

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

la Responsabilidad Extracontractual del Estado, la cual se sujetará a las reglas establecidas en la normativa correspondiente;

1) Si el responsable, encargado del tratamiento de datos personales o de ser el caso un tercero, es una entidad de derecho privado o una empresa pública se aplicará una multa de entre el 0.7% y el 1% calculada sobre su volumen de negocios, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa. La Autoridad de Protección de Datos Personales establecerá la 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 o de ser el caso, de un tercero hubiese sido previamente sancionado por dos o más infracciones precedentes que establezcan sanciones de menor gravedad a la que se pretende aplicar; o cuando hubiesen sido previamente sancionados por una infracción cuya sanción sea de igual o mayor gravedad a la que se pretende aplicar;
- c) La naturaleza del perjuicio ocasionado, es decir, las consecuencias lesivas para el ejercicio del derecho a la protección de datos personales; y,
- d) Reincidencia, es decir, cuando la infracción precedente sea de la misma naturaleza de aquella que se pretende sancionar.

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

Volumen de negocio. - A efectos del régimen sancionatorio de la presente ley, se entiende por volumen de negocio, a la cuantía resultante de la venta de productos y de la prestación de servicios realizados por operadores económicos, durante el último ejercicio que corresponda a sus actividades, previa deducción del Impuesto al Valor Agregado y de otros impuestos directamente relacionados con la operación económica.

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.

AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES

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

Funciones atribuciones y facultades. - La Autoridad de Protección de Datos Personales es el órgano de control y vigilancia encargado de garantizar a todos los ciudadanos la protección de sus datos personales, y de realizar todas las acciones necesarias para que se respeten los

principios, derechos, garantías y procedimientos previstos en la presente Ley y en su reglamento de aplicación, para lo cual le corresponde las funciones, atribuciones y facultades; previstas en la ley orgánica.

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

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

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

DISPOSICIONES TRANSITORIAS

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

Segunda. - Todo tratamiento realizado previo a la entrada en vigencia de la presente Ley deberá adecuarse a lo previsto en la presente norma dentro del plazo de dos años contados a partir de su publicación en el Registro Oficial.

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

Tercera. - Los responsables y encargados del tratamiento de datos personales que hayan implementado los preceptos recogidos dentro de esta Ley antes de plazo señalado en la Disposición Transitoria Primera obtendrán un reconocimiento por buenas prácticas por parte de la Autoridad de Protección de Datos Personales,

Cuarta. - La transferencia internacional de datos personales que hubiere sido realizada antes de la entrada en vigencia de la presente Ley será legítima, sin perjuicio de que el responsable del tratamiento de datos personales deba aplicar lo dispuesto en esta norma para acreditar su responsabilidad proactiva y demostrada.

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

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

DISPOSICIÓN FINAL

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

IMPACTOS DE LA LEY ORGANICA DE PROTECCION DE DATOS PERSONALES PARA EL SISTEMA DE SEGURO PRIVADO

Ecuador necesitaba contar de urgencia con una ley de protección de datos personales que regule la manera como las instituciones nacionales y extranjeras tratan, procesan, conservan, y utilizan comercialmente los datos personales de las personas naturales en Ecuador. Nuestro país debe cumplir con estándares mínimos, para llegar a ser considerado como un país confiable para la transferencia de datos.

Esta Ley Orgánica tiene como objetivo fundamental, garantizar el ejercicio de la protección de datos personales, de todos los ciudadanos, y para el cumplimiento de esta protección la ley involucra como integrantes del sistema de protección de datos, al titular, responsable del tratamiento, encargado del tratamiento, destinatario, autoridad de protección de datos personales y delegado de protección de datos.

En consecuencia, las actividades que realiza el sistema de seguro privado, integrado por las compañías de seguros, compañías de reaseguros, asesores productores de seguros, peritos de seguros e intermediarios de reaseguros, son parte de este nuevo Sistema de Protección de Datos.

Dentro de este sistema, las entidades del sistema de seguros privados en virtud de sus actividades, manejan datos personales muy sensibles, cuyo tratamiento se encuentra regulado mediante esta ley orgánica; por lo que deben establecer los mecanismos cruciales de protección de datos personales.

En primer lugar, en cuanto al consentimiento del titular de los datos, **DEBE SER VOLUNTARIO, LIBRE, ESPECÍFICO E INFORMADO E INEQUÍVOCO EN CUALQUIER MOMENTO**. Asimismo, los ciudadanos pueden solicitar todos los datos que una compañía tiene de ellos en un formato adecuado y que el ciudadano puede entregar posteriormente a otra empresa, si lo desea mediante el ejercicio del denominado derecho a la portabilidad de los datos.

Por otra parte, la nueva ley orgánica de protección de datos, implica que la información recopilada en grandes cantidades, deberá establecer una nueva forma de relacionarse con sus clientes en lo que se refiere a los datos personales. Para lo cual las empresas entre ellas las que pertenecen al sistema de seguros privado, deben realizar cambios amplios y fundamentales como la forma en que organizan la información. Por ello, algunos de los cambios más inmediatos y visibles pasarán por una redefinición de los Términos de Servicio.

Lo anterior considerando que el cliente es propietario de sus datos y solo se los puede usar con su consentimiento.

En segundo lugar, las sanciones que impone la ley orgánica de protección de datos, son importantes y se encuentran catalogadas como infracciones leves y graves, para las infracciones leves las multas corresponden del 0,1 a 0,07 % del volumen de negocio anual para las empresas públicas y privadas, y para las infracciones graves, la multa corresponderá del 0.7 al 1% del volumen de negocio anual para las empresas públicas y privadas.

Conforme las disposiciones transitorias de esta ley, la misma entrará en plena vigencia en dos años a partir de su publicación en el Registro Oficial, debiéndose en este mismo plazo adecuarse todo procedimiento realizado, con anterioridad a la entrada en vigencia de esta ley,

Para el efecto, deberá expedirse el Reglamento correspondiente, y la normativa para cada una de las actividades. En este caso para las entidades del sistema de seguro privado, regulada por la Junta de Política y Regulación Financiera y Controlada por la Superintendencia de Compañías, Valores y Seguros.

Por lo anterior, hay mucho trabajo por realizar para todos quienes integran el nuevo Sistema de Protección de Datos Personales.

Respecto a las oportunidades para el sector asegurador, considero que por el riesgo que tienen las empresas privadas y entidades públicas que por el giro de su negocio o servicio reciben gran cantidad de datos personales los cuales deben ser tratados según esta Ley Orgánica y de ser el caso transferidos cumpliendo los requisitos también previsto en la Ley Orgánica, tendrán la necesidad de proteger estos DATOS PERSONALES, no solo con la tecnología necesaria, sino también con productos de seguros de “cyber seguridad”, que ayuden a mitigar este riesgo alto a que están expuestas.

Quito, 4 de junio de 2021

Dra. Paulina Guerrero Vivanco

