RESUMEN LEGAL

LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES

Estado: Informe para Primer Debate fue conocido, debatido y aprobado en la sesión No. 109-2019-2021, de la Comisión Especializada Permanente de Soberanía, Integración, Relaciones Internacionales y Seguridad Integral, celebrada el 09 de noviembre de 2020.
Procede: Primer debate en el Pleno de la Asamblea Nacional.

El presente resumen compendia los aspectos más relevantes de la Ley Orgánica de Protección de Datos Personales. Se encuentra dividido en 13 apartados para brindar una visión amplia del enfoque y alcance la Ley.

Previo a su lectura, se considera importante revisar los siguientes conceptos:

- **Dato personal:** Dato que identifica o hace identificable a una persona natural, directa o indirectamente.
- **Volumen de negocio:** Resultado de la venta de productos y prestación de servicios, descontado impuestos, durante el último ejercicio fiscal.
- **Titular:** Persona natural cuyos datos son objeto de tratamiento.
- **Responsable del tratamiento:** Persona natural o jurídica, pública o privada, que decide sobre la finalidad y el tratamiento de datos personales.
- **Encargado del tratamiento:** Aquel que trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales.
- **Autoridad de Protección de Datos Personales:** Superintendencia de Protección de Datos Personales.
- **Delegado de protección de datos personales:** Persona natural encargada de informar al responsable o al encargado sobre sus obligaciones, y velar o supervisar el cumplimiento normativo y cooperar con la Autoridad. Sirve como punto de contacto entre la Autoridad y la entidad responsable del tratamiento de datos.

En líneas generales, se encuentra una visión intervencionista por parte de Estado ecuatoriano, se promueve una fuerte regulación amparada en la aplicación de altas sanciones económicas así como el establecimiento de preceptos rígidos para la valoración de las mismas, como la reincidencia y la reiteración, sobre las cuales no se han establecido periodo de vigencia, lo que implica que el administrado está a expuesto a la aplicación de una agravante de manera indefinida, sin que pueda recobrar su condición original.

Existen otros puntos complejos, como el tema de la regulación de transferencia de datos internacional, que se hace de muy difícil aplicación, pues transgrede el principio de extraterritorialidad de la Ley. También se observa la imposición de la obligación de informar y capacitar con relación al uso y tratamiento responsable, adecuado y seguro de datos personales, así como varias obligaciones que representarían una carga operativa adicional y en consecuencia un impacto económico en los administrados.

1. ASPECTOS GENERALES

- El objeto y finalidad de la ley es garantizar el ejercicio del derecho a la protección de datos personales.

- El derecho a la protección de datos personales, incluye el acceso, decisión sobre información y datos de este carácter.

- La Ley se aplicará al tratamiento de datos personales contenidos en cualquier tipo de soporte y a toda modalidad de uso posterior.

- La Ley no aplicará a:

1. Personas que usen los datos en actividades familiares o domésticas.
2. Personas fallecidas.
3. Datos anonimizados.
4. Actividades periodísticas y otros contenidos editoriales.
5. Los regulados en normativa especializada de igual o mayor jerarquía sobre gestiona de riesgos por desastres naturales y seguridad y defensa del Estado.
6. Datos o bases de datos para la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.
7. Datos que identifican o hacen identificable a personas jurídicas.

- Son accesibles al público y susceptibles de tratamiento los datos personales de comerciantes, representantes y socios 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.

- Sin perjuicio de los instrumentos internacionales ratificados por el Ecuador, la Ley aplicará cuando:

1. Tratamiento se realicen en territorio nacional.
2. El responsable o encargado del tratamiento se encuentre domiciliado en territorio nacional.
3. El responsable o encargado, que no esté domiciliado en el país, oferte bienes o servicios a residentes en el territorio nacional, independientemente de si realizan o no un pago o realice actividades relativas a la recolección de datos personales de residentes en Ecuador.
4. Responsable o encargado, 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.

- **Términos y Definiciones de mayor importancia:**

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

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

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

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

- Datos sensibles: Datos relativos a la 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.

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

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

- Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, y, en general, cualquier uso de datos personales.

- Volumen de negocio: Resultado 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.

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

2. SUJETOS DE REGULACIÓN

- **Titular:** Persona natural cuyos datos son objeto de tratamiento.
- **Responsable del tratamiento:** Persona natural o jurídica, pública o privada, que decide sobre la finalidad y el tratamiento de datos personales.
- **Encargado del tratamiento:** quien trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales.
- **Destinatario:** aquel que ha sido comunicado con datos personales.
- **Autoridad de Protección de Datos Personales:** Autoridad pública independiente, denominada "Superintendencia de Protección de Datos Personales" (en adelante la "Superintendencia" o "Autoridad") con personalidad jurídica y autonomía administrativa, técnica y financiera.
- **Entidades certificadoras:** Reconocida por la Superintendencia de Protección de Datos Personales, que podrá, de manera no exclusiva, proporcionar certificaciones en la materia.
- **Delegado de protección de datos personales:** Persona natural encargada de informar al responsable o al encargado sobre sus obligaciones, y velar o supervisar el cumplimiento normativo y cooperar con la Autoridad. Sirve como punto de contacto entre la Autoridad y la entidad responsable del tratamiento de datos.

3. LEGITIMIDAD DEL TRATAMIENTO DE DATOS PERSONALES

- Será legítimo y lícito si se cumple con *alguna* de las siguientes condiciones:

1. Por **consentimiento** del titular para el tratamiento de sus datos personales, para una o varias finalidades 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;
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.

- **Consentimiento será válido cuando la manifestación de voluntad sea**:

- Libre: exenta de vicios del consentimiento (error, fuerza y dolo).
- Específica: determinación concreta de los medios y fines del tratamiento.
- Informada: cumplir el principio de transparencia y efectivizar el derecho a este.
- Inequívoca: no presente dudas sobre el alcance de la autorización otorgada.
- El consentimiento podrá revocarse en cualquier momento sin justificación; responsable debe adoptar un procedimiento sencillo para el efecto.

4. PRINCIPIOS

1. **Juridicidad:** Tratarse con estricto apegado a los principios, derechos y obligaciones.

2. **Lealtad:** Conocimiento del titular de que se están recogiendo, utilizando, consultando o tratando datos personales que les conciernen y las formas en las que estos son o serán tratados. No se pueden tratar a través de medios o para fines ilícitos o desleales.

3. **Transparencia:** Información o comunicación sobre el tratamiento debe ser fácilmente accesible y de entender; relaciones derivadas del tratamiento deben ser transparentes.

4. **Finalidad:** Ser determinadas, explicitas y legitimas; no se podrán tratar datos para fines distintos para los que fueron recopilados.

5. **Pertinencia y minimización:** Ser pertinentes y estar limitados a lo estrictamente necesario

6. **Proporcionalidad:** Ser adecuado, necesario, oportuno, relevante y no excesivo en relación a las finalidades o la naturaleza de las categorías especiales.

7. **Confidencialidad:** Concebirse sobre la base del debido sigilo y secreto; el responsable del tratamiento deberá adecuar las medidas técnicas organizativas.

8. **Calidad y exactitud:** Deben ser exactos, íntegros, precisos, completos, comprobables, claros y actualizados (de ser el caso; esto es obligación del responsable.

9. **Conservación:** Durante un tiempo no mayor al necesario para cumplir con la finalidad de su tratamiento; el responsable establecerá´ plazos para su supresión o revisión periódica. El posterior tratamiento se realizará con determinados fines (archivo, investigación) siempre que se establezcan las garantías de seguridad y protección.

10. **Seguridad:** Los responsables y encargados deberán implementar todas las medidas de seguridades adecuadas y necesarias (aquellas aceptadas por el estado de la técnica).

11. **Responsabilidad proactiva y demostrada:** El responsable deberá acreditar el haber implementado mecanismos para la protección de datos personales (podrá valerse de estándares, sellos, sistemas de certificación, etc). Obligación de rendir cuentas sobre el tratamiento al titular y a la autoridad, y evaluar y revisar los mecanismos que adopte a fin de mejorar su nivel de eficacia.

12. **Aplicación favorable al titular:** En caso de duda, el ordenamiento jurídico o contractual, se interpretará y aplicará en el sentido más favorable al titular.

13. **Independencia del control** La Autoridad ejercerá un control independiente, imparcial y autónomo, y llevará a cabo acciones de prevención, investigación y sanción.

5. DERECHOS DEL TITULAR

- **Derecho de aplicación de principios de normativa especializada:** Los datos personales cuyo tratamiento se encuentre regulado en normativa especializada en materia de ejercicio de la libertad de expresión, sectores regulados por normativa específica, gestión de riesgos, desastres naturales, seguridad nacional y defensa del Estado; y, los datos personales que deban proporcionarse a autoridades administrativas o judiciales, 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.

- **Derecho a la información sobre:**

SEGURIDAD DE LOS DATOS

1. El origen de los datos personales cuando no se hayan obtenido directamente del titular;
2. Identidad y datos de contacto del responsable del tratamiento de datos personales, que incluirá: dirección del domicilio legal, número de teléfono y correo electrónico;
3. Identidad y datos de contacto del delegado de protección de datos personales, que incluirá: dirección domiciliaria, teléfono y correo electrónico;

DERECHOS Y OBLIGACIONES

4. La base legal para el tratamiento;
5. El carácter obligatorio o facultativo de las respuestas y consecuencias de proporcionar o no sus datos personales;
6. El efecto de suministrar datos personales erróneos o inexactos;
7. La posibilidad de revocar el consentimiento;
8. 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.
9. Los mecanismos para hacer efectivo su derecho a la portabilidad, cuando el titular lo solicite;
10. Dónde y cómo realizar sus reclamos ante el responsable del tratamiento de datos personales y la Autoridad de Protección de Datos Personales, y;

USO

11. Los fines del tratamiento.
12. Tipos de tratamiento;
13. Tiempo de conservación;
14. La existencia de una base de datos en la que constan sus datos personales;
15. Otras finalidades y tratamientos ulteriores;

16. 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;
17. La existencia de valoraciones y decisiones automatizadas, incluida la elaboración de perfiles.

Si los datos se obtienen directamente del titular, toda la información se debe comunicar previo a recoger los datos personales; en su defecto, se la deberá dentro los 30 días siguiente por cualquier modo comprobable.

- **Derecho de acceso:** Conocer y obtener gratuitamente del responsable todos sus datos personales y la información antes mencionada, sin necesidad de justificar. El responsable debe establecer métodos razonables para el efecto. El pedido debe ser atendido en el plazo de 15 días.

- **Derecho de rectificación y actualización:** Sobre datos personales inexactos o incompletos, para ello, el titular debe presentar los justificativos del caso cuando sea pertinente. Atención del requerimiento en el plazo de 15 días; en el mismo plazo se debe informar al destinatario sobre la rectificación.

- **Derecho de eliminación:** En los siguientes casos:

1. Tratamiento no cumpla con los principios de la Ley.
2. Tratamiento no sea necesario o pertinente para la finalidad.
3. Datos personales hayan cumplido con la finalidad.
4. Vencimiento del plazo de conservación de los datos personales.
5. Tratamiento afecte derechos fundamentales o libertades individuales.
6. Haya revocado o no haya otorgado el consentimiento para uno o varios fines específicos.
7. Exista obligación legal.

El responsable debe implementar métodos y técnicas para eliminar, hacer ilegible o dejar irreconocibles de forma definitiva y segura los datos. Esta obligación será gratuita y se debe hacer en el plazo de 15 días.

- **Derecho al olvido digital:** Por disposición del juez competente cuando:

1. Sean de carácter obsoleto.
2. No tengan valor histórico o científico.
3. No sean de relevancia pública.
4. Sean inadecuados, impertinentes o excesivos con relación a los fines y al tiempo transcurrido.

- **Derecho de oposición o negarse al tratamiento:** Cuando no afecten derechos y libertades fundamentales de terceros, la ley se lo permita y no se trate de información pública o cuyo tratamiento esté ordenado por la Ley.
- **Derecho de anulación:** Nulidad de los actos ilícitos vinculados a la obtención y tratamiento de datos personales ante la autoridad jurisdiccional.

- **Derecho a la portabilidad:** Recibir sus datos personales del responsable en un formato compatible, actualizado, estructurado, común, interoperable y de lectura mecánica, preservando sus características.

- **Derecho a la suspensión del tratamiento:** En los siguientes casos:

1. Titular impugne la exactitud de los datos personales.
2. Tratamiento sea ilícito y el interesado se oponga a la supresión y solicite -en su lugar la limitación de su uso.
3. Responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para reclamaciones.
4. Interesado se haya opuesto al tratamiento (art. 31 Datos Crediticios), mientras se verifica si motivos del responsable prevalecen sobre los del interesado.

- **Derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas.**

- **Derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas en categorías especiales de datos:** No se podrán tratar datos sensibles o datos de niños y adolescentes salvo se cuente con autorización ***expresa*** del representante legal o cuando el tratamiento sea para salvaguardar un interés público esencial, respete el principio de proporcionalidad e incluya salvaguardas para proteger los derechos.

- **Derecho de consulta:** De modo público y gratuito ante el Registro Nacional de Protección de Datos Personales.

- **Derecho a la educación digital:** Disponibilidad del conocimiento, aprendizaje, preparación, estudio, formación, capacitación, enseñanza e instrucción sobre el uso y manejo de las TIC, así como promover una cultura sensibilizada en el derecho de protección de datos personales.

Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad:

1. Si el solicitante no es titular de los datos personales o su representante legal no se encuentre debidamente acreditado.
2. Datos son necesarios para cumplir una obligación legal o contractual, orden judicial, resolución o mandato de autoridad.
3. Datos son necesarios para reclamos o recursos.
4. Se pueda causar perjuicios a derechos o afectación a intereses legítimos de terceros.
5. Se pueda obstaculizar actuaciones judiciales o administrativas en curso.
6. Datos son necesarios para ejercer el derecho a la libertad de expresión y opinión, o para proteger el interés vital del interesado o de otra persona natural.
7. En caso de mediar interés público.

8. Tratamiento de datos personales sea necesario para el archivo de información que sea patrimonio del Estado, investigación científica, histórica o estadística.

- **Ejercicio de los 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, 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.

- Los adolescentes mayores de doce (12) años y menores de quince (15) años, así como las niñas y niños, para el ejercicio de sus derechos necesitarán de su representante legal.

- Los adolescentes mayores de quince (15) años y menores de dieciocho (18) años, podrán ejercitarlos de forma directa ante la Autoridad de Protección de Datos Personales o ante el responsable de la base de datos personales del tratamiento.

- Los derechos del titular son irrenunciables.

6. CATEGORÍAS ESPECIALES DE DATOS

- Se considerarán **categorías especiales** de datos personales, los siguientes:

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

- **Consentimiento relativo a categorías especiales de datos**: En este tipo de datos se requerirá de la manifestación de la voluntad expresa del titular, manifestada por cualquier mecanismo permitido por la legislación ecuatoriana.

- **Datos personales de personas fallecidas:** Los titulares de derechos sucesorios de las personas fallecidas o las personas o instituciones que el fallecido haya designado expresamente podrán ejercer los derechos del titular, tales como, 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.

- **Datos crediticios:** Son datos cuyo tratamiento revela la solvencia patrimonial o crediticia, que permiten evaluar la conducta comercial o la capacidad de pago del titular de los datos.

- Únicamente pueden ser procesados si han sido obtenidos de fuentes de acceso público o directamente del acreedor.

- Estos datos no serán comunicados o difundidos, ni podrán tener cualquier finalidad secundaria.

- **Datos relativos a la salud:** Datos sobre el estado de salud de pacientes.

- 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.

- Las personas relacionadas con los datos relativos a la salud están obligadas a guardar confidencialidad sobre éstos.

- No se requeriría consentimiento del titular para el tratamiento de estos datos por razones de interés público.

7. TRANSFERENCIA O COMUNICACIÓN Y ACCESO A DATOS PERSONALES POR TERCEROS

- Datos personales podrán transferirse o comunicarse a terceros para el cumplimiento de fines directamente relacionados con las funciones legítimas del responsable o destinatario. La transferencia debe estar configurada dentro de una de las causales de legitimidad y debe contarse con el consentimiento del titular.

- **Acceso a datos personales por parte del encargado:** No se considerará transferencia o comunicación cuando sea necesario para prestar un servicio al responsable del tratamiento.

- Se considerará encargado al tercero que ha accedido legítimamente a los datos personales en estas consideraciones:

  1. El tratamiento realizado por el encargado debe estar regulado por un contrato; el tratamiento se efectuará conforme las instrucciones del responsable y no los usará para fines diferentes, ni los transferirá o comunicará a otros.
  2. Cumplida la prestación contractual, los datos personales deberán ser destruidos o devueltos al responsable bajo la supervisión de la Autoridad.
  3. El encargado será responsable de las infracciones por incumplimiento de las condiciones de tratamiento.

- **Acceso a datos personales por parte de terceros:** No se considerará transferencia o comunicación cuando sea necesario para la prestación de un servicio al responsable.

  1. El tratamiento realizado por el tercero debe estar regulado por un contrato; el tratamiento se efectuará conforme las instrucciones del responsable y no los usará para fines diferentes, ni los transferirá o comunicará a otros.
  2. Cumplida la prestación contractual, los datos personales deberán ser destruidos o devueltos al responsable bajo la supervisión de la Autoridad.
  3. El tercero será responsable de las infracciones por incumplimiento de las condiciones de tratamiento.

Excepciones al consentimiento del titular para la transferencia:

- Los datos han sido recogidos de fuentes accesibles al público.
- El tratamiento responda a la libre y legítima aceptación de una relación jurídica entre el responsable y titular, cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con la base de datos; esta será legítima en cuanto se limite a la finalidad.
- Los datos deban proporcionarse a autoridades administrativas o judiciales por solicitudes y órdenes amparadas en su competencia.

- La comunicación se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior con fines históricos, estadísticos o científicos (datos deben estar disociados).
- La comunicación de datos de carácter personal relativo a la salud 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.

- **Transferencia o comunicación internacional de datos personales:**

- Se podrán transferir o comunicar a países u organizaciones que brinden niveles adecuados de protección; se establecerán criterios en el Reglamento.

- Autoridad de Protección de Datos Personales emitirá´ resolución motivada sobre el cumplimiento de los niveles o garantías adecuados de protección.

- Transferencia o comunicación mediante garantías adecuadas, ello implica que el responsable o encargado deberá tomar medidas para compensar la falta de protección de datos en un tercer país cumpliendo por lo menos con: Observancia de principios, derechos y obligaciones; efectiva tutela del derecho a la protección de datos personales, con la disponibilidad permanente de acciones administrativas o judiciales, y, el derecho a solicitar la reparación integral, de ser el caso.

  Para la aplicación de este mecanismo, se requiere de instrumentos jurídicos vinculantes y exigibles entre autoridades y responsables, como los son: normas corporativas, cláusulas estándar de protección de datos, códigos de protección, mecanismos de certificación o sellos.

- Control continúo a la realidad internacional en materia de protección por parte de la Autoridad junto a la academia.

8. SEGURIDAD DE DATOS PERSONALES

- **El responsable o encargado, deberá:**

- Tomar en cuenta la categoría y volumen de los datos, estado de la técnica, mejores prácticas de seguridad integral y costos de aplicación.

- Identificar la probabilidad de riesgos.

- Implementar un proceso de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas.

- Evidenciar que las medidas adoptadas mitiguen los riesgos.

- Implementar medidas para garantizar que procesos y medios de tratamiento protejan los datos personales desde su diseño, así como sus configuraciones se encuentren por defecto en cumplimiento de la norma.

- **Medidas que se pueden incluir para la seguridad:**

- Medidas de anonimización, seudonomización o cifrado de datos.

- Medidas para mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento y acceso de datos, de forma rápida en caso de incidentes.

- Medidas para mejorar la resiliencia técnica, física, administrativa y jurídica.

- Podrán acogerse a estándares internacionales.

- **La evaluación de impacto del tratamiento de datos personales a cargo del responsable se efectuará en los siguientes casos:**

- Se identifique la probabilidad de que el tratamiento conlleve un alto riesgo para derechos y libertades del titular.
- La Autoridad de Protección de Datos Personales lo requiera.

- **Obligación de notificar la vulneración de la seguridad:**

- El responsable tiene la de los datos a la Autoridad de Protección de Datos Personales y la ARCOTEL en el término de 5 días desde que se conozca la vulneración.

- El encargado debe notificar al responsable cualquier vulneración dentro del término de 2 días.

- Por retraso injustificado en la notificación, se aplicarán sanciones.

- La notificación y ejecución oportuna de medidas de respuesta serán consideradas atenuantes a la infracción.

- La notificación al titular por parte del responsable sobre la vulneración cuando conlleve un riesgo a sus derechos y libertades fundamentales, en el término de 3 días.

- No se deberá notificar al titular cuando:

1. El responsable haya adoptado medidas de protección que se pueda demostrar que son efectivas.
2. El responsable haya tomado medidas que garanticen que el riesgo a derechos y libertades del titular no ocurrirá.
3. Se requiere un esfuerzo desproporcionado para la notificación.

- La falta de notificación será sancionada, así como la notificación y ejecución oportuna de medidas serán atenuantes a la infracción.

- **Acciones con relación a la vulneración de la seguridad de datos:**

- Conocida la vulneración, responsable debe efectuar el análisis de riesgo sobre los derechos de libertad de sus titulares.

- La Autoridad llevará un registro estadístico sobre las vulneraciones; podrá identificar posibles medidas de seguridad para estas y los sectores e instituciones más vulnerables, así como promoverá nuevas regulaciones para mejorar las seguridades.

- Solo se podrá sancionar al responsable o encargado cuando la vulneración sea por incumplimiento de las medidas de seguridad adecuadas.

- Los prestadores y proveedores de servicios de telecomunicaciones y proveedores de tecnología y servicios de seguridad, así como otros organismos, podrán acceder y efectuar tratamiento sobre datos personales de las notificaciones de vulneración solo para la detección, análisis, protección y respuesta ante incidentes, así como para adoptar e implementar medidas de seguridad.

4. RESPONSABLE Y DELEGADO DE PROTECCIÓN DE DATOS PERSONALES

- **Obligaciones del responsable del tratamiento de datos personales:**

- Aplicar e implementar requisitos y herramientas para garantizar y demostrar que el tratamiento de datos personales se ha realizado conforme la Ley.
- Aplicar e implementar procesos de verificación, evaluación, valoración periódica de la eficiencia, eficacia y efectividad de los requisitos y herramientas implementadas.
- Implementar políticas de protección de datos personales afines al tratamiento en cada caso en particular.
- Utilizar metodologías de análisis y gestión de riesgos adaptadas a las particularidades del tratamiento y de las partes involucradas.
- Realizar evaluaciones de adecuación al nivel de seguridad previas al tratamiento.
- Tomar medidas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas.
- Notificar a la Autoridad de Protección de Datos Personales y al titular de los datos acerca de violaciones a las seguridades implementadas.
- Implementar la protección desde el diseño y por defecto.
- Suscribir contratos de confidencialidad y manejo adecuado de datos personales con el encargado y el personal a cargo del tratamiento o que tenga conocimiento de los datos personales.
- Asegurar que el encargado ofrezca mecanismos suficientes para garantizar el derecho a la protección de datos personales.
- Registrar y mantener actualizado el Registro Nacional de Protección de Datos Personales.
- Designar al Delegado de Protección de Datos Personales, cuando corresponda.

El encargado tendrá las mismas obligaciones que el responsable de tratamiento de datos personales, en lo que sea aplicable.

- **Designación del delegado de protección de datos personales:** Se designará en las siguientes circunstancias:

  - Tratamiento lo realicen quienes conforman el sector público.

- Actividades del responsable o encargado requieran un control permanente y sistematizado por su volumen, naturaleza, alcance o finalidades.

- Tratamiento a gran escala de categorías especiales de datos.

- Tratamiento no se refiera a datos relacionados con la seguridad nacional y defensa del Estado que adolezcan de reserva ni fuesen secretos.

- **Funciones del delegado de protección de datos personales:**

- Asesorar al responsable, al personal del responsable y al encargado.

- Asesorar en el análisis de riesgo, evaluación de impacto y evaluación de medidas de seguridad, y supervisar su aplicación.

- **Para la ejecución de las funciones del delegado, el responsable y el encargado se deberá observar lo siguiente:**

- Garantizar la participación adecuada y oportuna del delegado en todas las cuestiones relativas a la protección de datos personales.

- Facilitar el acceso a los datos personales de las operaciones de tratamiento, así´ como todos los recursos y elementos necesarios.

- Capacitar y actualizar en la materia al delegado.

- No podrán destituir o sancionar al delegado por el desempeño de sus funciones.

- El delegado mantendrá relación directa con el más alto nivel ejecutivo y de decisión del responsable y con el encargado.

- El titular podrá contactar al delegado con relación al tratamiento de sus datos personales a fin de ejercer sus derechos.

- Obligación del delegado a mantener la más estricta confidencialidad.

- Delegado podrá desempeñar otras funciones dispuestas por el responsable o encargado, cuando no exista conflicto con las responsabilidades.

- Se creará un **Registro Nacional de protección de datos personales** y un **Registro Único de Responsables y Encargados Incumplidos.**

10. RESPONSABILIDAD PROACTIVA

- Los responsables y encargados ***podrán*** acogerse o adherirse a códigos de protección, estándares, certificaciones, sellos y mejores prácticas; esto no constituye eximente de la responsabilidad de cumplir con la Ley.

- **Códigos de conducta:** La Autoridad promoverá la elaboración de códigos de conducta por sectores, industrias, empresas, organizaciones, considerando lo que sigue:

• Estos deberán tomar en cuenta las necesidades específicas de los sectores.

• Responsables o encargado podrán adherirse o implementar estos códigos.

- **Atribuciones de las Entidades de Certificación:**

• Emitir certificaciones de cumplimiento.

• Emitir sellos de protección de datos personales.

• Llevar a cabo auditorias de protección de datos personales.

• Certificar los procesos de transferencias internacionales de datos personales.

11. REQUERIMIENTOS DIRECTOS Y DE LA GESTIÓN DEL PROCEDIMIENTO ADMINISTRATIVO

- El titular podrá en cualquier momento, de forma gratuita, presentar requerimientos, peticiones, quejas o reclamaciones directamente al responsable. El responsable deberá contestar en el término de 5 días.

- La Autoridad de Protección de Datos Personales podrá iniciar, de oficio o a petición del titular, actuaciones previas para conocer las circunstancias del caso o la conveniencia de iniciar el procedimiento.

- Procedimiento Administrativo:

- Si responsable no contesta el requerimiento o este fuere negado, el titular podrá presentar un reclamo administrativo ante la Autoridad de Protección de Datos Personales.

12. MEDIDAS CORRECTIVAS, INFRACCIONES Y RÉGIMEN SANCIONATORIO

- **Medidas correctivas**:

1. El cese del tratamiento, bajo determinadas condiciones o plazos.

2. La eliminación de los datos.

3. La imposición de medidas técnicas, jurídicas, organizativas o administrativas a garantizar un tratamiento adecuado de datos personales.

- Para el caso de infracciones leves se aplicará a los responsables, encargados y, de ser el caso, tercero, **únicamente medidas correctivas.** Si fueran incumplidas, se aplicarán las sanciones correspondientes.

- Si responsables, encargados y, de ser el caso, terceros, consten en el Registro Único de responsables y encargados incumplidos, la Autoridad activará directamente el procedimiento administrativo sancionatorio.

- Si los responsables, encargados y, de ser el caso, terceros, hayan presuntamente cometido una infracción grave, la Autoridad activara´ directamente el procedimiento administrativo sancionatorio.

- **Infracciones leves y graves tanto para el responsable como para el encargado**:

- **Sanciones por infracciones leves:** multa de entre el 3% y el 9% calculada sobre su volumen de negocio del ejercicio económico inmediatamente anterior al de la multa; esta será proporcional, considerando: intencionalidad, reiteración de la infracción, naturaleza del perjuicio ocasionado y reincidencia.

- **Sanciones por infracciones graves**: En el caso de 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 negocios del ejercicio económico inmediatamente anterior al de la multa, aplicando el principio de proporcionalidad y considerando: intencionalidad, reiteración de la infracción, naturaleza del perjuicio ocasionado y reincidencia.

- Posibilidad de aplicar medidas provisionales de protección o medidas cautelares determinados en la norma de procedimiento administrativo.

Las medidas correctivas y el régimen sancionatorio se aplicarán dentro de 2 años contados a partir de la entrada en vigencia de la Ley.

13. OTRAS DISPOSICIONES

- Todo tratamiento realizado previo a la entrada en vigencia de la Ley deberá adecuarse a este en el plazo de 2 años.

- Responsables y encargados que hayan implementado los preceptos de la Ley antes de la entrada en vigencia de esta, obtendrán un reconocimiento por buenas prácticas.

- Se plantean reformas a la Ley de Comercio Electrónico y a la Ley del Sistema Nacional de Registro de Datos Públicos en concordancia con los preceptos de la 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.

- Reformas a la Ley de Telecomunicaciones:

- Se eliminan las disposiciones sobre el procedimiento de la notificación al abonado o usuario particular en caso de violación de sus datos.

- Se eliminan algunas funciones de la ARCOTEL respecto de la seguridad de datos personales, así como el artículo sobre procedimientos de revelación y entrega de información.

- Obligación de prestadores de servicios de telecomunicaciones de adoptar las medidas adecuadas para preservar la seguridad de su red con el fin de garantizar la protección de los datos personales.

- Los abonados, clientes o usuarios tienen el derecho a no figurar en guías telefónicas o de abonados; derecho a ser informados de sus derechos sobre el uso de sus datos personales en guías.

- 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, salvo consentimiento de este.

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