

**ESTADO PLURINACIONAL DE BOLIVIA MINISTERIO DE LA PRESIDENCIA AGENCIA DE
GOBIERNO ELECTRÓNICO Y TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN –
AGETIC**

ANTEPROYECTO DE LEY DE PROTECCIÓN DE DATOS PERSONALES

AGETIC

2023

ÍNDICE
ANTEPROYECTO DE LEY DE PROTECCIÓN DE DATOS PERSONALES

TÍTULO I
DISPOSICIONES GENERALES
CAPÍTULO I
GENERALIDADES

- ARTÍCULO 1.(OBJETO).-**
- ARTÍCULO 2. (FINALIDAD).-**
- ARTÍCULO 3. (DEFINICIONES).-**
- ARTÍCULO 4. (ÁMBITO DE APLICACIÓN).-**
- ARTÍCULO 5. (TRANSVERSALIDAD).-**
- ARTÍCULO 6. ÁMBITO DE APLICACIÓN TERRITORIAL).-**
- ARTÍCULO 7. (EXCEPCIONES A LA APLICACIÓN DE LA LEY).-**
- ARTÍCULO 8. (ESQUEMA DE EXCEPCIONES).-**

CAPÍTULO II
PRINCIPIOS RECTORES

- ARTÍCULO 9. (PRINCIPIOS).-**

TÍTULO II
DERECHOS
CAPÍTULO I
EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA

- ARTÍCULO 10. (DERECHOS DE LOS TITULARES).-**
- ARTÍCULO 11. (INFORMACIÓN PARA EL TITULAR CUANDO LOS DATOS PERSONALES SE OBTENGAN DIRECTAMENTE DE DICHO TITULAR).-**
- ARTÍCULO 12. (INFORMACIÓN PARA EL TITULAR CUANDO LOS DATOS PERSONALES NO SE HAN OBTENIDO DEL TITULAR).-**
- ARTÍCULO 13. (PLAZO PARA LA PUESTA A DISPOSICIÓN DE LA INFORMACIÓN CUANDO LOS DATOS NO SE OBTUVIERON DE SU TITULAR).-**
- ARTÍCULO 14. (CASOS DE EXCEPCIÓN AL DERECHO A LA INFORMACIÓN SI LOS DATOS PERSONALES NO SE OBTUVIERON DE SU TITULAR).-**

CAPÍTULO II
EJERCICIO DE DERECHOS

- ARTÍCULO 15. (GRATUIDAD DE LOS DERECHOS).-**
- ARTÍCULO 16. (ACREDITACIÓN DE IDENTIDAD)**
- ARTÍCULO 17. (COMUNICACIÓN Y MODALIDADES DE EJERCICIO DE LOS DERECHOS DEL TITULAR DE DATOS).-**
- ARTÍCULO 18. (IMPROCEDENCIA DE LAS SOLICITUDES DE EJERCICIO DE DERECHOS).-**
- ARTÍCULO 19. (PLAZO DE RESPUESTA PARA SOLICITUDES DE EJERCICIO DE DERECHOS).-**
- ARTÍCULO 20. (REQUISITOS DE LA SOLICITUD PARA EL EJERCICIO DE DERECHOS).-**
- ARTÍCULO 21. (RECEPCIÓN Y ATENCIÓN DE SOLICITUDES DE EJERCICIO DE DERECHOS).-**
- ARTÍCULO 22. (CASOS EN LOS QUE NO PROCEDE EL EJERCICIO DE DERECHOS).-**
- ARTÍCULO 23. (MEDIO DE IMPUGNACIÓN CONTRA LAS RESPUESTAS A SOLICITUDES DE EJERCICIO DE DERECHOS).-**

CAPÍTULO III
RECLAMACIONES

- ARTÍCULO 24. (PROCEDIMIENTO DE RECLAMACIÓN).-**
- ARTÍCULO 25. (TRÁMITE DE RECLAMACIONES A TRAVÉS DE PLATAFORMAS DIGITALES).-**
- ARTÍCULO 26. (INICIO DEL PROCEDIMIENTO Y DURACIÓN).-**

- ARTÍCULO 27. (CASOS EN LOS QUE NO SE ADMITIRÁN LAS RECLAMACIONES).-
ARTÍCULO 28. (ACTUACIONES PREVIAS DE INVESTIGACIÓN).-
ARTÍCULO 29. (INICIO DEL PROCEDIMIENTO SANCIONADOR).-
ARTÍCULO 30. (CONFIDENCIALIDAD Y FE PÚBLICA DE LOS FUNCIONARIOS).-
ARTÍCULO 31. (MEDIDAS CAUTELARES).-
ARTÍCULO 32. (DESARROLLO DEL PROCEDIMIENTO).-**

TÍTULO III

RESPONSABLES, ENCARGADOS Y DELEGADO DE TRATAMIENTO DE DATOS PERSONALES

CAPÍTULO I

RESPONSABLES Y ENCARGADOS FUERA DEL TERRITORIO

- ARTÍCULO 33. (RESPONSABLES O ENCARGADOS ESTABLECIDOS FUERA DE TERRITORIO BOLIVIANO).-
ARTÍCULO 34. (COOPERACIÓN CON LA AUTORIDAD).-
ARTÍCULO 35. (CORRESPONSABILIDAD EN EL TRATAMIENTO).-**

CAPÍTULO II ENCARGADO

- ARTÍCULO 36. (ALCANCES DE LA PARTICIPACIÓN DEL ENCARGADO).-
ARTÍCULO 37. (REGLAS DE ACTUACIÓN PARA EL ENCARGADO).-
ARTÍCULO 38. (MODELOS DE CLÁUSULAS CONTRACTUALES).-
ARTÍCULO 39. (CONTRATACIÓN DE UN ENCARGADO POR PARTE DEL ENCARGADO AUTORIZADO).-**

CAPÍTULO III DELEGADO DE PROTECCIÓN DE DATOS

- ARTÍCULO 40. (OBJETIVO DEL DELEGADO).-
ARTÍCULO 41. (INDEPENDENCIA DEL DELEGADO EN EL EJERCICIO DE SUS FUNCIONES).-
ARTÍCULO 42. (FUNCIONES DEL DELEGADO DE PROTECCIÓN DE DATOS).-
ARTÍCULO 43. (DESIGNACIÓN DEL DELEGADO DE PROTECCIÓN DE DATOS).-**

TÍTULO IV

TRATAMIENTO DE DATOS PERSONALES SENSIBLES Y DE TUTELA ESPECIAL

- ARTÍCULO 44. (PROHIBICIÓN DE TRATAMIENTO DE DATOS PERSONALES SENSIBLES).-
ARTÍCULO 45. (INTERÉS SUPERIOR DEL MENOR Y CONSENTIMIENTO).-
ARTÍCULO 46. (TRATAMIENTO DE DATOS PERSONALES DE PERSONAS CON CAPACIDADES DIFERENTES).-
ARTÍCULO 47. (TRATAMIENTO DE DATOS PERSONALES DE PERSONAS FALLECIDAS).-**

TÍTULO V

TRATAMIENTO DE DATOS PERSONALES EN ÁMBITOS ESPECÍFICOS

- ARTÍCULO 48. (DATOS EN MEDIOS DE COMUNICACIÓN).-
ARTÍCULO 49. (TRATAMIENTO CON FINES PUBLICITARIOS).-**

TÍTULO VI

RÉGIMEN DE TRANSFERENCIAS INTERNACIONALES

CAPÍTULO I

RÉGIMEN DE GARANTÍAS ADECUADAS

- ARTÍCULO 50. (TRANSFERENCIA INTERNACIONAL).-**
- ARTÍCULO 51 (TRANSFERENCIAS INTERNACIONALES MEDIANTE GARANTÍAS ADECUADAS).-**
- ARTÍCULO 52. (GARANTÍAS QUE NO REQUIEREN AUTORIZACIÓN EXPRESA).-**
- ARTÍCULO 53. (GARANTÍAS QUE SÍ REQUIEREN AUTORIZACIÓN EXPRESA).-**
- ARTÍCULO 54. (NORMAS CORPORATIVAS VINCULANTES).-**
- ARTÍCULO 55 . (CONTENIDO DE LAS NORMAS CORPORATIVAS VINCULANTES).-**

CAPÍTULO II RÉGIMEN DE EXCEPCIONES PARA SITUACIONES ESPECÍFICAS

- ARTÍCULO 56. (EXCEPCIONES PARA SITUACIONES ESPECÍFICAS).-**

CAPÍTULO III RÉGIMEN DE TRANSFERENCIAS FUERA DEL RÉGIMEN DE GARANTÍAS ADECUADAS Y DEL RÉGIMEN DE EXCEPCIONES PARA SITUACIONES ESPECÍFICAS

- ARTÍCULO 57. (TRANSFERENCIAS FUERA DEL RÉGIMEN DE GARANTÍAS ADECUADAS Y DEL
RÉGIMEN DE EXCEPCIONES PARA SITUACIONES ESPECÍFICAS).-**

TÍTULO VII AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES, REGISTRO BOLIVIANO DE BANCOS DE DATOS

CAPÍTULO I AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES

- ARTÍCULO 58.(AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES).-**
- ARTÍCULO 59.(OBJETO).-**
- ARTÍCULO 60.(ATRIBUCIONES).-**
- ARTÍCULO 61. (RECURSOS PARA EL EJERCICIO DE SUS FUNCIONES).-**
- ARTÍCULO 62. (DESIGNACIÓN DEL TITULAR DE LA AUTORIDAD DE PROTECCIÓN DE DATOS
PERSONALES).-**
- ARTÍCULO 63. (CESE ANTICIPADO).-**
- ARTÍCULO 64. (REVISIÓN DE RESOLUCIONES DE LA AUTORIDAD DE PROTECCIÓN DE DATOS
PERSONALES).-**
- ARTÍCULO 65. (PLAN ANUAL DE AUDITORÍA DE PROTECCIÓN DE DATOS).-**
- ARTÍCULO 66. (INSTANCIA DE ASISTENCIA TÉCNICA).-**
- ARTÍCULO 67. (INTEROPERABILIDAD ENTRE ENTIDADES PÚBLICAS).-**

CAPÍTULO II REGISTRO BOLIVIANO DE BANCOS DE DATOS

- ARTÍCULO 68. (DEFINICIÓN Y REGLAMENTACIÓN).-**
- ARTÍCULO 69. (INSCRIPCIÓN DE BANCOS DE DATOS).-**

CAPÍTULO III MECANISMOS DE SEGURIDAD

- ARTÍCULO 70. (FACTORES PARA DETERMINAR LAS MEDIDAS DE SEGURIDAD).-**
- ARTÍCULO 71. (NOTIFICACIÓN DE VIOLACIÓN DE LA SEGURIDAD A LA AUTORIDAD).-**
- ARTÍCULO 72. (NOTIFICACIÓN DE VIOLACIÓN DE LA SEGURIDAD AL TITULAR).-**

**CAPÍTULO IV
ESQUEMAS PREVENTIVOS DE CUMPLIMIENTO**

**SECCIÓN I
PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO**

ARTÍCULO 73. (PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO).-

**SECCIÓN II
EVALUACIÓN DEL IMPACTO PARA PROTECCIÓN DE DATOS PERSONALES**

**ARTÍCULO 74. (EVALUACIÓN DEL IMPACTO PARA PROTECCIÓN DE DATOS PERSONALES).-
ARTÍCULO 75. (TRATAMIENTOS QUE REQUIEREN UNA EVALUACIÓN DE IMPACTO).-**

**SECCIÓN III
AUTORREGULACIÓN**

**ARTÍCULO 76. (AUTORREGULACIÓN).-
ARTÍCULO 77. (OBJETO DE LOS CÓDIGOS DE CONDUCTA).-
ARTÍCULO 78. (PROCEDIMIENTO PARA LA PRESENTACIÓN, REVISIÓN Y APROBACIÓN DE UN
CÓDIGO).-
ARTÍCULO 79. (ORGANISMOS DE SUPERVISIÓN AUTORIZADOS).-
ARTÍCULO 80. (ALCANCES DE CERTIFICACIÓN).-**

**TÍTULO VIII
INFRACCIONES Y SANCIONES**

**CAPÍTULO I
CONDICIONES PARA IMPONER SANCIONES, TIPO DE SANCIONES Y CLASIFICACIÓN DE
INFRACCIONES**

**ARTÍCULO 81. (CONDICIONES PARA LA IMPOSICIÓN DE SANCIONES).-
ARTÍCULO 82. (TIPO DE SANCIÓN).-
ARTÍCULO 83. (INFRACCIONES GRAVES).-
ARTÍCULO 84. (INFRACCIONES MUY GRAVES).-
ARTÍCULO 85. (INFRACCIONES LEVES).-
ARTÍCULO 86. (RÉGIMEN DE SANCIONES PARA AUTORIDADES DE ENTIDADES PÚBLICAS Y
SUS FUNCIONARIOS).-
ARTÍCULO 87. (PLAZO DE PRESCRIPCIÓN PARA SANCIONES).-
ARTÍCULO 88. (ALCANCES DE LAS RESOLUCIONES DE LA AUTORIDAD DE PROTECCIÓN DE
DATOS PERSONALES).-**

**DISPOSICIONES ADICIONALES
DISPOSICIÓN ABROGATORIA Y DEROGATORIA
DISPOSICIONES FINALES.**

ANTEPROYECTO DE LEY DE PROTECCIÓN DE DATOS PERSONALES

EXPOSICIÓN DE MOTIVOS

El registro de los datos personales de todas las personas que habitan nuestro Estado, en medios no automatizados, semiautomatizados y automatizados; en soportes físicos y digitales, por su progresiva y acelerada implementación institucional, desde entidades privadas y públicas, hace necesario establecer obligaciones y derechos de las personas que registran y almacenan datos, así también de los ciudadanos que suministran sus datos personales.

Estas personas que registran y almacenan datos, a efectos de utilizarlos para fines relacionados con su fin social o empresarial, son los denominados “Responsables”, cuyas actividades están reguladas en un régimen de Principios, responsabilidades, obligaciones y mecanismos de autorregulación, bajo la supervisión de una Autoridad de Protección de Datos Personales que velará por el respeto de los derechos de las personas que suministren sus datos, estos últimos se denominan “Titulares”, a quienes conciernen los datos bajo protección de la ley.

A partir de esta relación jurídica, el hecho de realizar acciones respecto a datos personales, por ejemplo: obtenerlos, recogerlos, registrarlos, almacenarlos, acceder a ellos, organizarlos, estructurarlos, conservarlos, adaptarlos o modificarlos, indexarlos, extraerlos, consultarlos, utilizarlos, poseerlos, aprovecharlos, comunicarlos por transmisión, difusión o cualquier modalidad de habilitación de acceso, cotejarlos o interconectarlos, limitarlos, suprimirlos o destruirlos y en general cualquier uso o disposición que se haga respecto a esa información, constituye “tratamiento”. Y es este tratamiento el elemento que ya no debe permanecer en las penumbras del Estado Constitucional de Derecho.

De acuerdo a procesos de investigación efectuadas por la misma Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC, un gran porcentaje de la población internauta, utiliza como medio de información, comunicación y difusión, además de otras actividades económicas; las redes sociales, emergentes a partir de la internet. Internet en la que se manifiestan diferentes relaciones sociales, desde relaciones familiares, pasando por relaciones laborales, académicas, económicas y hasta lúdicas.

En este contexto social, los datos personales no dejan de ser derechos de la personalidad o más conocidos como derechos personalísimos. Sin embargo, su disponibilidad se ha diferido al contexto digital, desdoblado así, un instituto del derecho privado o derecho civil, dándole dinámica en el mundo real y en la realidad digital. Y el Anteproyecto de Ley, regula la dinámica de los datos personales, tanto en archivos no automatizados en soporte físico, como bancos de datos digitales.

Son algunas de las razones fácticas, que hacen necesaria la inclusión de un sistema de protección de datos personales en el ordenamiento jurídico boliviano.

En este contexto, y en relación directa con los fundamentos expuestos, la Constitución Política del Estado establece en su Artículo 21, Numeral 2, que las bolivianas y bolivianos tienen derecho a la privacidad. Asimismo, el párrafo VI de su Artículo 14 señala que las extranjeras y los extranjeros en el territorio boliviano tienen los derechos y deben cumplir los deberes establecidos en la Constitución, salvo las restricciones que ésta contenga.

La misma norma suprema en los Artículos 130 y 131, dispone los presupuestos, señala el procedimiento y la autoridad competente para que las personas puedan conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación. El párrafo I del Artículo 130 menciona los derechos de conocer, objetar, eliminar y rectificar que se constituyen en los derechos ARCO (acceso, rectificación, cancelación y oposición) en materia de

protección de datos personales. Es decir, que se puede interponer la Acción de Protección de Privacidad para ejercer la protección de datos personales o cuando se afecte su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honor, honra y reputación.

En concordancia con la Constitución, el Parágrafo II del Artículo 60 de la Ley N° 254, del Código Procesal Constitucional señala como presupuesto de legitimación pasiva, que la persona natural o jurídica, pública o privada, que compile datos personales en un registro, que independientemente de tener o no una finalidad comercial, este destinado a producir informes, aunque no los circule o difunda.

La privacidad en relación directa con los datos personales, y estos últimos como parte de los derechos de la personalidad, resaltan su naturaleza jurídica, para permitir la libre autodeterminación de las personas.

Justamente, la relación existente entre la privacidad, los datos personales y la dinámica económica junto al fenómeno del mercadeo de datos, hacen necesario regular los derechos que tienen las personas naturales respecto a sus datos personales, cuando estos últimos son suministrados a terceros y estos los registran en bancos de datos automatizados, semiautomatizados y no automatizados, con el fin almacenarlos, acceder a ellos, organizarlos, estructurarlos, conservarlos, adaptarlos o modificarlos, indexarlos, extraerlos, consultarlos, utilizarlos, poseerlos, aprovecharlos, comunicarlos por transmisión, difundirlos o habilitar su acceso, cotejo o interconexión; limitarlos, suprimirlos o destruirlos y en general cualquier uso o disposición de esos datos concernientes a una persona identificada o que la hagan identificable.

Para ello, justamente, a efectos de evitar que esos procedimientos que efectúan otras personas o entidades (denominados responsables, encargados, exportadores o terceros en la ley) respecto a los datos personales de las personas naturales, sean discrecionales o conducentes a actividades ilícitas, se evidencia la urgencia de regular derechos de las personas, obligaciones de los terceros e instituciones que hagan cumplir la ley, con la finalidad de regular y garantizar el derecho a la privacidad y la autodeterminación informativa y proteger los datos personales de las personas naturales.

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

El Comité Jurídico Interamericano de la Organización de Estados Americanos adoptó la propuesta de declaración de principios de privacidad y protección de datos personales en las Américas.

Los Estándares de Protección de Datos Personales elaborados por la Red Iberoamericana de Protección de Datos (RIPD) y aprobados en junio de 2017 en el XV Encuentro Iberoamericano de Protección de Datos, se constituyen en un conjunto de directrices orientadoras que contribuyen a la emisión de iniciativas regulatorias de protección de datos personales en la región iberoamericana de aquellos países que no cuentan con estos ordenamientos, o en su caso, sirva como referente para la modernización y actualización de las legislaciones existentes.

La Agenda Patriótica, aprobada mediante ley N° 650 de 19 de enero de 2015, ha establecido entre sus 13 pilares: 2. Socialización y universalización de los servicios básicos con soberanía para vivir bien, 4. Soberanía científica y tecnológica con identidad propia y 11. Soberanía y transparencia en la gestión pública bajo los principios de no robar, no mentir y no ser flojo.

El Plan de Desarrollo Económico y Social 2021-2025 “Reconstruyendo la Economía para vivir Bien, hacia la Industrialización con sustitución de importaciones”, aprobado mediante Ley N° 1407 de 10 de noviembre de 2021, establece entre sus ejes: 5. Educación, investigación, ciencia y tecnología para el fortalecimiento y desarrollo de capacidades y potencialidades productivas 7. (...) gestión pública digitalizada y transparente; seguridad y defensa integral con soberanía nacional.

El Artículo 19 (Petición del Habeas Data) del Decreto Supremo No. 28168 de 17 de mayo de 2005 regula un pequeño procedimiento para poder ejercer los derechos de actualización, complementación, eliminación o rectificación de datos personales en el ámbito del Poder Ejecutivo.

La Ley N° 164 constituye precedente normativo de genética legislativa respecto a la protección de datos personales en el ámbito de las telecomunicaciones. Asimismo, el Reglamento para el desarrollo de tecnologías de información y comunicación establece que “las entidades públicas promoverán la seguridad informática para la protección de datos en sus sistemas informáticos, a través de planes de contingencia desarrollados e implementados en cada entidad”. Además señala en el área de telecomunicaciones los lineamientos generales para el tratamiento de datos personales en el sector público y privado.

El Artículo 56 (Protección de datos personales) del Decreto Supremo No. 1793 de fecha 13 de noviembre de 2013 establece los lineamientos de cómo se deben tratar los datos personales por la Entidad de Certificación Autorizada que emite el certificado y la firma digital.

Ley No. 393 de Servicios Financieros considera el tratamiento de datos personales en el ámbito financiero por Burós de Información (Artículo 346 y siguientes), sobre la confidencialidad de la información (Artículo 472 y siguientes) y la Central de Riesgo Crediticia (Artículo 478 y siguientes).

El inciso v) del artículo 22 del Decreto Supremo N° 4857 de 06 de enero de 2023, establece que el Ministerio de la Presidencia ejerce la rectoría del Gobierno Electrónico y/o Digital de Tecnologías de Información y Comunicación para el sector público del Estado Plurinacional, a fin de establecer políticas, lineamientos y normativa específica para su implementación, seguimiento y control.

La Ley N° 1080, de Ciudadanía Digital, de 12 de julio de 2012, señala que las y los servidores y funcionarios de las instituciones previstas en la presente Ley, utilizarán los datos personales y información generada en la plataforma de interoperabilidad y ciudadanía digital únicamente para los fines establecidos en normativa vigente. II. El incumplimiento de la anterior previsión, será sujeto a responsabilidad por la función pública; para el caso de instituciones privadas que presten servicios públicos delegados por el Estado, el ente que ejerza supervisión respecto a sus funciones deberá establecer los mecanismos pertinentes a fin de dar cumplimiento a esta norma.

Son las relaciones fácticas y disposiciones constitucionales y legales que hacen necesaria y congruente, la inclusión del sistema de protección de datos en el ordenamiento jurídico boliviano.

ANTEPROYECTO DE LEY DE PROTECCIÓN DE DATOS PERSONALES

TÍTULO I

DISPOSICIONES GENERALES

CAPÍTULO I

GENERALIDADES

ARTÍCULO 1.(OBJETO).- La presente ley tiene por objeto garantizar el ejercicio del derecho a la protección de los datos personales.

ARTÍCULO 2. (FINALIDAD).- La presente ley tiene por finalidad regular el tratamiento legítimo, controlado e informado de los datos personales.

ARTÍCULO 3. (DEFINICIONES).- Para los efectos de la Ley, se entenderá por:

1. ANONIMIZACIÓN.- La aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o reidentificación de una persona natural sin esfuerzos desproporcionados.

2. AUTODETERMINACIÓN INFORMATIVA.- El derecho que permite al titular de datos garantizar su potestad de control y disposición sobre sus datos personales.

3. AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES.- La entidad pública, con autonomía, que vela por el cumplimiento de la Ley, su reglamentación y demás normativa que se emita para garantizar el debido tratamiento de datos personales, con atribuciones de promoción, investigación, supervisión, resolución, reglamentación y sanción.

4. BANCO DE DATOS PERSONALES.- Conjunto organizado de datos personales, en sus diversas formas o modalidades de creación, almacenamiento, organización, tipo de soporte, tratamiento, procesamiento, localización o acceso y difusión. Se divide en:

- 1. BANCO DE DATOS AUTOMATIZADO.**- Son creados, tratados y/o almacenados a través de programas de ordenador, programas informáticos o soporte lógico "software".
- 2. BANCO DE DATOS NO AUTOMATIZADO.**- Son creados, tratados y/o almacenados de forma manual, con ausencia de programas de ordenador o programas informáticos.

5. BANCOS DE DATOS PRIVADOS.- Las personas naturales y jurídicas podrán crear bancos de datos para el tratamiento de datos personales y constituirse en responsables de tratamiento; únicamente en congruencia con la finalidad del servicio que ofrecen, en estricto cumplimiento de las disposiciones contenidas en la presente Ley.

6. BLOQUEO DE DATOS.- Identificación y reserva de datos personales, mediante medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, así como autoridades competentes que lo requieran, en particular, de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mencionadas responsabilidades.

7. CONSENTIMIENTO.- Manifestación de la voluntad libre, específica, inequívoca e informada, del titular de datos, a través de la cual acepta y autoriza el tratamiento de los datos personales que le conciernen.

8. DATOS BIOMÉTRICOS.- Datos personales relativos a las características físicas, fisiológicas o conductuales, de una persona natural, que la identifiquen de manera única o confirmen su identificación única, y que se obtienen a partir de un tratamiento técnico específico.

9. DATOS GENÉTICOS.- Datos personales relativos a las características genéticas, heredadas o adquiridas, de una persona natural que proporcionen una información única sobre su fisiología o la salud, obtenidos en particular del análisis de una muestra biológica de tal persona.

10. DATOS RELATIVOS A LA SALUD.- Datos personales que refieren a la salud física o mental de una persona natural.

11. DATOS PERSONALES.- Cualquier información concerniente a una persona natural identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando esto no requiera plazos o actividades desproporcionadas.

12. DATOS SENSIBLES.- Datos personales que se refieren a los aspectos más íntimos del titular de datos, o cuya utilización indebida pueda dar origen a discriminación o conllevar un riesgo grave para éste. Entre los datos sensibles, de manera enunciativa no limitativa, se encuentran los datos de origen racial, convicciones religiosas, opiniones políticas, datos relativos a la salud, a la vida, a la orientación sexual, los datos genéticos y los biométricos.

13. DESTINATARIO DE DATOS.- Persona natural o jurídica, privada, pública o mixta, nacional, internacional o transnacional, o servicio, al que se transfieran datos personales, se trate o no de un tercero.

14. DISOCIACIÓN DE DATOS.- Todo tratamiento de datos personales y/o sensibles de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

15. ELABORACIÓN DE PERFILES.- Tratamiento automatizado consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona natural, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de una persona; entre otros.

16. ENCARGADO.- Persona natural o jurídica, pública o privada, servicio u otro organismo, ajeno a la organización del responsable, que efectúe el tratamiento de los datos personales por delegación del mencionado responsable.

17. EVALUACIÓN DE IMPACTO PARA LA PROTECCIÓN DE DATOS PERSONALES.- Análisis de carácter técnico, a cargo de los responsables, que les permite conocer, identificar y mitigar los posibles riesgos a los derechos y libertades de los titulares, derivado de un determinado tratamiento por realizar, debido a la naturaleza, alcance, contexto o finalidades, especialmente, cuando se utilizan tecnologías novedosas.

18. FUENTES DE ACCESO PÚBLICO.- Bancos de datos cuyo acceso o consulta puede ser efectuada en forma lícita por cualquier persona, siempre que no existan restricciones y/o impedimentos legales para su acceso o utilización, entre ellos la infracción al principio de finalidad, tales como listas de colegios profesionales, diario oficial, medios de comunicación, registros públicos que disponga la ley, entre otros. No se considerará fuente de acceso público cuando la información que se encuentra en esa fuente se haya obtenido ilícitamente o sea de procedencia ilícita.

19. LEY.- Ley de Protección de Datos Personales.

20. SEUDONIMIZACIÓN.- Tratamiento de datos personales de manera 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 natural identificada o identificable.

21. TITULAR DE DATOS.- Persona natural a quien corresponden los datos personales.

22. TRANSFERENCIA DE DATOS.- Toda comunicación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural, o servicio, distinto del titular de datos personales.

23. RESPONSABLE.- Persona natural o jurídica de carácter privado, autoridad pública, servicio u organismo que, solo o en conjunto con otros, determinen la finalidad, medios y el alcance del tratamiento de datos personales.

24. TERCERO.- Persona natural o jurídica, privada, pública o mixta, nacionales, extranjeras o transnacionales, autoridad pública, servicio u otra entidad, distinta del responsable, del encargado, del titular de datos y de las personas autorizadas, de manera directa, por el responsable o encargado para tratar datos personales.

25. TRATAMIENTO DE DATOS PERSONALES.- Cualquier operación o procedimiento, de carácter automatizado o no, como la obtención, recogida, registro, almacenamiento, acceso, organización, estructuración, conservación, adaptación o modificación, indexación, extracción, consulta, utilización, posesión, aprovechamiento, comunicación por transmisión, difusión o cualquier modalidad de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción y, en general, cualquier uso o disposición de datos personales.

26. VIOLACIÓN DE LA SEGURIDAD DE LOS DATOS PERSONALES.- Incidente de seguridad que ocasione la divulgación, destrucción, pérdida o alteración, accidental o ilícita, de los datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. Afectación indebida a la confidencialidad, disponibilidad o integridad de los datos.

ARTÍCULO 4. (ÁMBITO DE APLICACIÓN).- I. Estarán obligados a cumplir con las disposiciones de esta Ley las personas naturales o jurídicas de carácter privado, público o mixto, o servicios que traten datos personales.

II. La presente Ley aplica al tratamiento de datos personales, ya sea automatizado, total o parcialmente, o al tratamiento no automatizado, contenidos o destinados a ser incluidos en un banco de datos personales.

ARTÍCULO 5. (TRANSVERSALIDAD).- Esta Ley será el marco jurídico general y de referencia para todo tratamiento de datos personales en Bolivia, por lo que resultará aplicable para todos los sectores y materias.

El régimen general de protección de datos personales aquí previsto podrán ser complementados mediante disposiciones de carácter sectorial que se establezcan otras leyes.

ARTÍCULO 6. ÁMBITO DE APLICACIÓN TERRITORIAL).- I. La presente Ley se aplicará en el contexto de las actividades realizadas en su establecimiento del responsable o del encargado, con independencia de que el tratamiento tenga lugar en Bolivia o no.

II. Conforme a lo establecido, esta Ley aplicará en los siguientes supuestos:

- a) Al tratamiento de datos personales que se realice en cualquier parte del territorio nacional.
- b) Al responsable o encargado que se encuentre domiciliado en cualquier parte del territorio nacional.
- c) Al responsable o encargado, que no se encuentren domiciliados en el territorio nacional cuando las actividades del tratamiento estén relacionadas con la oferta de bienes o servicios, dirigidos a residentes en el territorio nacional, o estén relacionadas con el control del comportamiento de los citados residentes ubicados en territorio boliviano.
- d) Al responsable o encargado no establecido en territorio nacional y que utilice o recurra a medios, automatizados o no, situados en territorio nacional para tratar datos personales, salvo que dichos medios se utilicen solamente con fines de tránsito.

ARTÍCULO 7. (EXCEPCIONES A LA APLICACIÓN DE LA LEY).- I. La Ley no aplicará el tratamiento de datos personales en los siguientes casos:

- a) Los datos personales, contenidos o destinados, en banco de datos personales creados por personas naturales para fines exclusivamente relacionados con su vida privada, familiar o doméstica. Se entenderá por fines exclusivamente relacionados con su vida privada, familiar o doméstica, la utilización de datos personales en un entorno de amistad, parentesco o grupo personal cercano y que no tengan como propósito una divulgación o utilización comercial. Esta excepción únicamente puede ser utilizada por personas naturales, en ningún caso podrá aplicarse a personas jurídicas, autoridades, organismos públicos o servicios.
- b) Tratamiento de personas fallecidas.
- c) Tratamiento, por parte de las autoridades competentes, relativos a políticas y relaciones exteriores, en materia de información clasificada.
- d) Tratamiento, por parte de las autoridades competentes, con fines de prevención, investigación, detección, procesamiento de conductas penales o ejecución de medidas cautelares o sanciones penales.
- e) Tratamiento, por parte de las autoridades competentes, con fines de inteligencia y/o contrainteligencia, de la seguridad y defensa del Estado y la seguridad ciudadana.
- f) Tratamiento que se realice en ámbito del ejercicio de las libertades de emitir opinión y de informar reguladas por la Constitución, la Ley de Imprenta, otras leyes relativas y tratados internacionales.

II. En los casos de excepción, previstos en los incisos c) y e), deberá darse cumplimiento a los estándares internacionales en materia de derechos humanos y a los principios de licitud, finalidad y proporcionalidad previstos en esta Ley.

ARTÍCULO 8. (ESQUEMA DE EXCEPCIONES).- I. Cualquier excepción o limitación al derecho a la protección de datos personales, adicional a las ya descritas, será válida siempre que cumpla con los siguientes requisitos:

- a) Que esté prevista en una ley.
- b) Que se establezca la finalidad del tratamiento objeto de la excepción o limitación.
- c) Que se indique la o las categorías de datos personales que serán parte de la excepción o limitación.
- d) Que se señale cuál es el alcance de las limitaciones establecidas, por lo que se deberá señalar qué principios y/o derechos se estarían limitando mediante la excepción. Para cumplir con este requisito, se deberán limitar únicamente los principios y/o derechos que resulten necesarios y evitar hacer excepciones que exenten de la totalidad de los principios y/o derechos.
- e) Que los datos personales queden sujetos a garantías adecuadas para evitar que se vulneren los derechos y libertades fundamentales de los titulares de datos, con independencia de ser parte de una excepción o limitación.
- f) Que se indique cuál es el plazo por el que se conservarán los datos personales objeto de la excepción o limitación.

II. Toda ley que establezca una excepción o limitación deberá estar justificada en la necesidad, así como ser adecuada y proporcional en una sociedad democrática, respetando en todo momento los derechos y las libertades fundamentales de los titulares de datos.

CAPÍTULO II PRINCIPIOS RECTORES

ARTÍCULO 9. (PRINCIPIOS).- La interpretación y aplicación de la presente Ley, su reglamentación y desarrollo normativo ulterior, se funda en los siguientes principios:

1. LICITUD.- El tratamiento de datos personales debe realizarse de acuerdo a las bases jurídicas legítimas establecidas en la presente Ley, de lo dispuesto en la Constitución Política del Estado, las leyes bolivianas y los tratados internacionales de derechos humanos aplicables a la materia. El tratamiento será considerado lícito cuando cumpla mínimamente una de las siguientes condiciones:

- a) El titular de datos haya dado su consentimiento para el tratamiento de uno o varios fines específicos.
- b) Para la ejecución de un contrato en el que el titular de datos sea parte o para la aplicación de medidas precontractuales, a petición del citado titular de datos.
- c) El tratamiento sea necesario para proteger intereses vitales del titular de datos o de otra persona natural, como su vida, salud o integridad.
- d) El tratamiento sea realizado por el responsable para el cumplimiento de una orden judicial o requerimiento fiscal, fundado y motivado, en atención a un proceso abierto y en curso.
- e) Para el cumplimiento de funciones en interés público o en ejercicio de atribuciones habilitadas por ley a las autoridades y entidades públicas.

Para la satisfacción de intereses legítimos perseguidos por el responsable, o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales, del titular de datos, que requieran la protección de datos personales, en particular cuando el titular sea niña, niño o adolescente. Lo establecido en este supuesto no será aplicable a los tratamientos de datos personales por parte de autoridades o entidades públicas en ejercicio de sus funciones.

Cuando el tratamiento se base en el consentimiento del titular de datos el responsable deberá ser capaz de demostrar que el mencionado titular de datos consintió dicho tratamiento. Si el consentimiento del titular de datos se da en el contexto de una declaración escrita, que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción a la presente Ley.

El consentimiento puede ser revocado por el titular en cualquier momento, la revocatoria no tendrá efecto retroactivo, por lo que la revocatoria no afectará la licitud del tratamiento previo a la citada revocatoria. El responsable del tratamiento de datos personales deberá garantizar que retirar el consentimiento sea tan fácil como otorgarlo, al menos.

Corresponderá al responsable recabar y guardar la prueba de la existencia del consentimiento, por parte del titular de datos, a través de cualquier medio, conforme a derecho.

2.CONFIDENCIALIDAD.- En el tratamiento de los datos personales es obligación del Responsable y del Encargado garantizar la reserva de la información, incluso, después de finalizada la relación con el titular de datos.

3.CALIDAD.- Los datos personales que vayan a ser tratados deben ser veraces, completos, exactos, y, en su caso, actualizados y serán conservados durante el tiempo necesario para el cumplimiento de las finalidades que motivaron su tratamiento.

Los datos personales podrían conservarse durante períodos más largos, al indicado en el párrafo anterior, siempre que, por una parte, se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos y, por la otra, que los citados tratamientos estén sujetos a las garantías adecuadas para proteger los derechos y libertades fundamentales de los titulares de datos. Dichas garantías obligan a que se dispongan medidas técnicas y organizativas para lograr que se traten únicamente los datos personales indispensables. La seudonimización forma parte de las medidas técnicas y organizativas que se pueden emplear para cumplir con el presente párrafo.

Una vez que los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades que motivaron su tratamiento, el responsable deberá suprimirlos o eliminarlos de sus bancos de datos personales. En la supresión de los datos personales, el responsable implementará métodos y técnicas orientadas a la eliminación definitiva y segura de éstos.

4. FINALIDAD.- Los datos personales deben ser tratados para una finalidad determinada, explícita y legítima. El tratamiento no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de tratamientos con fines de investigación histórica, estadística o científica y siempre que, cualquiera de estos tratamientos, esté

sujeto a las garantías adecuadas para proteger los derechos y libertades fundamentales de los titulares de datos. Dichas garantías obligan a que se dispongan medidas técnicas y organizativas para lograr que se traten únicamente los datos personales indispensables. La seudonimización forma parte de las medidas técnicas y organizativas que se pueden emplear para cumplir con el presente párrafo.

5.PROPORCIONALIDAD.- Los datos personales objeto de tratamiento, serán los que resulten adecuados, pertinentes y limitados, al mínimo necesario, con relación a la o las finalidades que justifiquen su tratamiento.

6.SEGURIDAD.- Los datos personales objeto de tratamiento, deberán protegerse con medidas de seguridad físicas, técnicas, y administrativas, adecuadas y necesarias, para evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, así como para garantizar su confidencialidad, integridad y disponibilidad.

7.TRANSPARENCIA.- El responsable adoptará las medidas que resulten necesarias para informar al titular de datos de manera transparente, concisa, inteligible, de fácil acceso, con lenguaje claro y sencillo, por escrito u otros medios, sobre la existencia y las características esenciales del tratamiento, en términos de lo establecido en los artículos 11 o 12 de esta Ley, según corresponda.

8.RESPONSABILIDAD.- Los responsables deberán implementar medidas técnicas y organizacionales, adecuadas, para garantizar y acreditar el cumplimiento de los principios y obligaciones previstas en la presente Ley, así como para rendir cuentas sobre el tratamiento a los titulares de datos y la Autoridad de Protección de Datos Personales.

El responsable aplicará medidas técnicas y organizativas adecuadas para garantizar y demostrar que todo tratamiento de datos que realice cumpla con la presente Ley.

9.LEALTAD.- El responsable tratará los datos personales privilegiando la protección de los intereses del titular y absteniéndose de tratar éstos a través de medios engañosos o fraudulentos. Se considerarán desleales aquellos tratamientos que den lugar a una discriminación injusta o arbitraria contra los titulares de datos.

TÍTULO II

DERECHOS

CAPÍTULO I

EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA

ARTÍCULO 10. (DERECHOS DE LOS TITULARES).- La autodeterminación informativa en sus diferentes modalidades permite al titular, ejercer los siguientes derechos ante el responsable de tratamiento de los datos personales y otras instancias habilitadas por Ley:

1.DERECHO DE ACCESO INTEGRAL E IRRESTRICTO.- El titular de datos tiene derecho a solicitar el acceso a los datos personales que le conciernan, así como conocer toda la información relacionada con el tratamiento y los derechos emergentes del tratamiento.

2.DERECHO DE RECTIFICACIÓN O ACTUALIZACIÓN.- El titular tiene derecho a rectificar o corregir sus datos personales, ante el responsable, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados.

3.DERECHO DE CANCELACIÓN O SUPRESIÓN.- I. El titular tiene derecho a cancelar o suprimir sus datos personales, de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en posesión del responsable y dejen de ser tratados por este último cuando:

- a) El tratamiento no cumpla con las disposiciones de la presente Ley.
- b) El tratamiento no sea necesario o pertinente para el cumplimiento de la o las finalidades o bien, se haya cumplido la finalidad y no exista impedimento para su supresión.
- c) El titular de datos haya revocado su consentimiento y esa sea la única causa habilitante para el tratamiento.

- d) Exista una obligación señalada en Ley.
 - e) El titular de datos se haya opuesto al tratamiento y no subsistan otros motivos legítimos para el tratamiento.
 - f) En el caso de que los datos personales se hayan hecho públicos y el responsable esté obligado a suprimir dichos datos, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables, que estén tratando los datos personales, de la solicitud del titular de datos de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.
- II. No procede la cancelación cuando el tratamiento sea necesario:
- a) Para ejercer el derecho a las libertades de emitir opinión y de informar.
 - b) Para el cumplimiento de una obligación legal.
 - c) Por razones de interés público, especialmente en el ámbito de la salud pública.
 - d) Para tratamientos con fines históricos, estadísticos o científicos y para estudios o investigaciones que atiendan fines de interés público, y
 - e) Para la formulación, ejercicio o defensa de una reclamación administrativa o judicial.

4.DERECHO DE OPOSICIÓN.- El titular podrá oponerse al tratamiento de sus datos personales cuando:

- a) Existan motivos fundados y legítimos relativos a una situación concreta personal, incluida la elaboración de perfiles, salvo que el responsable acredite motivos legítimos imperiosos para el tratamiento, que prevalezcan sobre los intereses, los derechos y las libertades del titular, o para la formulación, el ejercicio o la defensa de reclamaciones.
- b) El tratamiento de sus datos personales tenga por objeto la publicidad o mercadotecnia directa, incluida la elaboración de perfiles, en la medida que esté relacionada con dicha actividad.
- c) Los datos sean objeto de tratamiento con fines de investigación científica, histórica o estadística, salvo que el tratamiento sea necesario por razones de interés público.

5. DERECHO A LA LIMITACIÓN DEL TRATAMIENTO DE LOS DATOS PERSONALES.- I. El titular de datos tendrá derecho a obtener del responsable la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

- a) El titular de datos impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos.
- b) El tratamiento sea ilícito y el titular de datos se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.
- c) El responsable ya no necesite los datos personales para los fines del tratamiento, pero el titular de datos los requiera para la formulación, el ejercicio o la defensa de reclamaciones.
- d) El titular de datos se haya opuesto al tratamiento mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del titular de datos.
- e) El tratamiento se haya limitado en virtud de este artículo, dichos datos sólo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del titular de datos o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público

II. Todo titular que haya obtenido la limitación del tratamiento será informado por el responsable antes del levantamiento de dicha limitación.

6.DERECHO A LA PORTABILIDAD.- I. El titular de datos tendrá derecho a recibir los datos personales que le concierne, que haya facilitado a un responsable, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable cuando el tratamiento esté basado en el consentimiento o en un contrato, y dicho tratamiento se efectúe por medios electrónicos o automatizados.

II.El titular de datos tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

III. El ejercicio del derecho a la portabilidad se entenderá sin perjuicio del derecho a la cancelación.

IV. La Autoridad de Protección de Datos Personales publicará las normas técnicas y procedimientos para la transmisión de la información, que permitan hacer efectivo y factible este derecho.

7. DERECHO A NO SER OBJETO DE DECISIONES AUTOMATIZADAS.- I. El titular tendrá derecho a no ser objeto de decisiones automatizadas, incluida la elaboración de perfiles, que le produzca efectos jurídicos, o le afecte significativamente, que se basen únicamente en tratamientos automatizados destinados a evaluar, sin intervención humana, aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

II. Lo establecido en el párrafo anterior no se aplicará en los siguientes casos cuando:

- a) La decisión automatizada sea necesaria para la celebración o la ejecución de un contrato entre el titular de datos y un responsable.
- b) La decisión automatizada esté autorizada por el Derecho boliviano y sea aplicable al responsable, siempre que dicho responsable establezca medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del titular de datos.
- c) La decisión automatizada se base en el consentimiento expreso del titular de datos.

III. El responsable estará impedido para realizar decisiones automatizadas basadas en datos personales sensibles, salvo que el titular haya dado su consentimiento expreso o sea necesario ese tratamiento por razones de interés público.

8. DERECHO A REVOCAR AUTORIZACIÓN.- El titular podrá ejercer el derecho a revocar su autorización o consentimiento respecto al tratamiento de sus datos personales, en cualquier tiempo y lugar, sea de forma escrita o verbal. Esta revocación será procesada de forma tan sencilla como la obtención del consentimiento.

9. DERECHO A LA INDEMNIZACIÓN.- El titular tiene derecho a ser indemnizado cuando hubiere sufrido daños y perjuicios, como consecuencia del incumplimiento de la presente Ley y su desarrollo reglamentario, por lo que podrá promover ante los tribunales competentes, las acciones a que haya lugar, para hacer efectivo este derecho.

ARTÍCULO 11. (INFORMACIÓN PARA EL TITULAR CUANDO LOS DATOS PERSONALES SE OBTENGAN DIRECTAMENTE DE DICHO TITULAR).- I. Cuando se obtengan datos personales directamente de su titular, el responsable, en el momento en que los datos personales se obtengan, pondrá a su disposición la información que se describe:

- a) La identidad y los datos de contacto del responsable.
- b) Los datos de contacto del delegado de protección de datos, en su caso.
- c) Los fines del tratamiento y el fundamento o base jurídica del tratamiento.
- d) Cuando el tratamiento se base en los intereses legítimos del responsable o de un tercero, se deberá informar al respecto.
- e) Los destinatarios o las categorías de destinatarios de los datos personales, en su caso.
- f) Las transferencias internacionales de datos que pretenda llevar a cabo el responsable, así como la referencia a las garantías adecuadas y a los medios para obtener una copia de las citadas garantías o al hecho de que se hayan prestado.
- g) La posibilidad de ejercer los derechos de acceso, rectificación, supresión, limitación del tratamiento, oposición, así como el derecho a la portabilidad de los datos.
- h) El derecho a retirar el consentimiento en cualquier momento.
- i) El derecho a presentar reclamaciones ante la Autoridad de Protección de Datos Personales.
- j) Si la comunicación de datos personales forma parte de los requisitos legales o contractuales, o

un requisito necesario para suscribir un contrato, y si el titular de datos está obligado a facilitar los datos personales y a ser informado de las posibles consecuencias de no facilitar tales datos.

- k) La existencia de decisiones automatizadas, incluida la elaboración de perfiles, y, al respecto, al menos información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el titular de datos.

II. Cuando el responsable proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al titular de datos, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente, conforme a lo establecido en este artículo.

ARTÍCULO 12. (INFORMACIÓN PARA EL TITULAR CUANDO LOS DATOS PERSONALES NO SE HAN OBTENIDO DEL TITULAR).- I. Cuando los datos personales no se hayan obtenido de su titular, el responsable pondrá a su disposición la información que se describe:

responsable pondrá a su disposición la información que se describe:

- a) La identidad y los datos de contacto del responsable.
- b) Los datos de contacto del delegado de protección de datos, en su caso.
- c) Los fines del tratamiento y el fundamento o base jurídica del tratamiento.
- d) Las categorías de datos personales de que se trate.
- e) Cuando el tratamiento se base en los intereses legítimos del responsable o de un tercero, se deberá informar al respecto.
- f) Los destinatarios o las categorías de destinatarios de los datos personales, en su caso.
- g) Las transferencias internacionales de datos que pretenda llevar a cabo el responsable, así como la referencia a las garantías adecuadas y a los medios para obtener una copia de dichas garantías o al hecho de que se hayan prestado.
- h) La posibilidad de ejercer los derechos de acceso, rectificación, supresión, limitación del tratamiento, oposición, así como el derecho a la portabilidad de los datos.
- i) El derecho a retirar el consentimiento en cualquier momento.
- j) El derecho a presentar reclamaciones ante la Autoridad de Protección de Datos Personales.
- k) La fuente de la que proceden los datos personales.
- l) La existencia de decisiones automatizadas, incluida la elaboración de perfiles, y, al respecto, al menos información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el titular de datos.

II. Cuando el responsable proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al titular de datos, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente, conforme a lo establecido en este artículo.

ARTÍCULO 13. (PLAZO PARA LA PUESTA A DISPOSICIÓN DE LA INFORMACIÓN CUANDO LOS DATOS NO SE OBTUVIERON DE SU TITULAR).- El responsable facilitará la información indicada en los incisos a) al l), del artículo 12 de la presente Ley, conforme a lo siguiente:

- a) Dentro de un plazo razonable, una vez obtenidos los datos personales, sin que transcurra más de un mes a partir de su obtención.
- b) En el caso de que los datos personales vayan a utilizarse para comunicación con el titular, a más tardar en el momento de la primera comunicación con dicho titular.
- c) De tenerse previsto comunicarlos a otro destinatario, a más tardar en el momento en que los

datos personales sean comunicados por primera vez.

ARTÍCULO 14. (CASOS DE EXCEPCIÓN AL DERECHO A LA INFORMACIÓN SI LOS DATOS PERSONALES NO SE OBTUVIERON DE SU TITULAR).- I. Las disposiciones relativas al derecho a la información, cuando dichos datos no se obtuvieron del titular, no serán aplicables en los siguientes casos:

- a) El titular ya disponga de la información.
- b) La comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos o en la medida en que se pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del titular de datos.

II. La Autoridad de Protección de Datos Personales publicará los criterios conforme a los cuáles se considerará que una comunicación puede resultar imposible o suponer un esfuerzo desproporcionado, en el contexto del inciso b) del presente artículo.

CAPÍTULO II

EJERCICIO DE DERECHOS

ARTÍCULO 15. (GRATUIDAD DE LOS DERECHOS).- I. El ejercicio de los derechos previstos en la presente Ley será gratuito, sin perjuicio del costo de los materiales de reproducción y envío, en su caso.

II. La Autoridad de Protección de Datos Personales publicará los criterios conforme a los cuales los responsables podrán fijar los costos de reproducción y envío para evitar que con los mismos se afecte el ejercicio de los derechos establecidos en esta Ley.

III. El responsable no podrá establecer, para la presentación de solicitudes para el ejercicio de derechos, un servicio o medio que implique un costo para el titular de datos.

ARTÍCULO 16. (ACREDITACIÓN DE IDENTIDAD).- I. Para el ejercicio de los derechos establecidos en esta Ley será necesario acreditar la identidad del titular de datos y, en su caso, la identidad y personalidad con la que actúe su representante.

II. Únicamente por disposición legal, o en su caso, por mandato judicial, el ejercicio de los derechos previstos en esta Ley será factible a través de una persona distinta al titular de datos o a su representante.

III. Para el ejercicio de los derechos de menores o de personas que se encuentren en estado de interdicción o incapacidad se actuará conforme a las reglas de representación dispuestas en la legislación aplicable.

ARTÍCULO 17. (COMUNICACIÓN Y MODALIDADES DE EJERCICIO DE LOS DERECHOS DEL

TITULAR DE DATOS).- I. La información, con motivo del ejercicio de los derechos previstos en esta Ley, será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el titular de datos, la información podrá facilitarse verbalmente siempre que demuestre su identidad por otros medios.

II. Cuando el titular de datos presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el propio titular de datos solicite que se facilite de otro modo.

ARTÍCULO 18. (IMPROCEDENCIA DE LAS SOLICITUDES DE EJERCICIO DE DERECHOS).- I.

Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable podrá:

- a) Cobrar un canon razonable en función de los costos administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada. La Autoridad de Protección de Datos Personales publicará los criterios para el establecimiento de cánones razonables.
- b) Negarse a actuar respecto de la solicitud.

II. El responsable tendrá la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

ARTÍCULO 19. (PLAZO DE RESPUESTA PARA SOLICITUDES DE EJERCICIO DE DERECHOS).- I.

El responsable deberá establecer procedimientos internos sencillos que permitan el ejercicio de los derechos previstos en esta Ley, cuyo plazo de respuesta no deberá exceder de (30) treinta días hábiles contados a partir del día siguiente a la recepción de la solicitud.

II. El plazo de respuesta podrá ser ampliado, una sola vez, hasta por (20) veinte días hábiles adicionales cuando así lo justifiquen las circunstancias, y siempre que se le notifique al titular de datos la ampliación del plazo, antes de que venza el plazo de (30) treinta días.

ARTÍCULO 20. (REQUISITOS DE LA SOLICITUD PARA EL EJERCICIO DE DERECHOS).- I.

En la solicitud para el ejercicio de derechos no podrán exigirse mayores requisitos que los siguientes:

- a) El nombre del titular de datos y medio para recibir notificaciones.
- b) Los documentos que acrediten la identidad del titular de datos y, en su caso, la personalidad e identidad de su representante.
- c) La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos.
- d) La descripción del derecho a ejercer, así como las razones y/o documentos que sustenten su solicitud. Con relación a una solicitud de cancelación, el titular de datos deberá señalar las causas que lo motiven a solicitar la supresión de sus datos personales. En el caso de la solicitud de oposición, el titular de datos deberá manifestar las causas legítimas o la situación específica que lo llevan a solicitar el cese en el tratamiento. En el caso del derecho a la rectificación, el titular de datos deberá aportar la documentación que resulte necesaria para demostrar la realidad de sus datos personales.

II. En el caso de que la solicitud de ejercicio de derechos no satisfaga alguno de los requisitos descritos en este artículo, el responsable podrá prevenir al titular de datos dentro de los (5) cinco días hábiles siguientes a la presentación de la solicitud de ejercicio de derechos, por una sola ocasión, para que

subsane las omisiones dentro de un plazo de (10) diez días hábiles contados a partir del día siguiente al de la notificación.

III. Transcurrido el plazo sin subsanar o atender la observación, se tendrá por no presentada la solicitud de ejercicio de derechos.

IV. La observación tendrá por efecto suspender el plazo con el que cuenta el responsable para responder la solicitud de ejercicio de derechos.

ARTÍCULO 21. (RECEPCIÓN Y ATENCIÓN DE SOLICITUDES DE EJERCICIO DE DERECHOS).- I.

Las solicitudes para el ejercicio de derechos deberán presentarse ante el responsable, mediante escrito, formatos, medios electrónicos o cualquier otro medio que el citado responsable tenga habilitado para ese fin.

II. El responsable deberá tramitar toda solicitud para el ejercicio de derechos y entregar constancia de su recepción, ineludiblemente.

III. La Autoridad de Protección de Datos Personales publicará guías y formatos para la presentación de solicitudes de ejercicios de derechos y de ese modo facilitar a los titulares de datos el ejercicio de sus derechos.

IV. Los medios y procedimientos habilitados por el responsable para atender las solicitudes para el ejercicio de derechos deberán ser de fácil acceso y con la mayor cobertura posible, considerando el perfil de los titulares y la forma en que mantienen contacto cotidiano o común.

ARTÍCULO 22. (CASOS EN LOS QUE NO PROCEDE EL EJERCICIO DE DERECHOS).- I. Las únicas causas en las que el ejercicio de derechos no será procedente son las siguientes:

- a) El tratamiento sea necesario para el cumplimiento de un objetivo de interés público.
- b) El tratamiento sea necesario para el ejercicio de las funciones propias de las autoridades u organismos públicos.
- c) Cuando el tratamiento sea necesario para el cumplimiento de una disposición legal.

II. En todos los casos anteriores, el responsable deberá informar al titular de datos las razones por las que consideró que existe una causa de improcedencia, debiendo en su caso, acompañar las constancias que respalden su respuesta.

ARTÍCULO 23. (MEDIO DE IMPUGNACIÓN CONTRA LAS RESPUESTAS A SOLICITUDES DE EJERCICIO DE DERECHOS).-

Los titulares que se encuentren inconformes con la respuesta a una solicitud para el ejercicio de derechos, o bien, ante la falta de respuesta a una solicitud, podrán presentar una reclamación ante la Autoridad de Protección de Datos Personales.

**CAPÍTULO III
RECLAMACIONES**

ARTÍCULO 24. (PROCEDIMIENTO DE RECLAMACIÓN).- I. Los procedimientos de reclamación se tramitarán ante la Autoridad de Protección de Datos Personales en los siguientes supuestos:

- a) De oficio cuando dicha Autoridad tenga conocimiento de indicios que le hagan presumir la existencia de infracciones a la Ley.
- b) Mediante denuncia, presentada por cualquier persona, que haga de su conocimiento la comisión de posibles infracciones a la Ley. No será un impedimento jurídico el que el denunciante no guarde relación alguna con la persona denunciada y/o el tratamiento materia de la denuncia.
- c) En los casos en los que los titulares de datos reclamen que no ha sido atendida su solicitud de ejercicio de los derechos.

II. Para el supuesto establecido en el inciso c), el derecho a presentar una denuncia subsistirá por el periodo de un (1) año contado a partir del día en que haya ocurrido la situación denunciada. Si se trata de actos continuos, el plazo se contará a partir del día del último hecho o efecto producido.

ARTÍCULO 25. (TRÁMITE DE RECLAMACIONES A TRAVÉS DE PLATAFORMAS DIGITALES).-

Además de los esquemas presenciales, el procedimiento de reclamación podrá tramitarse, parcial o totalmente, a través de la o las plataformas digitales que la Autoridad de Protección de Datos Personales habilite para tal fin. La citada Autoridad publicará las reglas conforme a las cuales se gestionarán las distintas etapas del procedimiento a través de las plataformas digitales.

ARTÍCULO 26. (INICIO DEL PROCEDIMIENTO Y DURACIÓN).- I. El procedimiento de reclamación iniciará conforme a las reglas que se describen:

- a) Si el procedimiento se refiere, únicamente, a la falta de atención de una solicitud de ejercicio de los derechos establecidos en esta Ley, se iniciará la admisión a trámite. La Autoridad de Protección de Datos Personales contará con un plazo de seis (6) meses para resolver el procedimiento. El plazo se contará desde la fecha en que se hubiera notificado al reclamante el acuerdo de admisión a trámite. Transcurrido ese plazo, el titular podrá considerar estimada su reclamación.
- b) Si el procedimiento tiene por objeto la determinación de la posible existencia de una infracción a esta Ley, se iniciará mediante acuerdo de inicio adoptado por propia iniciativa o como consecuencia de una reclamación. El procedimiento iniciará por acuerdo de admisión a trámite. Admitida a trámite la reclamación, así como en los supuestos en que la Autoridad de Protección de Datos Personales actúe por propia iniciativa, con carácter previo al acuerdo de inicio, podrá existir una fase de actuaciones previas de investigación, que se regirá por lo previsto en el artículo 89 de esta Ley. El procedimiento de reclamación, para estos casos, tendrá una duración máxima de nueve meses contados a partir de la fecha del acuerdo de inicio o, en su caso, del proyecto de acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones.

ARTÍCULO 27. (CASOS EN LOS QUE NO SE ADMITIRÁN LAS RECLAMACIONES).- I. No se admitirán las reclamaciones presentadas cuando no versen sobre cuestiones de protección de datos personales, carezcan manifiestamente de fundamento, sean abusivas o no aporten indicios racionales de la existencia de una infracción.

II. Tampoco se admitirán las reclamaciones cuando el responsable o encargado, previa advertencia

realizada por la Autoridad de Protección de Datos Personales, hubiera implementado las medidas correctivas destinadas a poner fin al posible incumplimiento de la Ley y, además, se presente alguna de las siguientes circunstancias:

- a) Que no se haya causado perjuicio al titular de datos en el caso de las infracciones leves.
- b) Que el derecho del afectado quede plenamente garantizado mediante la aplicación de las medidas.

III. La Autoridad de Protección de Datos Personales publicará las reglas conforme a las cuales se gestionarán las actuaciones en torno a los dos incisos previstos en este artículo.

ARTÍCULO 28. (ACTUACIONES PREVIAS DE INVESTIGACIÓN).- I. Antes de la adopción del acuerdo de inicio de procedimiento, y una vez admitida a trámite la reclamación si la hubiese, la Autoridad de Protección de Datos Personales podrá llevar a cabo actuaciones previas de investigación a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento.

II. Las actuaciones previas de investigación tendrán una duración máxima de seis (6) meses contados desde la fecha del acuerdo de admisión a trámite o de la fecha del acuerdo por el que se decida su iniciación cuando la Autoridad de Protección de Datos Personales actúe por propia iniciativa. El plazo podrá ampliarse por tres (3) meses adicionales cuando la complejidad del asunto así lo requiera. La Autoridad de Protección de Datos Personales publicará los criterios conforme a los cuales se determinará que el plazo de un procedimiento puede ser ampliado.

ARTÍCULO 29. (INICIO DEL PROCEDIMIENTO SANCIONADOR).- Concluidas, en su caso, las actuaciones a las que se refiere el artículo anterior, corresponderá a la Autoridad de Protección de Datos Personales, cuando así proceda, dictar el inicio del procedimiento sancionador, en que se concretarán los hechos, la identificación de la persona o entidad contra la que se dirija el procedimiento, la infracción que hubiera podido cometerse y su posible sanción.

ARTÍCULO 30. (CONFIDENCIALIDAD Y FE PÚBLICA DE LOS FUNCIONARIOS).- I. El personal de la Autoridad de Protección de Datos Personales que participe en el procedimiento de reclamación estará obligado a mantener la confidencialidad respecto de la información a la que tengan conocimiento. La confidencialidad se mantendrá por tiempo indefinido.

II. El responsable o encargado, contra el que se haya presentado la reclamación, estará impedido para negar el acceso a la información y peticiones que la Autoridad de Protección de Datos Personales le formule, con motivo de un procedimiento de verificación. Tampoco podrá invocar la reserva o secreto.

III. El personal que participe en los procedimientos de reclamación, de parte de la Autoridad de Protección de Datos Personales, gozará de fe pública para el desarrollo de sus funciones en el contexto de dichos procedimientos.

ARTÍCULO 31. (MEDIDAS CAUTELARES).- I. La Autoridad de Protección de Datos Personales podrá acordar, motivadamente, la adopción de medidas cautelares necesarias y provisionales para la salvaguarda del derecho fundamental a la protección de datos personales.

II. En los casos en que la Autoridad de Protección de Datos Personales considere que la continuación del tratamiento, su comunicación o transferencia conlleva un daño grave del derecho a la protección de datos personales, podrá ordenar a los responsables o encargados el bloqueo de los datos y la cesación de su tratamiento y, en caso de incumplirse por los responsables o encargados dichos mandatos, proceder a su inmovilización.

III. Las medidas cautelares podrán ser solicitadas por el reclamante en el caso de advertir la posibilidad o existencia de un daño al derecho a la protección de datos personales.

VI. La Autoridad de Protección de Datos Personales publicará criterios que permitan determinar en qué casos se está en presencia de un daño grave, en el contexto de este artículo.

V. Estas medidas sólo podrán tener una finalidad correctiva y serán de carácter temporal

ARTÍCULO 32. (DESARROLLO DEL PROCEDIMIENTO).- A partir de lo dispuesto en el presente capítulo, en el Reglamento de la Ley y/o en las reglas que publique al respecto la Autoridad de Protección de Datos Personales, se desarrollarán las etapas para la tramitación del procedimiento de reclamación, incluida la etapa del procedimiento sancionador, así como todos aquellos aspectos de procedimiento necesarios para su gestión eficiente.

TÍTULO III
RESPONSABLES, ENCARGADOS Y DELEGADO DE TRATAMIENTO DE DATOS PERSONALES
CAPÍTULO I
RESPONSABLES Y ENCARGADOS FUERA DEL TERRITORIO

ARTÍCULO 33. (RESPONSABLES O ENCARGADOS ESTABLECIDOS FUERA DE TERRITORIO BOLIVIANO).- I. En el caso de que un responsable o encargado que no se encuentren domiciliados en el territorio nacional cuando las actividades del tratamiento estén relacionadas con la oferta de bienes o servicios, dirigidos a residentes en el territorio nacional o estén relacionadas con el control del comportamiento de los ciudadanos residentes en Bolivia, dicho responsable o encargado deberán designar por escrito un representante que estará establecido en Bolivia.

II. La obligación establecida en el párrafo anterior no será aplicable en los siguientes casos:

- a) Si se está en presencia de un tratamiento que sea ocasional, que no incluyan el manejo a gran escala de datos sensibles y que sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento.
- b) En el caso de autoridades u organismos públicos

III. El representante deberá atender, junto al responsable o al encargado, o en su lugar, a las consultas, en particular, de la Autoridad de Protección de datos Personales y de los titulares de datos, a fin de garantizar el cumplimiento de la Ley.

IV. La designación de un representante se entenderá sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable o encargado.

ARTÍCULO 34. (COOPERACIÓN CON LA AUTORIDAD).- El responsable y el encargado y, en su caso, sus representantes cooperarán con la Autoridad de Protección de datos Personales en el

desempeño para que dicha autoridad esté en posibilidad de llevar a cabo un adecuado ejercicio de sus funciones.

ARTÍCULO 35. (CORRESPONSABILIDAD EN EL TRATAMIENTO).- I. Cuando dos o más personas sean responsables, y definan conjuntamente los objetivos y los medios del tratamiento, serán considerados corresponsables del tratamiento.

II. Siendo corresponsables, determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respecto a las obligaciones que señala la presente Ley, en particular, en cuanto al ejercicio de los derechos del titular y a sus respectivas obligaciones de suministro de información conforme a los artículos 11 y 12 de esta Ley.

III. El acuerdo de responsabilidades, al que refiere el párrafo anterior, contendrá las funciones y relaciones de corresponsabilidad respecto al titular, se pondrá, en sus aspectos esenciales, a disposición del titular. Con independencia de la existencia del acuerdo de responsabilidades, los titulares podrán ejercer sus derechos, indistintamente, con cualquiera de los responsables.

CAPÍTULO II

ENCARGADO

ARTÍCULO 36. (ALCANCES DE LA PARTICIPACIÓN DEL ENCARGADO).- I. En los casos en los que el responsable haya contratado a algún encargado, éste realizará las actividades de tratamiento sin ostentar poder alguno de decisión sobre el alcance y contenido del citado tratamiento, por lo que su actuación se limitará a las instrucciones documentadas que haya recibido por parte del responsable.

II. En el caso de que el encargado incumpla las instrucciones del responsable y decida por sí mismo sobre el alcance, contenido, medios y demás cuestiones del tratamiento, asumirá la calidad de responsable, conforme a la presente Ley, respecto del tratamiento o tratamientos en los que haya actuado más allá de las instrucciones documentadas. Lo anterior, sin perjuicio de otras responsabilidades en que incurra con su actuar indebido.

III. El responsable únicamente podrá elegir un encargado que ofrezca garantías suficientes, para aplicar medidas técnicas y organizativas, que permitan que el tratamiento sea conforme a lo previsto en la Ley y garantice la protección de los derechos del titular de datos. Los encargados podrán valerse de los esquemas de autorregulación previstos en esta Ley para demostrar que resultan idóneos para ser elegidos.

ARTÍCULO 37. (REGLAS DE ACTUACIÓN PARA EL ENCARGADO).- I. La relación entre el responsable y el encargado se regirá por un contrato o cualquier otro instrumento jurídico, que vincule al encargado con el responsable, y se establecerá, al menos, el objeto, alcance, contenido, duración, naturaleza y finalidad del tratamiento, el tipo de datos personales, las categorías de titulares, así como las obligaciones y responsabilidades del responsable y del encargado.

II. El contrato o cualquier otro instrumento jurídico, que vincule al encargado con el responsable, deberá estipular las siguientes obligaciones para el encargado:

- a) Tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias internacionales de datos personales sea a otro país o una organización internacional, salvo que esté obligado en virtud de un mandato legal o de un tratado o cualquier otro instrumento internacional vinculante para Bolivia.
- b) Garantizar que las personas autorizadas para tratar datos personales se hayan obligado a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad.
- c) Cumplir con el principio de seguridad e implementar las medidas de seguridad a las que refiere el artículo 68 de la presente Ley.

- d) Apoyar al responsable, siempre que forme parte de los acuerdos documentados entre el responsable y el encargado, para que dicho responsable esté en posibilidades de responder a las solicitudes que reciba de los titulares de datos con motivo del ejercicio de los derechos previstos en esta Ley.
- e) Asistir al responsable, siempre que forme parte de los acuerdos documentados entre el responsable y el encargado, con el cumplimiento de las obligaciones relacionadas con la privacidad desde el diseño y por defecto, las evaluaciones de impacto para protección de los datos personales, el delegado de protección de datos y los mecanismos de autorregulación, en lo que resulte aplicable a cada responsable.
- f) Suprimir, devolver o comunicar a un nuevo encargado, a elección del responsable, los datos personales objeto de tratamiento una vez concluida la prestación de servicios con el responsable, sin que pueda conservar copia alguna, salvo que una disposición legal exija la conservación de los datos personales.
- g) Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

ARTÍCULO 38. (MODELOS DE CLÁUSULAS CONTRACTUALES).- La Autoridad de Protección de Datos Personales elaborará y pondrá a disposición, de los responsables y encargados, modelos de cláusulas contractuales y/u otros instrumentos jurídicos para orientar y facilitar el cumplimiento del artículo 37 de esta Ley, sobre las reglas de actuación del encargado.

ARTÍCULO 39. (CONTRATACIÓN DE UN ENCARGADO POR PARTE DEL ENCARGADO AUTORIZADO).- Existe la posibilidad de que un encargado, ya autorizado por el responsable, contrate a otro encargado, para apoyarlo con el tratamiento para el que fue contratado, siempre que se cumpla con los siguientes requisitos:

- a) Lo haya autorizado previamente el responsable y esté documentada la autorización. Esto deberá cumplirse siempre que se contrate a un nuevo encargado por parte del encargado ya autorizado.
- b) El encargado autorizado por el responsable y el encargado por contratar celebren un contrato u otro instrumento jurídico vinculante en el que se establezcan los alcances de la contratación. Para su validez, este contrato o instrumento jurídico deberá ser aprobado por el responsable, con la finalidad de que dicho responsable valore y, en su caso, valide y asuma los alcances de los servicios a contratar por el encargado por él autorizado. La aprobación de parte del responsable deberá documentarse.

CAPÍTULO III DELEGADO DE PROTECCIÓN DE DATOS

ARTÍCULO 40. (OBJETIVO DEL DELEGADO).- I. Es la persona natural o jurídica cuyo objetivo es constituirse, al interior del responsable o encargado, en el garante del cumplimiento de la presente Ley, su Reglamento y demás regulación aplicable. El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado o desempeñar sus funciones a través de un contrato de servicios.

II. El delegado de protección de datos debe designarse teniendo en consideración su perfil profesional y en específico que cuente con conocimientos especializados en Derecho, experiencia probada en datos personales, así como su capacidad para desempeñar las funciones indicadas en el artículo 42 de esta Ley. Para ser designado delegado no será necesario poseer un tipo de titulación y/o estar certificado, lo que no obsta para que mediante un título y/o certificación se acredite que se posee el perfil profesional idóneo.

ARTÍCULO 41. (INDEPENDENCIA DEL DELEGADO EN EL EJERCICIO DE SUS FUNCIONES).-I. El delegado de protección de datos debe actuar de forma independiente en el ejercicio de sus funciones.

II.El responsable y el encargado garantizarán que el delegado de protección de datos participe de forma adecuada y oportunamente en todas las cuestiones relativas a la protección de datos personales.

III.El responsable y el encargado respaldarán al delegado de protección de datos en el desempeño de sus funciones, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, así como para el mantenimiento de sus conocimientos especializados.

IV.El responsable y el encargado garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones.

El delegado de protección de datos no debe ser destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

VI.El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones.

ARTÍCULO 42. (FUNCIONES DEL DELEGADO DE PROTECCIÓN DE DATOS).- El delegado de protección de datos tendrá, al menos, las siguientes funciones:

- a) Informar y asesorar al responsable o al encargado y a los empleados que participen en cualquier fase del tratamiento, sobre las obligaciones a las que están sujetos con motivo de esta Ley y demás regulación aplicable en el ámbito de la protección de los datos personales.
- b) Supervisar el cumplimiento de la Ley, y demás regulación aplicable, así como de las políticas del responsable o del encargado en materia de protección de datos personales.
- c) Asesorar en materia de elaboración de evaluaciones de impacto para protección de los datos personales y supervisar su aplicación.
- d) Cooperar con la Autoridad de Protección de Datos Personales y ser su punto de contacto para cualquier cuestión en de datos personales.

ARTÍCULO 43. (DESIGNACIÓN DEL DELEGADO DE PROTECCIÓN DE DATOS).- El responsable y el encargado designarán un delegado de protección de datos en los casos que se describen:

- a) El tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial.
- b) Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala.
- c) Las actividades principales del responsable o del encargado consistan en el tratamiento de alta sensibilidad de datos.
- d) Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.
- e) El responsable o el encargado publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la Autoridad de Protección de Datos Personales.

TÍTULO IV

TRATAMIENTO DE DATOS PERSONALES SENSIBLES Y DE TUTELA ESPECIAL

ARTÍCULO 44. (PROHIBICIÓN DE TRATAMIENTO DE DATOS PERSONALES SENSIBLES).- Queda prohibido el Tratamiento de datos personales sensibles, excepto en los siguientes casos:

- a) El titular de datos haya dado su consentimiento explícito para el tratamiento de sus datos sensibles.
- b) El tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable o del titular de datos, en el ámbito del derecho laboral y la seguridad social.
- c) Para salvaguardar los intereses vitales del titular de datos, o de un tercero, y el titular de datos se encuentre física o jurídicamente incapacitado para otorgar su consentimiento. En esta circunstancia, los representantes legales deberán otorgar su autorización.
- d) El tratamiento sea necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.
- e) El tratamiento tenga una finalidad histórica, estadística o científica. En este caso deberán adoptarse las medidas conducentes para proteger los derechos de los titulares de datos.
- f) El tratamiento se refiera a datos personales que el titular de datos haya hecho manifiestamente públicos.
- g) El tratamiento sea necesario por razones del interés público, de conformidad con la Constitución, las leyes y el marco jurídico en general, por lo que deberá ser proporcional al fin perseguido y respetar los derechos de los titulares de datos.

ARTÍCULO 45. (INTERÉS SUPERIOR DEL MENOR Y CONSENTIMIENTO).- I. Las autoridades y organismos públicos competentes, con el apoyo de la Autoridad de Protección de Datos Personales, diseñarán e implementarán programas de estudio con contenidos educativos que le permita a los menores un uso responsable de sus datos personales en el contexto de la era digital.

II. En virtud del interés superior de las niñas, niños y adolescentes, queda prohibido el tratamiento de sus datos personales, excepto cuando los padres, la o el titular de la guarda o patria potestad haya brindado su consentimiento al efecto y siempre que no le ocasione perjuicio.

ARTÍCULO 46. (TRATAMIENTO DE DATOS PERSONALES DE PERSONAS CON CAPACIDADES DIFERENTES).- I. El consentimiento para el tratamiento de datos personales de personas con capacidades diferentes y declaradas interdictas, será otorgado por la o el tutor habilitado por Ley.

II. Asimismo, para las personas con capacidades diferentes no interdictas se les otorgará la información en los medios idóneos para su comprensión, asegurando dicho extremo de manera documental.

ARTÍCULO 47. (TRATAMIENTO DE DATOS PERSONALES DE PERSONAS FALLECIDAS).- I. Las personas naturales, vinculadas al fallecido, que demuestre poseer un interés legítimo, respecto de los datos personales de la persona fallecida, podrán ejercer ante el responsable los derechos de acceso y, en su caso, de rectificación o supresión, respecto de los datos de la persona fallecida.

II. La Autoridad de Protección establecerá criterios para facilitar la determinación de casos de interés jurídico y legítimo, en el contexto del párrafo anterior.

TÍTULO V

TRATAMIENTO DE DATOS PERSONALES EN ÁMBITOS ESPECÍFICOS

ARTÍCULO 48. (DATOS EN MEDIOS DE COMUNICACIÓN).- I. Los datos personales difundidos en medios de comunicación convencionales y difusión masiva como la televisiva, radial, escrita, plataformas web y medios de difusión a partir de tecnologías de la información y comunicación, no podrán ser considerados como una aceptación tácita para la creación de bancos de datos, ni para el tratamiento de datos personales. Dichas comunicaciones deberán enmarcarse en todo momento a los principios y derechos consagrados en la presente Ley.

II. Los medios de comunicación social quedarán sujetos a las disposiciones de esta ley en lo relativo al tratamiento de datos que efectúen con una finalidad distinta a la de opinar e informar.

ARTÍCULO 49. (TRATAMIENTO CON FINES PUBLICITARIOS).- Las entidades que se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, gestión comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos hayan sido facilitados por los titulares y hayan sido otorgados a través de un consentimiento previo, informado y expreso, a tal efecto:

- a) Los titulares tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les concierne en cuyo caso serán dados de baja del tratamiento de forma inmediata, cancelándose las informaciones que sobre ellos figuren, a simple solicitud.
- b) Los mensajes publicitarios y comerciales deberán ser claramente identificados con esa naturaleza.
- c) Los titulares tendrán derecho a conocer el origen de sus datos personales cuando hayan recibido comunicaciones comerciales o mensajes publicitarios.

TÍTULO VI

RÉGIMEN DE TRANSFERENCIAS INTERNACIONALES

CAPÍTULO I RÉGIMEN DE GARANTÍAS ADECUADAS

ARTÍCULO 50. (TRANSFERENCIA INTERNACIONAL).- Toda comunicación de datos personales a otro país u organización internacional, que realice un responsable o encargado, será considerada una transferencia internacional de datos personales y para su validez deberá cumplir, con las reglas previstas en esta Ley, y demás regulación aplicable, al respecto.

ARTÍCULO 51 (TRANSFERENCIAS INTERNACIONALES MEDIANTE GARANTÍAS ADECUADAS).-

I. El responsable o el encargado podrán transferir datos internacionalmente si cumplen con alguna de las garantías que se describen a continuación y siempre que los titulares de datos cuenten con derechos exigibles y acciones legales efectivas.

II. Existen dos tipos de garantías, las que no requieren de la autorización expresa de la Autoridad de Protección de Datos Personales y las que sí la requieren.

ARTÍCULO 52. (GARANTÍAS QUE NO REQUIEREN AUTORIZACIÓN EXPRESA).- Entre las garantías adecuadas que no requieren autorización expresa de Autoridad de Protección de Datos Personales, se encuentran:

- a) Los instrumentos jurídicamente vinculantes y exigibles entre autoridades y/u organismos públicos.
- b) Las normas corporativas vinculantes de conformidad con el artículo 54 de esta Ley.
- c) Las cláusulas tipo de protección de datos aprobadas por la Autoridad de Protección de Datos Personales.
- d) Los códigos de conducta aprobados de acuerdo con el artículo 78 de esta Ley, junto con compromisos vinculantes y exigibles del responsable o el encargado en el país destinatario de aplicar garantías adecuadas, incluidas las relativas a los derechos de los titulares de datos.
- e) Los mecanismos de certificación aprobados conforme al artículo 80 de esta Ley, junto con

compromisos vinculantes y exigibles del responsable o el encargado en el país destinatario de aplicar garantías adecuadas, incluidas las relativas a los derechos de los titulares de datos.

ARTÍCULO 53. (GARANTÍAS QUE SÍ REQUIEREN AUTORIZACIÓN EXPRESA).- Entre las garantías que sí requieren de una autorización de la Autoridad de Protección de Datos Personales se encuentran las siguientes:

- a) Las cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en otro país u organización internacional.
- b) Las disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los titulares de datos.

ARTÍCULO 54. (NORMAS CORPORATIVAS VINCULANTES).- La Autoridad de Protección de Datos Personales aprobará normas corporativas vinculantes, en su carácter de mecanismo de autorregulación, siempre que:

- a) Sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial.
- b) Confieran expresamente a los titulares de datos derechos exigibles con relación al tratamiento de sus datos personales.

ARTÍCULO 55 . (CONTENIDO DE LAS NORMAS CORPORATIVAS VINCULANTES).- I. Las normas corporativas vinculantes especificarán, al menos, los siguientes elementos:

- a) La estructura y los datos de contacto del grupo empresarial y de cada uno de sus miembros.
- b) Las transferencias o conjuntos de transferencias, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de titulares de datos involucrados y el nombre del país o países destinatarios.
- c) Su carácter jurídicamente vinculante, tanto a nivel interno como externo.
- d) La aplicación de los principios de esta Ley, así como los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes.
- e) Los derechos de los titulares de datos y los medios para ejercerlos, en particular el derecho a presentar una reclamación ante la Autoridad de Protección de Datos Personales y ante los tribunales de Bolivia y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes.
- f) La aceptación por parte del responsable o del encargado, establecidos en el territorio de Bolivia, de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier otro miembro del grupo empresarial que no esté establecido en Bolivia.
- g) Los medios en los que se informará a los titulares de datos sobre cualquier contenido informativo relacionado con las normas corporativas vinculantes.
- h) Las funciones del delegado de protección de datos o de la persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes, dentro del grupo empresarial.
- i) Los procedimientos de reclamación.
- j) Los mecanismos establecidos dentro del grupo empresarial para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos deberán incluir auditorías y métodos para garantizar acciones correctivas para proteger los derechos del titular

de datos. Los resultados de dicha verificación deberán comunicarse a la Autoridad de Protección de Datos Personales cuando así lo solicite.

- k) Los mecanismos para comunicar y registrar las modificaciones a las normas y para notificar esas modificaciones a la Autoridad de Protección de Datos Personales.
- l) El mecanismo de cooperación con la Autoridad de Protección de Datos Personales para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial.

II. La Autoridad de Protección de Datos Personales establecerá el formato y los procedimientos para el intercambio de información entre los responsables y/o los encargados con dicha Autoridad conforme a lo dispuesto en el presente artículo.

CAPÍTULO II

RÉGIMEN DE EXCEPCIONES PARA SITUACIONES ESPECÍFICAS

ARTÍCULO 56. (EXCEPCIONES PARA SITUACIONES ESPECÍFICAS).- I. En los casos en los que el régimen de garantías adecuadas no resulte posible, una transferencia internacional podrá efectuarse siempre que se cumpla con alguno de los supuestos siguientes:

- a) El titular de datos haya dado expresamente su consentimiento para la transferencia internacional, después de haber sido informado de los posibles riesgos para su esfera de derechos, debido a la ausencia de garantías adecuadas.
- b) La transferencia sea necesaria para la ejecución de un contrato entre el titular de datos y el responsable o para la ejecución de medidas precontractuales adoptadas a solicitud del titular de datos.
- c) La transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del titular de datos, entre el responsable y otra persona natural o jurídica.
- d) La transferencia sea necesaria por razones de interés público.
- e) La transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones.
- f) La transferencia sea necesaria para proteger los intereses vitales del titular de datos o de otras personas, cuando el titular de datos esté física o jurídicamente incapacitado para dar su consentimiento.

II. En el caso de los supuestos previstos en los incisos a), b) y c) no serán aplicables a las actividades llevadas a cabo por las autoridades u organismos públicos.

CAPÍTULO III

RÉGIMEN DE TRANSFERENCIAS FUERA DEL RÉGIMEN DE GARANTÍAS ADECUADAS Y DEL RÉGIMEN DE EXCEPCIONES PARA SITUACIONES ESPECÍFICAS

ARTÍCULO 57. (TRANSFERENCIAS FUERA DEL RÉGIMEN DE GARANTÍAS ADECUADAS Y DEL RÉGIMEN DE EXCEPCIONES PARA SITUACIONES ESPECÍFICAS).- I. Cuando una transferencia no pueda llevarse a cabo conforme al régimen de garantías adecuadas y no resulte aplicable ninguna de las excepciones para situaciones específicas, de manera extraordinaria, podrá llevarse a cabo una transferencia internacional si se cumplen los siguientes requisitos:

- a) Que sea una transferencia internacional no repetitiva o sistemática.
- b) Que se trate de una transferencia internacional que involucre a un número limitado de titulares de datos.
- c) Que sea una transferencia internacional necesaria a los fines de intereses legítimos imperiosos

perseguidos por el responsable, en tanto que no prevalezcan los intereses o derechos y libertades del titular de datos.

- d) Que el responsable haya evaluado todas las circunstancias del caso para la transferencia internacional y, basándose en esta evaluación, haya ofrecido garantías apropiadas con respecto a la protección de datos personales. La evaluación y las garantías apropiadas deberán quedar inscritas en los registros a los que hace referencia el artículo 68, inciso b) de la presente Ley.
- e) Que el responsable informe a la Autoridad de Protección de Datos Personales de la transferencia internacional.
- f) Que el responsable informe a los titulares de datos sobre los contenidos señalados en el artículo 11 de esta Ley, así como una descripción detallada y comprensible de los intereses legítimos imperiosos perseguidos.

II. La Autoridad de Protección de Datos Personales publicará las reglas mediante las cuales establezca criterios y oriente sobre los alcances de los supuestos previstos en el presente artículo, así como sobre el procedimiento para que los responsables cumplan con las obligaciones de informar, a la Autoridad de Protección de Datos Personales y a los titulares, en los casos establecidos en los incisos e) y f) de este artículo.

TÍTULO VII

AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES, REGISTRO BOLIVIANO DE BANCOS DE DATOS

CAPÍTULO I

AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES

ARTÍCULO 58. (AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES).- Se crea la Autoridad de Protección de Datos Personales, como una institución pública descentralizada de derecho público, con personalidad jurídica, autonomía de gestión administrativa, financiera legal y técnica y patrimonio propio.

ARTÍCULO 59. (OBJETO).- La Autoridad de Protección de Datos Personales tiene por objeto constituirse en el garante de la protección de datos personales en Bolivia, para lo cual contará con facultades de regulación, supervisión, vigilancia, control, promoción, difusión, cooperación, prevención, resolución y sanción, a efectos de que se respeten los principios, derechos, deberes, responsabilidades, mecanismos y, en general, toda obligación prevista en la presente Ley, así como para generar una cultura del tratamiento responsable de los datos personales entre responsables, encargados, titulares de datos y en general en toda la sociedad boliviana.

ARTÍCULO 60. (ATRIBUCIONES).- La Autoridad de Protección de Datos Personales tiene las siguientes atribuciones:

- a) Controlar la aplicación de esta Ley y hacerla aplicar.
- b) Garantizar la efectividad y respeto de los derechos establecidos en esta Ley.
- c) Diseñar e impulsar políticas públicas dirigidas a la generación de conciencia sobre el papel de los datos personales en el contexto de la sociedad actual, así como sobre la comprensión de los riesgos, normas, garantías y derechos con motivo del tratamiento de datos. Estas políticas tendrán un especial énfasis en las actividades relacionadas con menores.
- d) Promover y propiciar la sensibilización entre responsables y encargados respecto de sus obligaciones, derivado de esta Ley, y, especialmente, sobre su responsabilidad social en el tratamiento de datos en Bolivia.

- e) Impulsar la incorporación en los programas de educación, en todos los niveles de formación, de la protección de los datos personales, como una herramienta indispensable para lograr una convivencia equilibrada entre las personas y la tecnología, con especial enfoque en los menores.
- f) Potenciar la utilización de las plataformas y herramientas digitales para el ejercicio de los derechos y para la presentación de reclamaciones, como un medio para que el derecho a la protección de los datos personales, en Bolivia, llegue al mayor número de personas posible.
- g) Poner a disposición de responsables y encargados herramientas que faciliten el cumplimiento de la Ley. De manera enunciativa no limitativa, se podrán elaborar guías, manuales, formularios y plataformas digitales que contribuyan a la comprensión de las obligaciones de esta Ley y su debida implementación.
- h) Propiciar, al máximo de sus posibilidades, que los procedimientos de reclamación, impulsados a instancia de un titular de datos, sean procedimientos cercanos a cualquier persona, de modo que las formalidades jurídicas o la falta de conocimiento jurídico, de los titulares de datos, no sea un obstáculo que les impida hacer efectivos sus derechos, sin perjuicio de la imparcialidad con la que se deban tramitar esas reclamaciones.
- i) Garantizar, en la medida de sus posibilidades, condiciones de accesibilidad para que los titulares de datos que forman parte de grupos vulnerables puedan ejercer, en igualdad de circunstancias sus derechos.
- j) Elaborar y publicar estudios e investigaciones para difundir y ampliar el conocimiento sobre la protección de los datos personales, así como divulgar y emitir recomendaciones, estándares y mejores prácticas al respecto.
- k) Crear y administrar el registro para códigos de conducta y autorregulación, según establece esta Ley.
- l) Diseñar y aplicar indicadores y criterios para evaluar el cumplimiento de la Ley, a través de los distintos actores participantes.
- m) Promover la capacitación en protección de datos personales, con especial énfasis entre los responsables y encargados, para lo cual contará con una oferta permanente, al respecto, por lo cual buscará aprovechar al máximo las ventajas del uso de plataformas digitales.
- n) Practicar las auditorías programadas conforme al plan anual que se apruebe.
- o) Promover la implementación de la privacidad desde el diseño y por defecto, la evaluación de impacto para protección de los datos personales, del delegado de protección de datos y de la autorregulación, como herramientas con un valor preventivo excepcional, independientemente de su obligatoriedad para los casos previstos en la Ley.
- p) Incentivar la existencia de centros y organizaciones especializadas en la generación de conocimiento en el ámbito de la protección de datos.
- q) Interpretar la Ley, su reglamento y demás regulación que emita en ejercicio de sus funciones.
- r) Emitir reglamentación específica, y demás regulación que se indica en la presente Ley, además de aquella que sea necesaria, así como supervisar su cumplimiento en el marco de la normativa aplicable.
- s) Conocer y resolver de las reclamaciones que reciba en términos de lo establecido en la presente Ley y demás regulación aplicable.
- t) Supervisar, controlar y evaluar las actividades efectuadas por el responsable y encargado.
- u) Sancionar a responsables y encargados conforme a lo establecido en la presente Ley.
- v) Ordenar al responsable o encargado que atiendan las solicitudes de ejercicio de los derechos de los titulares de datos.
- w) Ordenar al responsable o encargado que las operaciones de tratamiento se ajusten a las disposiciones de la presente Ley y, cuando proceda, de una determinada manera y dentro de un plazo específico.
- x) Imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición.
- y) Ordenar la suspensión de transferencias internacionales.
- z) Disponer la adopción de medidas cautelares necesarias y provisionales para la salvaguarda del derecho fundamental a la protección de datos personales, en términos de lo indicado al respecto en la Ley.
- aa) Tener del responsable y del encargado el acceso a todos los datos personales e información necesaria para el ejercicio de sus funciones, así como obtener el acceso a todos los locales, establecimientos y demás instalaciones del responsable y del encargado, incluidos cualquier

- equipo y medios de tratamiento de datos, de acuerdo a lo previsto en esta Ley y demás regulación aplicable.
- bb) Sugerir o recomendar los ajustes o adecuaciones a la legislación que resulten acordes con la evolución tecnológica, informática o comunicacional.
 - cc) Suscribir acuerdos o convenios con organismos extranjeros de regulación y supervisión del tratamiento de datos personales, para cooperación, capacitación e intercambio de información.
 - dd) Crear, dirigir y administrar el Registro Boliviano de Bancos de Datos, así como coordinar las acciones necesarias con entidades del sector público y privado para su efectivo funcionamiento.
 - ee) Llevar un registro estadístico sobre vulneraciones a la seguridad de datos personales e identificar posibles medidas de seguridad para cada una de ellas.
 - ff) Promover e incentivar los derechos señalados en esta Ley e implementar campañas pedagógicas para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos.
 - gg) Las demás que le confiera la presente Ley y demás normas aplicables.

ARTÍCULO 61. (RECURSOS PARA EL EJERCICIO DE SUS FUNCIONES).- La Autoridad de Protección de Datos, financiará sus operaciones con las siguientes fuentes:

- a) El presupuesto del Estado que se le asigne.
- b) Los montos que recaude por concepto de sanciones.
- c) Las donaciones y créditos nacionales o externos a que se haga acreedor.
- d) Las fuentes de financiamiento adicionales que permita la legislación.

ARTÍCULO 62. (DESIGNACIÓN DEL TITULAR DE LA AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES).- I. Para la designación de la persona a cargo de la dirección de la Autoridad de Protección de Datos Personales se deberá tener en consideración su trayectoria profesional, en particular, que cuente con conocimientos jurídicos especializados y experiencia probada en datos personales, así como a su capacidad para desempeñar las funciones indicadas en el artículo 60 de esta Ley.

II. La persona a cargo de la dirección de la Autoridad de Protección de Datos Personales será designada por un periodo de cuatro años, con posibilidades de renovar esa designación, únicamente, por otro periodo de cuatro años.

III. Se deberán propiciar las condiciones para que el proceso de selección y designación, de la persona a cargo de la dirección de la Autoridad de Protección de Datos Personales, sea transparente.

IV. La persona designada tendrá la representación legal de la Autoridad de Protección de Datos Personales y ejercerá sus funciones con plena independencia y objetividad y no estará sujeta a instrucción alguna en su desempeño.

ARTÍCULO 63. (CESE ANTICIPADO).- La persona a cargo de la dirección de la Autoridad de Protección de Datos Personales podrá ser cesada de su cargo, previo a la terminación de su mandato, únicamente por las siguientes causas graves:

- a) Incumplimiento grave de sus obligaciones.
- b) Incapacidad sobrevenida para el ejercicio de su función.
- c) Incompatibilidad.
- d) Condena firme por delito doloso.

ARTÍCULO 64. (REVISIÓN DE RESOLUCIONES DE LA AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES).- I. Las resoluciones que emita la Autoridad de Protección de Datos Personales ponen fin a la vía administrativa, por lo que, únicamente, serán revisables por los tribunales bolivianos, conforme a la legislación aplicable.

II. La Autoridad de Protección de Datos Personales publicará las resoluciones que dicte para transparentar su actuación y como una fuente de generación de conocimiento para la sociedad

boliviana. La citada Autoridad publicará las reglas conforme a las cuales se llevará a cabo la publicación para no vulnerar los derechos de los titulares vinculados a esas resoluciones.

ARTÍCULO 65. (PLAN ANUAL DE AUDITORÍA DE PROTECCIÓN DE DATOS).- I. La Autoridad de Protección de Datos Personales realizará auditorías periódicas de oficio, para verificar el cumplimiento de la presente Ley, de acuerdo con el plan anual que al efecto establezca.

II. La Autoridad de Protección de Datos Personales publicará las reglas y criterios conforme a los cuales desarrollará los planes de auditoría aquí referidos.

ARTÍCULO 66. (INSTANCIA DE ASISTENCIA TÉCNICA).- La Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación, es la instancia de asistencia técnica para la supervisión y verificación de los medios de control que implemente la Autoridad de Protección de Datos Personales.

ARTÍCULO 67. (INTEROPERABILIDAD ENTRE ENTIDADES PÚBLICAS).- Las entidades públicas, dentro del desempeño de sus funciones, podrán realizar la comunicación de datos personales en el marco de sus competencias, cumpliendo con lo previsto en esta Ley,

CAPÍTULO II

REGISTRO BOLIVIANO DE BANCOS DE DATOS

ARTÍCULO 68. (DEFINICIÓN Y REGLAMENTACIÓN).- I. El Registro Boliviano de Bancos de Datos es el catálogo de naturaleza administrativa y de libre consulta para los ciudadanos; bajo tuición de la Autoridad de Protección de Datos Personales. No supone el acceso a las bases de datos sino a una lista de ellas, ni que los responsables entreguen una copia de las bases de datos a la Autoridad de Protección de Datos Personales.

Este catálogo registra:

- a) Los bancos de datos personales de naturaleza pública, privada o mixta, con sus correspondientes datos de identificación, que permitan el ejercicio del derecho a la autodeterminación informativa, de acuerdo con la presente Ley.
- b) Los registros de transferencias internacionales de datos.
- c) Las Resoluciones Administrativas emitidas por la Autoridad de Protección de Datos.
- d) Otra información en procura de la tutela efectiva del derecho a la autodeterminación informativa, conforme a la Ley y su reglamentación.

II. Los requisitos para la creación, administración y cancelación de bancos de datos, serán establecidos por la Autoridad de Protección de Datos.

III. Las obligaciones previstas en este artículo no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda implicar un riesgo para los derechos y libertades de los titulares de datos, no sea ocasional, o incluya categorías de datos sensibles.

ARTÍCULO 69. (INSCRIPCIÓN DE BANCOS DE DATOS).- I. Todos los bancos de datos con fines de tratamiento de datos personales, creados por personas naturales, personas jurídicas públicas, privadas o mixtas, nacionales, internacionales o transnacionales, deben ser inscritos en el Registro Boliviano de Bancos de Datos que al efecto habilite la Autoridad de Protección de Datos Personales, salvo la excepción descrita en el artículo anterior.

II. La inscripción en el Registro Boliviano de Bancos de Datos no implica la transferencia de datos ni posibilita el conocimiento del contenido de los bancos de datos, excepto cuando exista un procedimiento de investigación en curso.

III. Ningún Responsable podrá poseer datos personales de naturaleza distinta a los declarados en el registro. El incumplimiento dará lugar a las acciones previstas por ley.

CAPÍTULO III

MECANISMOS DE SEGURIDAD

ARTÍCULO 70. (FACTORES PARA DETERMINAR LAS MEDIDAS DE SEGURIDAD).- I. El responsable y el encargado deben adoptar las medidas técnicas y organizativas necesarias para garantizar el cumplimiento del principio de seguridad establecido en esta Ley.

II. Con la finalidad de asegurar un nivel de seguridad adecuado al riesgo, los responsables y encargados tendrán en cuenta el estado actual de la técnica y los costos de aplicación, junto con la naturaleza, alcance, contexto y fines del tratamiento, así como la probabilidad de los riesgos y la gravedad para los derechos y libertades de los titulares.

III. Entre los aspectos a incluir en la aplicación de medidas técnicas y organizativas, para garantizar un nivel de seguridad adecuada al riesgo, se encuentran:

- a) La seudonimización y el cifrado de datos personales.
- b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia, permanentes, de los sistemas y servicios de tratamiento.
- c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.
- d) Los procesos de verificación, evaluación y valoración, regulares, de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

IV. La Autoridad de Protección de Datos Personales deberá recibir los recursos humanos, materiales y financieros que le permitan contar con la infraestructura idónea para desarrollar investigaciones o procedimientos, así como participar en investigaciones internacionales, elaborar guías y manuales para orientar a responsables y encargados en el cumplimiento de este principio o publicar estudios especializados, en materia de seguridad de los datos personales.

V. Los responsables y encargados podrán valerse de los esquemas de autorregulación previstos en esta Ley para demostrar el cumplimiento de este principio.

ARTÍCULO 71. (NOTIFICACIÓN DE VIOLACIÓN DE LA SEGURIDAD A LA AUTORIDAD).- I. La violación de la seguridad de los datos personales, será notificada, por parte del responsable a la Autoridad de Protección de Datos Personales, en el plazo máximo de cuarenta y ocho (48) horas contadas a partir de que haya sido constatada, salvo que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de los titulares.

II. El encargado notificará sin dilación indebida al responsable las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

III. La notificación deberá señalar al menos lo siguiente:

- a) Una descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, de las categorías y el número aproximado de interesados afectados, y de las categorías y el número aproximado de registros de datos personales afectados.

- b) La comunicación del nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- c) Una descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
- d) Las medidas adoptadas o propuestas por el responsable para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

IV. En el caso de que no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

V. El responsable deberá documentar cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la Autoridad de Protección de Datos Personales verificar el cumplimiento de lo dispuesto en el presente artículo.

VI. La Autoridad de Protección de Datos Personales emitirá las reglas adicionales que resulten necesarias para el cumplimiento de este artículo.

ARTÍCULO 72. (NOTIFICACIÓN DE VIOLACIÓN DE LA SEGURIDAD AL TITULAR).- I. Cuando la violación de la seguridad signifique riesgo alto para los derechos del titular, este último tiene derecho a ser notificado de tal evento sin dilación indebida.

II. La comunicación al titular de datos deberá contener una descripción en un lenguaje claro y sencillo de la naturaleza de la violación de la seguridad de los datos personales, así como la información y las medidas a que se refiere el artículo 71 de la Ley, en los incisos b),c) y e), al menos.

III. La notificación al titular de datos no será necesaria si se cumple alguna de las condiciones siguientes:

- a) Si el responsable adoptó medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular, aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado.
- b) Si el responsable tomó medidas posteriores que garanticen que ya no exista la probabilidad de que se materialice el alto riesgo para los derechos y libertades del titular de datos.
- c) Si la notificación conlleva un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública, o una medida semejante, por la que se informe de manera igualmente efectiva a los titulares de datos. La Autoridad de Protección de Datos Personales publicará las reglas para orientar sobre el tipo de casos que podrían ubicarse en este supuesto, así como para el tipo de comunicaciones que podrían utilizarse para cumplir.

IV. Cuando el responsable todavía no haya comunicado al titular de datos la violación de la seguridad de los datos personales, la Autoridad de Protección de Datos Personales, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en los tres incisos de este artículo.

CAPÍTULO IV

ESQUEMAS PREVENTIVOS DE CUMPLIMIENTO

SECCIÓN I PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

ARTÍCULO 73. (PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO).- I. Previo a la implementación de cualquier proyecto, plan, programa u otro, que implique el tratamiento de datos personales, todo responsable deberá aplicar, desde el diseño, las medidas adecuadas para garantizar la protección de

los datos personales, para que desde la determinación de los medios e, incluso, durante el tratamiento mismo, se hagan efectivos los principios, derechos y demás obligaciones previstas en la presente Ley.

II. El responsable garantizará que sus servicios, programas, sistemas, plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología, que implique tratamiento, cumplan o se ajusten por defecto a los principios, derechos y demás obligaciones previstas en la presente Ley.

III. Los responsables podrán valerse de los esquemas de autorregulación previstos en esta Ley para demostrar el cumplimiento de este artículo.

IV. La Autoridad de Protección de Datos Personales publicará guías, estudios y recomendaciones para la generación de conocimiento sobre la privacidad desde el diseño y por defecto, así como para orientar el criterio de los responsables y encargados para facilitar su implementación.

SECCIÓN II EVALUACIÓN DEL IMPACTO PARA PROTECCIÓN DE DATOS PERSONALES

ARTÍCULO 74. (EVALUACIÓN DEL IMPACTO PARA PROTECCIÓN DE DATOS PERSONALES).- I.

Todo responsable que vaya a realizar un tratamiento que haga probable la existencia de un alto riesgo para los derechos y libertades de los titulares de datos, debido a la naturaleza, alcance, contexto o finalidades de ese tratamiento, especialmente si utilizan tecnologías novedosas, deberá efectuar una evaluación de impacto para protección de los datos personales, antes del inicio del tratamiento.

II. La evaluación de impacto para protección de los datos personales debe elaborarse por los responsables.

ARTÍCULO 75. (TRATAMIENTOS QUE REQUIEREN UNA EVALUACIÓN DE IMPACTO).- I.

Con independencia de otros casos que los propios responsables determinen, como susceptibles de una evaluación de impacto para protección de los datos personales, será obligatorio que se realicen en los tratamientos que se describen a continuación:

- a) Evaluación sistemática y exhaustiva de aspectos personales de personas naturales que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas naturales o que les afecten significativamente de modo similar.
- b) Tratamiento a gran escala de datos sensibles.
- c) Observación sistemática a gran escala de una zona de acceso público.

II. La Autoridad de Protección de Datos Personales publicará una lista de los tipos de tratamientos que requieren una evaluación de impacto para protección de los datos personales, así como la lista de los tratamientos que no la requieren.

SECCIÓN III AUTORREGULACIÓN

ARTÍCULO 76. (AUTORREGULACIÓN).- I. El responsable o el encargado podrán adherirse, de manera voluntaria, a esquemas de autorregulación vinculante.

II. Los esquemas de autorregulación vinculante tendrán por finalidad contribuir a la correcta aplicación de la presente Ley, y demás regulación en la materia, teniendo en cuenta las características específicas de los tratamientos.

III. Entre los esquemas de autorregulación vinculante se podrán desarrollar códigos de conducta y sistemas de certificación.

ARTÍCULO 77. (OBJETO DE LOS CÓDIGOS DE CONDUCTA).- I. Los códigos de conducta servirán como herramientas coadyuvantes para lograr la correcta aplicación de la Ley, y demás regulación en la materia, y serán elaborados teniendo en cuenta las características específicas del sector al que corresponda, así como las necesidades específicas de las micro, pequeñas y medianas empresas.

II. Las asociaciones u organismos representativos de categorías de responsables o encargados podrán elaborar códigos de conducta o modificar o ampliar los ya existentes.

III. Los códigos de conducta contendrán mecanismos que permitan a los organismos de supervisión del cumplimiento, regulados en el artículo 79 de la presente Ley, efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados que se hayan comprometido a aplicarlo, sin perjuicio de las facultades de la citada Autoridad de Protección de Datos Personales.

ARTÍCULO 78. (PROCEDIMIENTO PARA LA PRESENTACIÓN, REVISIÓN Y APROBACIÓN DE UN CÓDIGO).- I. Las asociaciones u organismos que elaboren un código de conducta o modifiquen o amplíen un código existente, presentarán el proyecto de código, ante la Autoridad de Protección de Datos Personales.

II. La Autoridad de Protección de Datos Personales valorará el proyecto presentado y determinará si se adecua con la Ley, y la regulación aplicable, para su aprobación, siempre que considere que el proyecto de código, modificación o ampliación ofrece garantías adecuadas.

III. Una vez aprobado un código de conducta, modificación o ampliación de un código existente, la Autoridad de Protección de Datos Personales registrará y publicará ese código.

IV. La Autoridad de Protección de Datos Personales publicará las reglas con los plazos y requisitos para el desarrollo de este procedimiento, así como las reglas para la creación y operación del registro mediante el cual se inscribirán y darán a conocer los códigos de conducta aprobados.

ARTÍCULO 79. (ORGANISMOS DE SUPERVISIÓN AUTORIZADOS).- I. Los organismos reconocidos por la Autoridad de Protección de Datos Personales podrán supervisar el cumplimiento de un código de conducta.

II. Un organismo podrá ser acreditado para supervisar el cumplimiento de un código de conducta siempre que:

- a) Demuestre, conforme a los requisitos establecidos por la Autoridad de Protección de Datos Personales, su independencia y pericia con relación al objeto del código de conducta.
- b) Haya establecido procedimientos que le permitan evaluar la idoneidad de los responsables y encargados, correspondientes, para aplicar el código, supervisar el cumplimiento de sus disposiciones y examinar periódicamente su aplicación.
- c) Haya establecido procedimientos para tratar las reclamaciones relativas a infracciones del código o a la manera en que el código haya sido o esté siendo aplicado por un responsable o encargado, y para transparentar dichos procedimientos y estructuras para el público en general.

- d) Haya acreditado ante la Autoridad de Protección de Datos Personales que sus funciones no dan lugar a conflicto de intereses.

III.La Autoridad de Protección de Datos Personales establecerá los criterios de acreditación para que un organismo supervise el cumplimiento de un código de conducta.

IV.El o los organismos de supervisión del cumplimiento de un código de conducta deberán, con sujeción a garantías adecuadas, tomar las medidas oportunas en caso de infracción del código por un responsable o encargado del tratamiento, incluida la suspensión o exclusión de éste, debiendo informar de dichas medidas y de las razones de las mismas a la Autoridad de Protección de Datos Personales.

V. La Autoridad de Protección de Datos Personales revocará la acreditación de un organismo de supervisión del cumplimiento de un código de conducta si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo infringe la Ley y demás regulación aplicable.

VI. El presente artículo no será aplicable a los tratamientos llevados a cabo por autoridades y organismos públicos.

ARTÍCULO 80. (ALCANCES DE CERTIFICACIÓN).- I.Los sistemas de certificación servirán como herramientas coadyuvantes para lograr la correcta aplicación de la Ley, y demás regulación en la materia, teniendo en cuenta las necesidades específicas de las micro, pequeñas y medianas empresas.

II. La certificación será voluntaria y estará disponible a través de un proceso transparente.

III.La certificación no limitará la responsabilidad del responsable o encargado en cuanto al cumplimiento de la presente Ley y se entenderá sin perjuicio de las atribuciones de la Autoridad de Protección de Datos Personales.

IV.La certificación en virtud del presente artículo será expedida por los organismos de certificación o por la Autoridad de Protección de Datos Personales, conforme a los parámetros aprobados por dicha Autoridad de Protección de Datos Personales, los cuales deberá publicar de forma accesible.

V.Los responsables o encargados que sometan su tratamiento al mecanismo de certificación deberán facilitar el acceso a toda la información y a las actividades de tratamiento que resulten necesarias para el proceso de certificación, ya sea al organismo de certificación o a la Autoridad de Protección de Datos Personales, según corresponda.

VI.La certificación se expedirá por un período máximo de tres (3) años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes.

VII.La certificación será retirada cuando no se cumplan o se hayan dejado de cumplir los requisitos para la certificación.

VIII. La Autoridad de Protección de Datos Personales conservará en un registro todos los mecanismos de certificación y los pondrá a disposición pública mediante un registro de carácter público, conforme a las reglas que publique para ese fin.

TÍTULO VIII

INFRACCIONES Y SANCIONES

CAPÍTULO I

CONDICIONES PARA IMPONER SANCIONES, TIPO DE SANCIONES Y CLASIFICACIÓN DE INFRACCIONES

ARTÍCULO 81. (CONDICIONES PARA LA IMPOSICIÓN DE SANCIONES).- I. La Autoridad de Protección de Datos Personales impondrá las sanciones a las infracciones cometidas, esas sanciones deberán ser efectivas, proporcionadas y disuasorias.

II. Las sanciones se impondrán, en función de las circunstancias de cada caso en particular. Para la imposición de las sanciones se tendrá en cuenta:

- a) La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito del tratamiento de que se trate, así como el número de personas afectadas y el nivel de los daños y perjuicios generados.
- b) La intencionalidad o negligencia en la comisión de la infracción.
- c) Cualquier medida tomada por el responsable o encargado para aminorar los daños y perjuicios generados.
- d) El grado de responsabilidad del responsable o del encargado, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud a los derechos de rectificación y oposición de esta Ley;
- e) Toda infracción anterior cometida por el responsable o el encargado del tratamiento.
- f) El nivel de cooperación con la Autoridad de Protección de Datos Personales con el propósito de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción.
- g) Las categorías de los datos de carácter personal relacionados con la infracción.
- h) La forma en la que la Autoridad de Protección de Datos Personales tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida.
- i) Las medidas que hayan sido ordenadas previamente contra el responsable o el encargado de que se trate, en relación con el mismo asunto, el cumplimiento de dichas medidas;
- j) La adhesión a algún código de conducta o a algún esquema de autorregulación.
- k) El carácter continuado de la infracción.
- l) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
- m) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
- n) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
- o) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.

- p) La afectación a los derechos de los menores.
- q) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos, así como haber llevado a cabo una evaluación de impacto para protección de los datos personales para el tratamiento relacionado con la infracción, sin que existiera obligación para realizar la citada evaluación de impacto.
- r) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado.
- s) Cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

ARTÍCULO 82. (TIPO DE SANCIÓN).- I. Las infracciones a la presente Ley serán sancionadas por la Autoridad de Protección de Datos Personales de conformidad con lo siguiente:

- a) Con una advertencia en el caso de que el tratamiento sea susceptible de infringir lo dispuesto en la presente Ley.
- b) Con apercibimiento en los casos de tratamientos en los que se haya infringido lo previsto en esta Ley.
- c) Con la prohibición, temporal o definitiva de un tratamiento o tratamientos, en el supuesto de que con el tratamiento o tratamientos se haya infringido lo establecido en la Ley.
- d) Con multa en los casos de tratamientos en los que se haya infringido lo señalado en la presente Ley.

II. La Autoridad de Protección de Datos Personales podrá imponer una multa en lugar o además del apercibimiento o prohibición del tratamiento.

ARTÍCULO 83. (INFRACCIONES GRAVES).- I. Se consideran graves, y prescribirán a los dos años, el incumplimiento de:

- a) Las obligaciones del responsable y del encargado a tenor de los artículos 45 párrafo segundo, 33,34,35,36,37,39,40,41,42,43,69,70,71,72,73,74 y 75 de esta Ley.
- b) Las obligaciones de los organismos de certificación establecidas en los artículo 80 de la presente Ley.
- c) Las obligaciones a cargo de los organismos de supervisión indicadas en el artículo 79, cuarto párrafo de esta Ley.

II. En los casos descritos en el presente artículo, la Autoridad de Protección de Datos Personales sancionará de acuerdo con multas de 5.000 UFV.- (Cinco Mil Unidad de Fomento de Vivienda) a 50.000 UFV.- (Cincuenta Mil Unidad de Fomento de Vivienda).

ARTÍCULO 84. (INFRACCIONES MUY GRAVES).- I. Se consideran muy graves y prescribirán a los tres años el incumplimiento de:

- a) Las obligaciones derivadas de los principios previstos en el artículo 9 de la presente Ley.
- b) Las obligaciones, relacionadas con los derechos de los titulares, establecidas en los artículos 10,11,12,13,14,15,16,17,18,19,20,21,22,23 y 47 de esta Ley.
- c) Las obligaciones vinculadas con las transferencias de datos personales previstas en los artículos 50,51,52,53,54,55,56 y 57 de la presente Ley.
- d) El incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la Autoridad de Protección de Datos Personales o el no facilitar acceso para que la citada Autoridad de Protección de Datos

Personales ejerza sus atribuciones.

III. Las infracciones de las disposiciones descritas en este artículo se sancionarán con multas de 50.000 UFV.- (Cincuenta Mil Unidad de Fomento de Vivienda) a 100.000UFV.- (Cien Mil Unidad de Fomento de Vivienda).

IV. En ningún caso, la multa impuesta puede exceder del (10%) diez por ciento del capital del infractor, tomando en cuenta el último capital declarado en sus estados financieros.

ARTÍCULO 85. (INFRACCIONES LEVES).- Se consideran leves y prescribirán al año las infracciones de carácter meramente formal de los artículos mencionados para infracciones graves y muy graves si la Autoridad de Protección de Datos Personales estima, en atención a las circunstancias concretas del caso, que la violación no conlleva un riesgo importante para los derechos de los titulares de datos y no afecta a la esencia de la obligación en cuestión. En tales casos, la multa podría llegar a ser sustituida por un apercibimiento.

ARTÍCULO 86. (RÉGIMEN DE SANCIONES PARA AUTORIDADES DE ENTIDADES PÚBLICAS Y SUS FUNCIONARIOS).- I. En el caso de una autoridad de entidad pública que forme parte del Estado, sea quien cometa alguna de las infracciones previstas en esta Ley, la Autoridad de Protección de Datos Personales dictará resolución sancionando con apercibimiento.

II. Sin perjuicio de las sanciones administrativas previstas en la presente Ley, la Autoridad de Protección de Datos Personales hará del conocimiento de las instancias a cargo de los procedimientos disciplinarios las resoluciones dictadas respecto de autoridades de entidades públicas, con la finalidad de que dichas instancias adopten las determinaciones que correspondan en su ámbito de competencia. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

ARTÍCULO 87. (PLAZO DE PRESCRIPCIÓN PARA SANCIONES).- El plazo de prescripción de las sanciones comenzará a contarse desde el día en el que sea ejecutable la resolución por la que se impone la sanción o que haya transcurrido el plazo para recurrir.

ARTÍCULO 88. (ALCANCES DE LAS RESOLUCIONES DE LA AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES).- I. Toda resolución que dicte la Autoridad de Protección de Datos Personales, en la que se hubiese determinado la comisión de una infracción a la Ley, se establecerán las medidas que deberán adoptar para el cese de la conducta y/o para restituir en sus derechos, a él o los titulares afectados, por los efectos de la infracción cometida.

II. La resolución se notificará al responsable o encargado y a los afectados que tuvieran la condición de titulares de datos, en su caso.

DISPOSICIONES ADICIONALES

DISPOSICIÓN ADICIONAL ÚNICA.- Los procedimientos específicos existentes que tengan por objeto constituir derechos, determinar sus alcances o resolver situaciones jurídicas determinadas, relacionada con el tratamiento de datos personales, seguirán subsistiendo y deberán tramitarse previamente al ejercicio de los derechos de rectificación, cancelación u oposición se debe tramitar estos procedimientos y una vez resueltos por la autoridad o juez competente podrán ejercerse los derechos de esta Ley.

DISPOSICIÓN ABROGATORIA Y DEROGATORIA

DISPOSICIÓN ABROGATORIA Y DEROGATORIA.- Se abrogan y derogan todas las disposiciones contrarias a la presente Ley.

DISPOSICIONES FINALES.

DISPOSICIÓN FINAL PRIMERA.- En un plazo no mayor a ciento veinte (120) días calendario, computables a partir de su publicación, el Órgano Ejecutivo reglamentará la presente Ley mediante Decreto Supremo.

DISPOSICIÓN FINAL SEGUNDA.- La presente Ley entrará en vigencia dos años después de su publicación.

DISPOSICIÓN FINAL TERCERA.- La Autoridad de Protección de Datos Personales deberá crearse dentro del plazo de tres (3) meses, contados a partir de la publicación de la Ley y la persona que se designe para dirigirla deberá ser nombrada a más tardar dentro de los tres meses siguientes al de su creación.

DISPOSICIÓN FINAL CUARTA.- Las reglas de funcionamiento del servicio profesional de carrera, de la Autoridad de Protección de Datos Personales, deberán publicarse por la propia autoridad, en un plazo máximo de tres meses a partir de la designación de la persona a cargo de su dirección.

DISPOSICIÓN FINAL QUINTA.- La Ley es aplicable a todo tratamiento de datos con independencia de que se trate de datos personales que se hayan estado tratando, o se hayan obtenido, con anterioridad a su entrada en vigor.

AGETIC