DEPARTAMENTO ESTUDIOS, REFERENCIAS Y SERVICIOS TÉCNICOS

AL-DEST-ITS-002-2022

INFORME DE: PROYECTO DE LEY

"LEY DE PROTECCIÓN DE DATOS PERSONALES"

EXPEDIENTE Nº 23.097

INFORME JURIDICO DEL TEXTO SUSTITUTIVO

ELABORADO POR:

GEORGINA GARCIA ROJAS
ASESORA PARLAMENTARIA

REVISIÓN FINAL Y AUTORIZACIÓN

SELENA REPETTO AYMERICH
DDIRECTORA A.I

16 DE NOVIEMBRE 2022

ASAMBLEA LEGISLATIVA
de la República de Costa Rica

TABLA DE CONTENIDO

I.- RESUMEN DEL PROYECTO 4

II.- CONSIDERACIONES DE FONDO 5

2.1.- Análisis del principio de conexidad en la propuesta legal 5
2.2.- Estándares internacionales base del proyecto. 16
2.2.2.- El Convenio 108 17
2.2.3.- Estándares de Protección de Datos Personales para los Estados Iberoamericanos 18
2.2.4.- Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales (1980) 19

III.- SOBRE EL ARTICULADO DEL TEXTO SUSTITUTIVO 20

3.1. Capítulo I Disposiciones generales 20
3.2. Capítulo II Principios de protección de datos personales 28
3.3. Capítulo III Derechos del titular 32
3.4. Capítulo IV Responsable y encargado del tratamiento 34
3.5. Capítulo V Transferencias internacionales de datos personales 37
3.6. Capítulo VI Medidas proactivas en el tratamiento de datos personales 38
3.7. Capítulo VII Disposiciones aplicables a tratamientos concretos 39
3.8. Capítulo VIII Agencia de Protección de Datos 42
3.9. Capítulo X Régimen sancionador 44
3.9. Capítulo XI Derecho de indemnización 46
3.7. Disposiciones de transitorias 46
3.8. Conclusiones 46

IV.- ASPECTOS DE TÉCNICA LEGISLATIVA 47

4.1. Redacción del proyecto de ley 47
4.2. Estructura de la ley 48
4.3. Título del proyecto de ley 49

V.- ASPECTOS DE PROCEDIMIENTO 50

5.1. Votación 50
5.2. Delegación 50
5.3. Consultas 50

VI.- FUENTES 51

6.1. Constitucionales 51

6.2. Leyes y Reglamentos..... 51
6.3. Pronunciamientos administrativos..... 52
6.4. Otras..... 52

VII.- ANEXOS 7.1. CUADRO COMPARATIVO DE TEXTOS..... 52

CUADRO COMPARATIVO ENTRE EL TEXTO BASE DEL PROYECTO DE LEY 23097 Y EL TEXTO SUSTITUTIVO..... 53

ASAMBLEA LEGISLATIVA
de la República de Costa Rica

AL-DEST-ITS-002-2022

INFORME JURÍDICO AL TEXTO SUSTITUTIVO[1]

"LEY DE PROTECCIÓN DE DATOS PERSONALES"

EXPEDIENTE Nº 23.097

I.- RESUMEN DEL PROYECTO

El proyecto de ley pretende reformar integralmente el marco regulatorio en la materia, derogando la *"Ley de protección de la persona frente al tratamiento de sus datos personales"*[2], debido a que se encuentra desactualizada en relación con los estándares internacionales y los retos de la creciente digitalización de la sociedad; además de la poca incidencia que ha tenido el tratamiento de los datos en el sector público.[3]

Los principales aspectos que se destacan en el proyecto se refieren a:

- Actualizar conceptos y añadir aquellos no presentes en la legislación actual.
- Fortalecer el derecho a la protección de datos expandiendo su protección más allá del derecho a la intimidad.
- Definir reglas claras para la limitación al derecho de protección de datos personales y la transferencia de datos entre instituciones públicas.
- Desarrollar y ampliar nuevas bases de legitimación, adicional del consentimiento informado.
- Ampliar la gama de principios y derechos del tratamiento de datos personales.
- Establecer las excepciones a la prohibición del tratamiento de datos sensibles y las obligaciones del responsable y encargado.
- Regular las transferencias de datos internacionales conforme los estándares del RGPD el Convenio 108+ y las Directrices de la OCDE en la materia.
- Sustituir la actual Agencia de Protección de Datos de los Habitantes (PRODHAB) por una Agencia de Protección de Datos Personales, con grado

[1] Elaborado por Georgina García Rojas, Asesora Parlamentaria, Departamento de Servicios Técnicos.
[2] Ley N°8968 del 5 de setiembre de 2011.
[3] En la exposición de motivos, se detalla de la siguiente forma: *"porque luego de una década de existencia, la legislación actual ha tenido una modesta incidencia en la forma en cómo se tratan los datos personales en Costa Rica en el sector privado, pero en el sector público, la incidencia ha sido prácticamente nula. Si bien no cabría indicar que la legislación ha sido letra muerta, sí se puede asegurar que no ha propiciado un desarrollo suficiente del derecho a la privacidad del habitante. Además, se trata de una legislación desactualizada frente a los retos de la creciente digitalización de la sociedad, y los acontecimientos recientes que se mencionarán más adelante, así lo acreditan."*

de desconcentración máxima y adscrita al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Micitt).

- Fortalecer las medidas proactivas en el tratamiento de datos para elevar los controles de protección implementados por el Responsable, así como definir las condiciones para la licitud de tratamientos concretos.
- Ampliar el régimen sancionatorio e incluir el volumen de ventas para determinar la cuantía, con la finalidad de contar con un mayor efecto disuasorio.
- Regular el procedimiento en caso de posible vulneración de la normativa de protección de datos y el derecho del titular a la reparación del daño sufrido, producto de una violación de su derecho a la protección de datos personales.
- Establecer reglas para tratamientos de datos personales en actividades concretas como: videovigilancia, geolocalización en el trabajo, comportamiento crediticio del sector financiero y no financiero, salud, actividades electorales, actos administrativos, rectificación en Internet, entre otros.

El cuerpo del proyecto de ley está compuesto por un total de 83 artículos y seis disposiciones transitorias, el cual pretende derogar la *"Ley de protección de la persona frente al tratamiento de sus datos personales"*[4] y la vez, actualizar el marco regulatorio a los más altos estándares en la materia.

II.- CONSIDERACIONES DE FONDO

En atención a la aprobación de un texto sustitutivo por la Comisión Permanente Especial de Ciencia, Tecnología y Educación, en la sesión ordinaria N°16 del 10 de noviembre de 2022, producto de la aprobación, se hace imperioso realizar un análisis de conexidad de la presente propuesta de ley a efecto de verificar el cumplimiento del principio de conexidad.

2.1.- Análisis del principio de conexidad en la propuesta legal

El principio de conexidad en el ámbito legislativo se ha conceptualizado así: *"las modificaciones que se introducen a un proyecto de reforma constitucional, ley o acuerdo, deben ser conformes con la finalidad o propósito original de la iniciativa y guardar relación con ella."*[5]

Este principio de conexidad, la Sala Constitucional lo ha desarrollado en relación con los principios democrático, derecho de iniciativa y el derecho de enmienda; donde determina el lineamiento esencial de este, al indicar que:

[4] La cual está compuesta por 34 artículos y tres disposiciones transitorias.
[5] **Departamento de Servicios Técnicos**. Oficio N°AL-DEST-CJU-087-2015 de 17 de agosto de 2015. CONSULTA sobre "Conexidad de moción 137 que introdujo modificaciones al inciso a) del artículo 18 de la Ley N°9028, Ley general para el control de Tabaco y sus efectos nocivos, en relación con el contenido del texto del expediente N°19.407, Ley para mejorar la lucha contra el contrabando".

"Emanan del principio democrático tanto el derecho de iniciativa, regulado en la Constitución, como el derecho de enmienda, del cual se ocupa el Reglamento Legislativo al tratar las llamadas mociones de fondo y de forma. Ambos se originan en ese principio y en su virtud constructiva. El primero implica participación, porque es el medio legítimo de impulsar el procedimiento legislativo para la producción de una ley que recoja los puntos de vista de quien la propone. El derecho de enmienda también es un medio de participar en el proceso de formación de la ley, que hace posible influir en el contenido definitivo de ésta. Ambos derechos están necesariamente relacionados y han de ser observados durante el proceso formativo de la ley, pero ninguno de ellos puede tiranizar al otro (por regla general). Así, por ejemplo, no puede aprovecharse la enmienda para excluir de raíz la materia a la que el proyecto se refiere bajo la particular concepción de su proponente legítimo (ya fuera que se intente o no usurpar las ventajas de un proceso ya avanzado). Pero tampoco puede pretenderse que la iniciativa impone a la Asamblea el limitado deber de aprobar el proyecto o rechazarlo, sin posibilidad de ahormar con arreglo a los diversos puntos de vista de los diputados (...). Es aproximadamente en este sentido que se suele decir que el texto formulado con la iniciativa fija el marco para el ejercicio del derecho de enmienda.
(…)
Como ha señalado este Tribunal en varias decisiones previas, la garantía que proporciona el principio de conexidad para la protección tanto del derecho de iniciativa, como del derecho de enmienda, en el marco del procedimiento legislativo, atiende esencialmente, a la materia sobre la que versa el proyecto formulado originalmente. Es decir, lo que se pretende con la protección que otorga ese principio no es impedir u obstruir el ejercicio de lo que la Sala ha denominado 'función política transaccional' que se refiere a la posibilidad que tienen las y los diputados de ir ajustando con sus opiniones, dentro del marco que fija la iniciativa, el proyecto originalmente propuesto".[6]

El principio de conexidad atiende esencialmente a la materia sobre la que versa el proyecto formulado originalmente, al existir una unidad de materia con el texto original. El texto base de la iniciativa de ley, puede sufrir modificaciones –texto transado- siempre que mantenga su unidad lógica y su propia identidad, sin que se altere su materia esencial. Se requiere que el texto sustitutivo mantenga una conexión necesaria y razonable con el texto original.[7] Es decir, el *"balance que debe imperar entre los derechos de iniciativa y enmienda de los legisladores y los límites que a ellos imponen los principios constitucionales de conexidad y democrático",* donde se determina la posibilidad de modificar el texto, siempre y cuando conserve su objeto y sentido original.[8]

---

[6] **Sala Constitucional.** Voto N°3441-2004.

[7] En este sentido, la Sala Constitucional señaló: *"… la conexidad se dirige, entonces, a lograr que se respete el derecho de iniciativa de conformidad con el cual se establece el hilo conductor básico (la raíz) que ha servido de ratio o motivo para el proyecto original y que, por eso mismo, no puede ser dejado de lado, sea a través de cambios en la finalidad del proyecto, o bien, por la inclusión de meras disposiciones aisladas que regulan temas cualitativamente diferentes".* (Voto N°3441-2004).

[8] *"**V.- Sobre los alcances del principio de conexidad.** En la sentencia No. 2010-16335 de las 15:50 hrs. de 29 de septiembre de 2010 reiteró la Sala anteriores decisiones suyas sobre el balance que debe imperar entre los derechos de iniciativa y enmienda de los legisladores y los límites que a ellos imponen los principios constitucionales de conexidad y democrático, en los términos que siguen:*

De lo anterior, podemos concluir que el principio de conexidad está estrechamente ligado al respeto del hilo conductor del texto base original del proyecto de ley, el cual no puede ser dejado de lado.

En relación con la función política transaccional, que opera a lo interno de los órganos legislativos, específicamente en la discusión del proyecto de ley –texto base-; las enmiendas introducidas en la iniciativa puede ser operada mediante una moción de Texto Sustitutivo[9], -como sucedió en la iniciativa en estudio- donde las modificaciones al texto del proyecto de ley obedecen a los aportes de instituciones públicas, de organismos especializados del sector privado, cámaras empresariales como la Cámara de Tecnologías de Información y Comunicación, y órganos internacionales, como la Asociación Latinoamericana de Internet, Access Now y Derechos Digitales, enmiendas que fueron congruentes con ajustar la normativa a los más altos estándares en la materia, específicamente, los del Reglamento General de Protección de Datos Personales de la Unión Europea[10], Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales N°3/2018

"…el derecho de enmienda deriva del principio democrático y está regulado expresamente por el Reglamento de la Asamblea Legislativa. A través de él, los diputados participan en el proceso de formación de la ley, de manera que pueden influir en el contenido definitivo de ésta a través de la presentación de mociones tendentes a modificar el contenido del proyecto original. De conformidad con la jurisprudencia de este Tribunal, este derecho debe ser observado durante todo el proceso de formación de la ley y constituye "parámetro de constitucionalidad", de manera que una violación a su núcleo básico provoca la inconstitucionalidad de la norma que se aprueba. Este derecho se relaciona íntimamente con el derecho de iniciativa, también de observancia obligatoria durante el procedimiento de aprobación de una ley. Este último supone participación, porque es el medio legítimo de impulsar el procedimiento legislativo para la producción de una ley que recoja los puntos de vista de quien la propone. El objeto del derecho de iniciativa es fundamental, porque sirve de marco referencial durante la tramitación del procedimiento y se convierte en un límite intrínseco para la presentación de enmiendas. En este sentido, la Sala ha insistido en que existe un marco dentro del cual la Asamblea Legislativa puede realizar lo que se denomina "función política transaccional", para la cual tiene, naturalmente, mayor disposición y para la cual la Constitución la estructura (a partir del artículo 105). Por ello, tanto el derecho de iniciativa como el de enmienda deben ser observados durante el proceso de formación de la ley, pero ninguno puede prevalecer sobre el otro. Así, ni el derecho de enmienda puede utilizarse para convertir el proyecto inicial en uno sustancialmente diferente al presentado originalmente –siendo éste uno de sus límites-, ni el de iniciativa puede prevalecer de manera que la Asamblea -y los diputados en particular- vea limitadas sus potestades de discusión y de ajustar el proyecto según se estime pertinente. Es por ello que se ha dicho que el texto propuesto por medio del derecho de iniciativa original es el que fija el marco general del proyecto y se dentro de éste que deben ponderarse las modificaciones que se pretendan introducir por medio del ejercicio del derecho de enmienda." (ver también las resoluciones #2008-10450 de las 9:00 horas del 23 de junio; #2008-5179 de las 11:00 horas del 4 de abril; #2008-2521 de las 8:31 horas del 22 de febrero, las tres de 2008; #2007-17104 de las 9:36 horas del 23 de noviembre de 2007; y la #3513-94 de las 8:57 horas del 15 de julio de 1994, anteriormente citada).
En suma, puede modificarse o complementarse un proyecto de ley, en tanto éste conserve su objeto y sentido original. De lo contrario, deberá ocurrirse a una nueva iniciativa y a un nuevo proyecto de ley, que contemple los cambios desligados del primer proyecto, cumpliéndose todos los pasos indispensables del procedimiento parlamentario correspondiente." **Sala Constitucional. Voto Nº 5274-2011 de las 15:19 horas del 27 de abril de 2011.**

[9] Las cuales deben perseguir la búsqueda del hilo conductor básico de la orientación en la misma dirección del proponente, aunque no siempre bajo la misma perspectiva. Como ejemplo, se citan los expedientes legislativos N°17.502 *"Sistema de Banca para el Desarrollo"* -**Sala Constitucional** avaló el texto sustitutivo-, y el N°18.255 "Ley de Profesionalización del Servicio Exterior" –criterio del **Departamento de Servicios Técnicos**. Oficio N°AL-DEST-CJU-100-2015 de 25 de setiembre de 2015 en consulta sobre análisis de conexidad del "borrador" de Texto Sustitutivo de la "Ley de Profesionalización del Servicio Exterior", donde avala texto sustitutivo.

[10] Reglamento General de Protección de Datos Personales (RGPDP) número 2016/679, el cual entró en vigor en la Unión Europea el 25 de mayo de 2018.

de España[11] y los Estándares de Protección de Datos Personales de la Red Iberoamericana de Protección de Datos Personales[12].

Para el proyecto de ley en estudio, y para efectos de determinar la conexidad del texto sustitutivo aprobado[13], es necesario analizar si el texto respeta el principio de conexidad con el texto original de la iniciativa -texto base-. Para ello, en el apartado de "Anexos" del presente informe jurídico, se puede consultar la tabla comparativa entre el texto base presentado y el texto sustitutivo, donde se destacan las enmiendas realizadas al texto sustitutivo.

De la comparación de la estructura de los textos -inicial y sustitutivo-, podemos determinar que ambos mantienen la misma, compuesta por 83 artículos. La diferencia radica, en la adición de una disposición transitoria en el **texto sustitutivo**[14]. La estructura es la siguiente:

- Capítulo I Disposiciones generales
- Capítulo II Principios de protección de datos personales
- Capítulo III Derechos del titular
- Capítulo IV Responsable y encargado del tratamiento
- Capítulo V Transferencias internacionales de datos personales
- Capítulo VI Medidas proactivas en el tratamiento de datos personales
- Capítulo VII Disposiciones aplicables a tratamientos concretos
- Capítulo VIII Agencia de Protección de Datos
- Capítulo IX Procedimiento en caso de posible vulneración a la normativa de protección de datos
- Capítulo X Régimen sancionador
- Capítulo XI Derecho de indemnización
- Transitorios

Comparado el contenido de ambos**,** se evidencia que, en el **texto sustitutivo**, se realizaron modificaciones tanto de orden formal, como de fondo. Las modificaciones de orden formal refieren a:

- Reformas de varios artículos
- Adición de una nueva disposición transitoria -II-

[11] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales de España, la cual entró en vigor el 7 de diciembre de 2018.
[12] Estándares de Protección de Datos Personales para los Estados Iberoamericanos, del 20 de junio de 2017. Los cuales pueden ser consultado en la siguiente dirección web: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf
[13] El cual fue aprobado por la Comisión Permanente Especial de Ciencia, Tecnología y Educación, visible en el acta de la sesión ordinaria N° del 10 de noviembre de 2022.
[14] La Comisión Permanente Especial de Ciencia, Tecnología y Educación, en la sesión ordinaria N°16 del 10 de noviembre de 2022 emitió dictamen afirmativo unánime.

Las otras modificaciones refieren a temas de fondo, donde en algunos casos se amplía o modifica lo planteado en el texto inicial. Dentro de las reformas de fondo, se destacan:

- Se precisa que los principios y derechos en el texto aplican a los habitantes, independientemente de su nacionalidad, y se modifica *"de la región"* por *"del país"* -artículo 1-
- Se adiciona la definición de *"violación de seguridad de los datos personales"*, se elimina la de *"transferencia de datos"*, y se modifican las definiciones de *"anonimización"*, *"base de datos"*, *"cesión de datos"*, *"consentimiento"*, *"datos biométricos"*, *"datos personales sensibles"*, *"datos relativos a la salud"*, *"encargado"*, *"fuentes de acceso público"*, *"grupo económico"*, *"normas corporativas vinculantes"*, *"tercero"* y *"tratamiento"* -artículo 2-
- Se modifica la frase *"Administración Pública centralizada y descentralizada"* por *"Administración Pública en sentido amplio"* -artículo 3-
- Se eliminan los supuestos de no aplicabilidad de la ley de los incisos c y d -artículo 4-
- Se aclara que, en caso de fallecimiento del titular, los únicos legitimados para ejercer los derechos son los herederos, previa acreditación -artículo 5-
- Se cambia *"grupo empresarial"* por *"grupo económico"* -artículo 6-
- Se reforman las *"excepciones generales al derecho a la protección de datos personales"* -artículo 7-
- Se ajusta la redacción, se establece un plazo de verificación no mayor a 10 días hábiles en el punto a), se adiciona un inciso 6, y se cambia la palabra *"transferencia"* por *"cesión"* -artículo 8-
- Se agregan puntos i y j en el inciso 1, que incluyen *"el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del Responsable o del Titular en el ámbito del derecho laboral"* y *"El tratamiento sea efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos"*, como excepciones. Además, se modifica la redacción de los puntos a y d, y se agregan "*investigación en salud"* y *"pandemias debidamente declaradas por las autoridades de salud competentes",* como excepciones a la prohibición -artículo 10-
- Se adiciona que los registros de condenas podrán estar también bajo el control del Ministerio de Justicia y un inciso 2, que indica que los funcionarios judiciales y abogados podrán realizar tratamiento de datos cuando tengan por objeto tratar la información de sus clientes para el ejercicio de sus funciones, bajo la obligación de secreto profesional -artículo 11-
- Se elimina *"bajo ninguna circunstancia un dato personal sensible podrá ser incorporado en una base de datos de acceso público"* -artículo 12-

- Se sustituye *"el responsable observará"* por *"deberá realizarse conforme a los principios"* y se cambia la redacción del listado de principios -artículo 13-
- Se sustituye "*recogió"* por *"recolectó"* y se agrega un inciso 2 que indica que *"En todos los casos anteriores el Titular tendrá derecho de solicitar rectificación de sus datos personales"* -artículo 14-
- El principio de lealtad se modifica para que indique que *"el tratamiento de los datos personales será legítimo solo cuando se realice con fundamento en alguna de las siguientes bases de legitimación:",* y se adiciona un inciso 2 para indicar que los puntos b, c, f y h del inciso 1 estarán sujetos al cumplimiento de estándares internacionales, principios y criterios de legalidad, proporcionalidad y necesidad -artículo 15-
- Se cambia la palabra *"asistencia"* por "*participación"* -artículo 17-
- Se adiciona que además serán desleales los tratamientos que *"excedan las expectativas razonables del Titular respecto a sus finalidades"* -artículo 18-
- Se sustituye *"las transferencias, nacionales o internacionales"* por *"la existencia de cesiones y/o transferencias internacionales"* y se incluye "las categorías de servicios" -artículo 19-
- Se adiciona que el responsable no podrá tratar los datos personales en su posesión para finalidades análogas o compatibles a aquéllas que motivaron el tratamiento original -artículo 20-
- Se modifica el *"principio de exactitud"* -artículo 22-
- Se modifica el nombre a "principio de responsabilidad proactiva" y se agregan 2 incisos que establecen como mecanismos para que el responsable cumpla con el principio, designar un delegado de protección de datos y llevar el registro de tratamiento de datos, cuando sean requeridos por ley. Además, en el punto b del inciso 3 cambia *"sistemas de administración de riesgos"* por *"mecanismos para el análisis de riesgos"* y agrega *"y en caso de que corresponda, evaluaciones de impacto de datos personales"* -artículo 23-
- Se adiciona al encargado como obligado de establecer las medidas. Se cambia "*garantizar"* por *"mantener"* y *"vulneración"* por *"violación de la seguridad de los datos personales"* -artículo 24-
- Se sustituye *"vulneración"* por *"violación"*
- Se modifica el inciso 4 en el sentido de que el responsable *"deberá presentar actualizaciones periódicas a la Agencia de Protección de Datos Personales sobre el informe inicial, cada vez que se disponga de información nueva o diferente sobre el incidente, hasta la fecha en que la investigación del incidente haya concluido y que el incidente asociado se haya mitigado y resuelto por completo."* -artículo 25-
- Se agrega un inciso 3 que indica *"Los derechos del Titular son irrenunciables. Será nula de pleno derecho toda estipulación en contrario."* -artículo 27-
- Se incluye en el inciso 1, que los derechos *"se ejercerán por medio escrito, y serán comunicados al Responsable en los medios que hubiese puesto a disposición del Titular, por medio del oficial de protección de datos (de haberlo), o, en su defecto, en su domicilio social o establecimiento comercial*

abierto al público". También, se adiciona que *"salvo que otro plazo se estableciera en la Ley, la respuesta a una solicitud de ejercicio de derechos por parte de un afectado deberá comunicarse en un plazo de cinco días hábiles posteriores a su recepción, al medio señalado por el afectado."* -artículo 28-

- Se modifican varios puntos del *"derecho de acceso"* -artículo 29-
- Se modifican varios puntos del "derecho de cancelación o supresión" -artículo 31-

  Se agregan en el inciso b los supuestos de *"publicidad"* y *"prospección comercial"*. Tratándose del inciso 2, se aclara que "*el Responsable del tratamiento deberá responder la solicitud en el plazo máximo de cinco días hábiles"* -artículo 32-
- Se modifican varios puntos del *"derecho a no ser objeto de decisiones automatizadas"* -artículo 33-
- Se elimina que por vía reglamentaria se establezcan los requerimientos, plazos, términos y condiciones en los que los titulares podrán ejercer sus derechos y se sustituye con que será improcedente el ejercicio de los derechos ARCO y portabilidad, en los casos ahí establecidos. Asimismo, se adiciona que cuando el tratamiento sea necesario para el ejercicio de las funciones propias de las autoridades públicas, deberán estar expresamente establecidas en la ley. Se sustituye la palabra *"canon"* por *"cargo"* -artículo 36-
- Se modifican las *"obligaciones del responsable del tratamiento"* -artículo 37-
- Se modifica la *"cesión de datos"* -artículo 39-
- Se cambia en el inciso 6 la frase *"una norma reguladora de dichas competencias*" por *"acto administrativo"* -artículo 40-
- Se modifican varios puntos de la *"formalización de la prestación de servicios del encargado",* referentes a las cláusulas que debe incluir el contrato de prestación de servicios. Adicionalmente, se aclara que la formalización de la suscripción del contrato de encargo será responsabilidad del responsable -artículo 41-
- Se complementa la frase *"actividades de tratamiento"* con *"de datos personales"* y se sustituye la palabra *"transfirieron"* y *"transferirán"*, por *"cedieron"* y *"cederán"*. Adicionalmente, se elimina que en el caso de las transferencias realizadas con base en el artículo 44, apartado 1, inciso d), se tuvieran que incluir en el registro, la documentación de garantías adecuadas -artículo 43-
- Se ajusta la estructura de las *"reglas generales para las transferencias internacionales de datos personales"* -artículo 45-
- Se adiciona que el responsable aplicará, desde el diseño, las medidas preventivas, *"teniendo en cuenta el estado de la técnica, el costo de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entrañe el tratamiento de los datos para los derechos y libertades de los Titulares"* -artículo 47-

- Se incluye a la Asamblea Legislativa como una de las entidades en las que el Responsable deberá designar un oficial de protección de datos y que, en el caso de entidades bancarias y financieras, sujetas a la regulación del SUGEF, se designará de acuerdo a las regulaciones sectoriales que se dicten. Además, se elimina que el responsable deba informar a la Agencia de Protección de Datos en un plazo de diez días naturales y se incluye que *"los Responsables que designen un oficial de protección de datos, sea por mandato legal o de forma voluntaria, deberán poner a disposición del Titular sus datos de contacto en cualquier aviso o política de privacidad de la que disponga".* Entre otros ajustes, se incluye que *"el oficial de protección de datos personales estará obligado por el secreto profesional y el deber de confidencialidad en lo que respecta al desempeño de sus funciones"* -artículo 48-
- Se modifican los dos plazos, uno de dos meses y otro de un mes, por cinco días hábiles -artículo 49-
- Se incluye a al encargado, junto con el responsable, como sujeto que podrá adherirse, de manera voluntaria, a esquemas de autorregulación vinculante, que tengan por objeto, contribuir a la correcta aplicación de la Ley y establecer procedimientos de resolución de conflictos. Asimismo, se aclara que los mecanismos de autorregulación mencionados en el inciso 3, serán *"los elaborados por las asociaciones y otras organizaciones, nacionales o internacionales, de alcance general o sectoriales"* -artículo 50-
- Se agrega como supuesto para la evaluación de impacto, los datos relativos a condenas e infracciones penales, en el inciso 4 se modifica la palabra *"podrá"* por *"deberá"*, y se elimina el inciso 6, que indicaba que *"cuando proceda, el responsable podrá recabar la opinión de los titulares o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento"*. Por último, se sustituye la frase *"autoridad de control"* por *"Agencia de Protección de Datos"* -artículo 51-
- Se modifica el inciso 8, indicando que *"se prohíbe el uso de sistemas de identificación biométrica en tiempo real en espacios públicos a través de cámaras o sistemas de videovigilancia que tengan por finalidad la identificación indiscriminada o masiva de las personas"* -artículo 52-
- Se aclara que además de los trabajadores del sector público, incluye a los trabajadores del sector privado, y se agregan las salas de lactancia dentro de los supuestos en los que no se admite la instalación de sistemas de grabación de sonidos ni de videovigilancia -artículo 53-
- Se aclara que incluye a los trabajadores del sector privado, no sólo los del sector público -artículo 54-
- Se modifica la totalidad del texto de *"datos relativos al comportamiento crediticio del sector financiero y no financiero"* -artículo 55-
- Se eliminan los puntos b y e del inciso 1, se agrega en el punto iv) que la designación de un representante legal en el país si el promotor de un ensayo clínico no está establecido en el territorio nacional, será *"para que responda*

por el cumplimiento de las obligaciones derivadas de esta Ley", y se sustituye la referencia a *"legislación"* en el inciso e, por *"Ley 9234 Ley Reguladora de Investigación Biomédica"* -artículo 56-

- Se ajustan varios puntos de las "*disposiciones generales".* Los principales son, que se indica que la Agencia de Protección de Datos *"es la autoridad nacional de control encargada de la regulación y protección de los datos personales de los habitantes de la República"* y se modifica la frase *"será un órgano adscrito al MICITT"* por *"será un órgano desconcentrado del MICITT".* Adicionalmente, se aclara que no podrán *"impugnarse las resoluciones ante el MICITT ni ser avocadas sus competencias por este"* -artículo 61-
- Se aclara que *"la denominación salario base utilizada en esta Ley debe entenderse como la contenida en el artículo 2 de la Ley No. 7337 de 5 de mayo de 1993",* y que no se aceptarán donaciones de empresas que se dediquen a comercialización de datos, *"sean nacionales o internacionales"*. Además, se agrega en el punto b del inciso 1 la frase *"en los términos que establezca el reglamento a esta ley"* -artículo 62-
- Se agregan 2 funciones a la Agencia de Protección de Datos, se modifica el inciso f y se sustituye en el inciso c *"Asesorar"* por *"Emitir criterio"* -artículo 63-
- Se adiciona un inciso, indicando que, para llevar a cabo funciones de investigación, la Agencia podrá *"dictar y ejecutar medidas cautelares en sede administrativa para garantizar la protección de los datos personales de los habitantes".* También, se hace referencia a que la Agencia podrá actuar sin comprobación previa de indicios, cuando se trate de auditorías preventivas -artículo 64-
- Se incluyen los impedimentos para ser nombrado Director y/o Adjunto, así como que cuando cesen de su cargo por incapacidad esta debe ser por 6 meses y cuando sea por condena firme de delito doloso, podrá ser incluso en grado de tentativa -artículo 65-
- Se cambia la palabra *"comunicación"* por *"cesión"* en el inciso 2 -artículo 70-
- Se aclara que los encargados estarán sujetos al régimen sancionador, *"en el cuanto su responsabilidad no se derive de instrucciones giradas por el Responsable, o del incumplimiento de este a las disposiciones de esta Ley o su reglamento"* -artículo 72-
- Se minimizaron los montos de las sanciones -artículo 73-
- Se elimina el punto n del inciso 1, que establecía como infracción muy grave *"no facilitar el acceso del personal de la autoridad de protección de datos competente a los datos personales, información, locales, equipos y medios de tratamiento que sean requeridos por la autoridad de protección de datos para el ejercicio de sus poderes de investigación"*. También, en el punto p se cambia la palabra "*transferencia"* por *"cesión"* -artículo 74-
- Se aclara que constituye una infracción muy grave, además de los otros derechos, no solo el impedimento o la obstaculización o la no atención reiterada de los derechos de supresión, sino también de cancelación -artículo 75-

- Se ajusta el error en la palabra *"tranferido"* en el inciso c y se sustituye por *"cedido o transferido"* -artículo 76-
- Se modifica el plazo de 12 meses por 6 meses -artículo 77-
- Se ajusta el error en la palabra *"desentralizada"* y se corrige por *"descentralizada"*. Se elimina el inciso 3 que indicaba que la Agencia podía proponer también la iniciación de actuaciones disciplinarias contra los funcionarios implicados cuando existan indicios suficientes para ello y se sustituye por *"los funcionarios públicos que incurran en algunas de las infracciones establecidas en los artículos 74, 75 y 76 y se haya demostrado la culpa o dolo en su accionar u omisión, serán sancionados con la suspensión de su cargo por hasta noventa días, sin goce de salario, sin perjuicio de otras sanciones previstas en el régimen disciplinario aplicable al funcionario. 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 79-
- Se cambia el plazo de prescripción de 1 año a 3 años para el ejercicio de acciones tendientes a la reparación de los daños sufridos -artículo 81-
- En la disposición transitoria I se sustituye "Agencia de Protección de los Habitantes" por *"PRODAHB"*.
- Se adiciona la disposición transitoria II para establecer que *"La PRODHAB continuará desarrollando sus funciones hasta que estas puedan ser asumidas de forma coordinada por la Agencia de Protección de Datos Personales creada en esta Ley, una vez que al menos su dirección haya sido designada y cuente con capacidad operativa para funcionar, lo que determinará la dirección mediante resolución que deberá ser publicada en el Diario La Gaceta y comunicada al público en general. Dicha transición deberá completarse en un periodo máximo de un año a partir de la entrada en vigor de esta Ley. Todos los procedimientos administrativos que estuvieran en trámite ante PRODHAB serán trasladados a la Agencia de Protección de Datos Personales a partir de que esta entre en funcionamiento, y serán continuados en el estado que estuvieren y hasta su efectiva finalización"*.
- En la disposición transitoria III se sustituye *"Agencia de Protección de los Habitantes"* por *"PRODHAB"*.
- En la disposición transitoria IV se adiciona que además de adecuar su funcionamiento, quienes ostenten condición de responsables y encargados, deberán adecuar el tratamiento de datos personales a las disposiciones de la Ley.

La exposición de motivos enmarca el objetivo del proyecto de ley, al expresar que:

> *"Este proyecto introduce reglas y protocolos claros al respecto para que el* ***uso de datos en el sector público sea transparente, seguro y respetuoso*** *de los derechos fundamentales de la ciudadanía.*

> ***Con esta nueva norma, Costa Rica contará con las herramientas más avanzadas en materia de protección de datos personales*** *para hacer frente a los retos de una economía fundamentada principalmente en los datos, que urge que los Estados promulguen reglas claras y estandarizadas que permitan conciliar la importancia de los flujos transfronterizos de datos personales con unas garantías suficientemente amplias que garanticen el cumplimento de la protección de datos de los ciudadanos en un entorno de gran incertidumbre tecnológica, en donde desconocemos no sólo el impacto que algunas tecnologías ya existentes podrán llegar a tener (piénsese en la Inteligencia Artificial), sino también las tecnologías que no han sido todavía desarrolladas."*

De manera que las enmiendas realizadas se enmarcan en lo señalado en la exposición de motivos, referente a realizar una reforma legal integral al marco regulatorio en la materia y a su vez, derogar *la "Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales".* De esta manera, con la propia explicación de la iniciativa se identifica que el texto sustitutivo obedece a modificar la propuesta del texto inicial, donde se plantean aspectos necesarios que se circunscriben al mismo eje temático que regula el texto inicial.

Es oportuno precisar que las enmiendas realizadas al texto sustitutivo obedecen al estudio del órgano legislativo, con la recepción de opiniones en la materia producto de las consultas por escrito realizadas a las institucionales, con el fin de añadir modificaciones al proyecto para que amplíe o fortalezca los objetivos de la propuesta supracitados.

En consideración con las enmiendas descritas anteriormente, es importante destacar que **las enmiendas planteadas en la propuesta de texto sustitutivo mantienen una conexión necesaria y razonable con el texto original. Es decir, las modificaciones guardan un hilo conductor básico, con la unidad lógica y propia de identidad con el texto original** -el cual consiste en derogar *la "Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales" y realizar una reforma legal integral al marco regulatorio en la materia*-, al ser un objetivo tan amplio, no se altera el contenido de lo propuesta en la exposición de motivos; es decir, se mantiene la naturaleza de ampliar sustancialmente las herramientas necesarias para otorgar mayores derechos y garantías en materia de protección de datos personales, de acuerdo con los estándares internacionales. De forma que esta asesoría considera que el texto sustitutivo en análisis **guarda el respeto del principio de conexidad con el texto original.**

En este sentido, **por la naturaleza de las enmiendas introducidas en el texto sustitutivo, es fundamental el resguardo del principio de publicidad**. Es decir, en este caso concreto, se requiere la necesaria publicidad del texto sustitutivo, a efecto de no vulnerar la garantía de la participación ciudadana.

2.2.- Estándares internacionales base del proyecto

En la exposición de motivos del proyecto se aprecia que el texto normativo tiene una marcada influencia de los más importantes estándares internacionales: el Reglamento (UE) 2060/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (RGPD)[15], el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de Estrasburgo del 28 de enero de 1981 y sus Protocolos (Convenio 108), los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, promulgados por la Red Iberoamericana de Protección de Datos Personales en el año 2017 y las Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales (1980).

Debido a lo anterior, esta asesoría considera importante presentar a continuación a las y los Diputados, una síntesis de lo más relevante que han desarrollado estos marcos internacionales en la materia y que ahora se pretenden incorporar en el ordenamiento jurídico costarricense mediante este proyecto de ley.

2.2.1.- Reglamento (UE) 2060/679 del Parlamento Europeo y del Consejo

El RGPD desarrolla un derecho uniforme de la protección de datos personales en los países miembros de la Unión Europea (UE), para lo cual establece como prioridades la protección de los datos personales como derecho fundamental, bajo la premisa de permitir al mismo tiempo los flujos transfronterizos de datos personales, no solo entre países miembros de la UE, sino también entre la UE y países no pertenecientes a la Unión y organizaciones internacionales, considerando el Reglamento como necesarias estas transferencias para la expansión del comercio y la cooperación internacionales (Considerandos 5 y 101).

Consiente del creciente aumento de la recopilación y automatización en el tratamiento de los datos personales gracias a la evolución tecnológica, el Reglamento ofrece un marco de seguridad jurídica para facilitar la libre circulación de datos personales, garantizando al mismo tiempo un elevado nivel de protección a sus ciudadanos, ya que entiende el Reglamento además que dicha protección es necesaria para asegurar otros derechos como la libertad, seguridad, justicia, progreso económico y social, así como al bienestar de las personas físicas.

Aunado a lo anterior, el RGPD reconoce el respeto de todos los derechos fundamentales, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística (Considerando 4).

[15] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016. https://www.boe.es/doue/2016/119/L00001-00088.pdf

El Reglamento de igual forma establece las pautas principales para el tratamiento de datos personales a través de los siguientes 7 principios: licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad, responsabilidad proactiva (Art. 5). Adicional, el RGPD plantea varias bases de licitud del tratamiento además del consentimiento informado.

En consecuencia y a causa de los estándares impuestos por el RGPD en el tratamiento de datos personales, las corporaciones multinacionales, en especial las grandes tecnológicas, han decidido observar el cumplimiento del Reglamento para garantizar de forma global la máxima protección de sus usuarios, lo cual se puede entender gracias al tamaño del mercado de la UE, los estándares estrictos establecidos en el Reglamento y la capacidad reguladora, este fenómeno de adaptación de la regulación europea al resto del mundo, se ha conocido como el efecto Bruselas[16].

El RGPD vino a marcar un hito en la materia desde su publicación en el año 2016, por tal razón, varios países en la región han decidido actualizar su legislación o desarrollar nuevas leyes en Protección de datos, adoptando los principios y derechos expresados en el Reglamento, tal es el caso de Brasil, Ecuador, Paraguay y Panamá, que cuentan con nuevos marcos legales promulgados después del año 2016 y los cuales siguen los lineamientos del RGPD. En el caso de Argentina y Chile estos discuten proyectos para actualizar su legislación, Argentina para reformar su Ley 25.326 del año 2000 y los Diputados y Diputadas de Chile discuten el proyecto de ley que busca reemplazar la Ley 19.628 sobre Protección a la Vida Privada y Protección de Datos de Carácter Personal.

2.2.2.- El Convenio 108

El Convenio 108[17] es firmado en Estrasburgo Francia el 28 de enero de 1981 y ha sido la base de las leyes internacionales de protección de datos de más de 40 países europeos[18], fue influenciado entre otros, por las Directrices de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales de 1980 y nace del interés de los países miembros de la UE por ampliar la protección de los derechos y las libertades de sus ciudadanos, especialmente el derecho a la vida privada y la libre circulación de información entre los países, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados.

Si bien en un inicio su adhesión fue exclusiva para países miembros de la UE, fue hasta el año 2013 que se permite la adhesión de países no miembros de la Unión

[16] https://es.wikipedia.org/wiki/Efecto_Bruselas
[17] Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. https://rm.coe.int/16806c1abd
[18] Informe Explicativo de Convenio. https://rm.coe.int/informe-explicativo-de-convenio/1680968479.

Europea, siendo Uruguay el primer país no europeo signatario del Convenio. En Latinoamérica, además de Uruguay, México y Argentina son partes del Convenio.

Debido a las nuevas amenazas a la vida privada derivadas del uso de nuevas tecnologías, el Convenio se ha modernizado en el año 2018 bajo el nombre Convenio 108+, esta actualización está disponible para adhesión de países a partir de junio del mismo año y en días recientes Argentina ha sido el país número 33 en firmar el Convenio 108+.

Para entender la importancia del Convenio para los intereses de Costa Rica, es de tal relevancia a nivel global que el 7 de mayo de 2021 el Instituto Interamericano de Derechos Humanos (IIDH) obtuvo por unanimidad la condición de Observador, lo que evidencia la seguridad jurídica en materia de protección de datos que los países parte proyectan a los demás países, organizaciones o a las personas.

En el año 2018 se celebró en el país el Encuentro Iberoamericano de Protección de Datos concluyó con éxito, en el cual Francisco Peiró, representante de la Delegación de la Unión Europea en Costa Rica, manifestó su interés en que Costa Rica logre la adecuación al Convenio 108, pues según su criterio “invertir en privacidad genera beneficio y crea nuevas oportunidades de negocio” en referencia a la mejora de flujo de datos, garantías e inversión extranjera que este paso podría concebir para nuestro país[19]. De acuerdo con lo señalado por el Proyecto de Ley aquí analizado, uno de sus principales objetivos es cumplir con los estándares de adecuación del Convenio para lograr su adhesión.

2.2.3.- Estándares de Protección de Datos Personales para los Estados Iberoamericanos

Los “Estándares de Protección de Datos de los Estados Iberoamericanos”[20] fueron aprobados y publicados por la Red Iberoamericana de Protección de Datos (RIPD o Red), el 20 de junio de 2017. Entre sus propósitos se encuentra impulsar y contribuir al fortalecimiento y adecuación de los procesos regulatorios en la región.

Los Estándares ofrecen un conjunto de directrices orientadoras que contribuyan a la emisión de normativa en materia de protección de datos personales en iberoamericana para aquellos países que aún no cuentan con estos marcos legislativos, o que sirvan como referente para la modernización y actualización de las legislaciones existentes.

De manera sucinta y conforme al Artículo 1, sus objetivos principales son: a) establecer un conjunto de principios y derechos de protección de datos personales; b) elevar el nivel de protección de datos personales para responder a las necesidades y exigencias internacionales; c) garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física en los

[19] Encuentro Iberoamericano de Protección de Datos. https://cutt.ly/bMjxGyo
[20] Estándares de Protección de Datos de los Estados Iberoamericanos. https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

Estados Iberoamericanos; d) facilitar el flujo de los datos personales entre los Estados Iberoamericanos y más allá de sus fronteras; e) Impulsar el desarrollo de mecanismos para la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos.

En cuanto a los principios que establecen los Estándares, el artículo 10.1. señala que "En el tratamiento de datos personales, el responsable observará los principios de legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad."

También estipula el texto reglas generales para la relación con el Encargado del tratamiento, para las transferencias de datos personales y establece medidas proactivas en el tratamiento de datos personales.

2.2.4.- Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales (1980)

Las Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales (1980) (Las Directrices) fueron adoptadas bajo los tres principios que siguen los países de la OCDE: democracia pluralista, respeto de los derechos humanos y economías de mercado abiertas, se hicieron efectivas el 23 de septiembre de 1980[21].

Las Directrices fueron revisadas en el 2013, el texto revisado modernizó el enfoque de la OCDE y reforzó su integración con otros trabajos sobre cooperación en materia de cumplimiento de la ley de privacidad[22], entre ellos el documento del Marco de Privacidad de la OCDE[23].

Similar a los demás instrumentos internacionales previamente reseñados, las Directrices plantean unos principios en línea don los demás marcos normativos internacionales: limitación de recogida, calidad de los datos, especificación del propósito, limitación de uso, salvaguardia de la seguridad, transparencia, participación individual y responsabilidad.

La OCDE recomienda a sus países miembros implementar Políticas en materia de privacidad para cumplir con las evaluaciones de cumplimiento, pero en especial recomienda a los países “evitar la elaboración de leyes, políticas y prácticas destinadas a proteger la privacidad y las libertades individuales que pudieran crear obstáculos al flujo transfronterizo de datos personales excediendo los requisitos para tal protección” (Tercera Parte).

[21] Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales (1980). https://www.oecd.org/sti/ieconomy/15590267.pdf.

[22] OECD work on privacy. https://www.oecd.org/digital/ieconomy/privacy.htm.

[23] THE OECD PRIVACY FRAMEWORK. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

De lo anterior, se interpreta que en la actualidad la protección de datos es un asunto global que requiere armonización y reglas de aplicación homogéneas en las diferentes jurisdicciones, con el propósito de ofrecer la máxima protección de los datos personales de cualquier persona independiente de su nacionalidad y además garantizar el flujo de datos personales entre países, dentro de un marco de seguridad jurídica, bajo este prisma, se observa que este Proyecto de Ley 23.097 se inspira en los marcos internacionales más robustos en Protección de Datos y respecto a los cuales Costa Rica presenta un rezago importante en materia de cumplimiento y adecuación.

III.- SOBRE EL ARTICULADO DEL TEXTO SUSTITUTIVO

La iniciativa, como se mencionó anteriormente, pretende la aprobación de una nueva legislación que incluya la derogatoria de la ley actual. La propuesta de texto sustitutivo contiene más del doble del articulado del actual texto de la Ley N°8968, y se aparta en su mayoría, del contenido de esta.

Como primer elemento importante a tomar en consideración sobre el texto del proyecto de ley, según se ha indicado tanto en la exposición de motivos, la idea es actualizar la regulación a la luz de los parámetros del Reglamento General de Protección de Datos N°679-2016 de la Comisión Europea[24], Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales N°3/2018 de España[25] y los Estándares de Protección de Datos Personales de la Red Iberoamericana de Protección de Datos Personales[26].

De esta manera, a la luz de las observaciones enviadas por distintos sectores y entidades del país consultadas, el texto sustitutivo incorpora muchas de ellas. Para estos efectos, se presenta un listado de los temas del articulado y las modificaciones introducidas de mayor relevancia, con comentarios.

3.1. Capítulo I Disposiciones generales

En el ***Capítulo I Disposiciones generales*** se modifican:

- Objetivo -artículo 1-
- Definiciones[27] -artículo 2-

[24] Reglamento General de Protección de Datos Personales (RGPDP) número 2016/679, el cual entró en vigor en la Unión Europea el 25 de mayo de 2018.
[25] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales de España, la cual entró en vigor el 7 de diciembre de 2018.
[26] Estándares de Protección de Datos Personales para los Estados Iberoamericanos, del 20 de junio de 2017. Los cuales pueden ser consultado en la siguiente dirección web: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf
[27]Específicamente a: Anonimización, Base de datos, Cesión de datos, Consentimiento, Datos Biométricos, Datos genéticos, Datos personales, Datos personales sensibles, Datos relativos a la

- Ámbito de aplicación subjetivo -artículo 3-
- Ámbito de aplicación objetivo -artículo 4-
- Datos de personas fallecidas -artículo 5-
- Ámbito de aplicación territorial -artículo 6-
- Excepciones generales al derecho a la protección de datos personales -artículo 7-
- Tratamientos de datos por obligación legal, interés público o ejercicio de poderes públicos y cesiones interinstitucionales de datos en el sector público -artículo 8-
- Tratamiento de datos personales sensibles -artículo 10-
- Tratamiento de datos personales relativos a condenas e infracciones penales -artículo 11-
- Tratamiento de datos personales sensibles obtenidos de fuentes de acceso público -artículo 12-

El artículo 1 referido al objetivo de la ley, aclara que los principios y derechos de protección de datos personales son aplicables a los habitantes, independientemente de su nacionalidad y que la finalidad de facilitar el flujo internacional de datos es coadyuvar el crecimiento económico del país, no de la región; modificaciones que fueron introducidas en contraste con el texto original, en virtud de los comentarios de UCCAEP.

El artículo 2 establece las definiciones. Las siguientes fueron objeto de modificaciones significativas, en aras de precisar su concepto:

Anonimización: Se agrega que la aplicación de medidas para impedir la identificación o reidentificación de una persona física, no debe ser solo sin esfuerzos desproporcionados, sino sin plazos de esta misma naturaleza. Adicionalmente, se agrega que se tendrán en cuenta para estos efectos "*factores como los costos y el tiempo necesario para la identificación o reidentificación de la persona a la luz de la tecnología disponible en el momento del tratamiento*."

Base de datos: Distinto al texto original, se señala que la base de datos será tal, *"independientemente de que los datos se encuentren respaldados en soportes físicos o electrónicos",* por criterio de UCCAEP.[28]

Cesión de datos: Se amplían los sujetos de la definición, al establecer que la cesión de datos también se dará cuando la revelación de estos sea realizada a una entidad u organización distinta al titular, por recomendación de UCCAEP.[29]

---

salud, Encargado, Exportador, Fuentes de acceso público, Grupo económico, Elaboración de perfiles, Normas corporativas vinculantes, Responsable, Seudoanonimización, Sistema de identificación biométrica, Tercero, Titular, Tratamiento, y Violación de la seguridad de los datos personales.

[28] **UCCAEP**. Oficio N° DE-086-22 de 30 de agosto de 2022.
[29] Ibíd.

Consentimiento: Se mejora indudablemente la aplicación práctica del concepto, al incluir que dicha manifestación de voluntad podrá ser proveniente del representante del titular de los datos.

Datos biométricos: Se incluye al final del concepto la frase *"entre otros"*, con la intención de ejemplificar que dicha definición no se limita únicamente a datos dactiloscópicos o imágenes faciales. Además, se eliminan los datos conductuales, ya que el comportamiento no identifica inequívocamente al titular y se mantiene en constante cambio, como lo indicó la Asociación Latinoamericana de Internet.[30]

Datos personales sensibles: El texto original incluye como criterio para determinar un dato personal sensible aquellos *"cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste"*. Esta frase se elimina en el texto sustitutivo, en atención a los comentarios de la Asociación Latinoamericana de Internet, en virtud de que ello requiere de un esfuerzo interpretativo que puede distorsionar la posibilidad de realizar tratamientos legítimos y genera una innecesaria amplitud.[31] Asimismo, en el marco de los comentarios de la misma entidad, los de la Corte Suprema de Justicia[32], y los de CAMTIC[33], se elimina el carácter enunciativo del artículo, para generar mayor seguridad jurídica y eliminar el margen de interpretación.

Datos relativos a la salud: En atención a los comentarios del Colegio de Optometristas[34] y el Colegio de Farmacéuticos[35], se incluye posterior a "*incluida la prestación de servicios de atención sanitaria"*, la frase *"en el ámbito público o privado"*, para mayor seguridad en cuanto a los alcances del concepto.

Fuentes de acceso público: Siguiendo los comentarios de la Asociación Latinoamericana de Internet, se elimina la prohibición presente en el texto original, de existir solo cuando una ley les haya dado ese carácter o sea necesario para cumplir los fines previstos en esa ley. Lo anterior, argumentado con base en el carácter restrictivo de esta limitación[36], lo cual fue, además, replicado por la Corte Suprema de Justicia, indicando que el hecho de que sus bases de datos deban seguir este criterio, afectaría su operatividad[37]. Por otro lado, motivado por la sugerencia de UCCAEP, se enumeran adicionales supuestos de fuentes de acceso

[30] **Asociación Latinoamericana de Internet**. Oficio de 29 de julio de 2022, suscrito por la señora Sissi Maribel de la Peña Mendoza, directora para México y Centroamérica.
[31] Ibíd.
[32] **Corte Suprema de Justicia.** Oficio N°SPP155-2022, suscrito por la señora Silvia Navarro Romanini, secretaria general.
[33] **Cámara de Tecnologías de Información y Comunicación.** Oficio de 8 de agosto de 2022, suscrito por el señor Christian Sánchez Alcázar, director ejecutivo.
[34] **Colegio de Optometristas de Costa Rica**. Oficio N°COCR-174-Ago-2022 de 22 de agosto de 2022, suscrito por el doctor Enrique Garita Mora, presidente.
[35] **Colegio de Farmacéuticos de Costa Rica.** Oficio N°JD-0184-08-2022 de 23 de agosto de 2022, suscrito por la doctora Lidiette Fonseca González, presidente.
[36] **Asociación Latinoamericana de Internet**. Oficio de 29 de julio de 2022. Op. cit.
[37] **Corte Suprema de Justicia.** Oficio N°SPP155-2022. Op.cit.

público, como: el diario oficial La Gaceta y el Boletín Judicial; las publicaciones realizadas en medios masivos de comunicación; y, las guías, publicaciones, anuarios, directorios y similares que tengan la finalidad comunicar públicamente la pertenencia de determinadas personas a organizaciones gremiales, asociaciones, colegios profesionales[38]. Lo anterior se complementa en el texto sustitutivo, con la inclusión de la frase *"El funcionamiento de las bases de datos de acceso público respetará los términos de la presente Ley, en especial en cuanto a los principios de legitimación y minimización."*

Grupo económico: Previamente titulado *"grupo empresarial"*, se abandona el concepto *"grupo constituido por una empresa que ejerce el control y sus empresas controladas"*, por la dificultad de comprensión que generaba, de acuerdo con el Ministerio de Economía, Industria y Comercio[39]. En cambio, se sustituye por la definición presente en la Ley 9736, por solicitud de UCCAEP[40].

Tratamiento: Se sustituye el concepto *"transferencia"* por *"cesión"*.

Finalmente, se eliminó la definición de transferencia de datos y se incluyó la de violación de la seguridad de los datos personales.

El artículo 3 regula el *"ámbito de aplicación subjetivo"* de la ley, la cual será aplicable a *"las personas físicas o jurídicas de carácter privado, y a la Administración Pública en sentido amplio, que realicen tratamiento de datos personales en el ejercicio de sus actividades y funciones".* En ese sentido, el texto original hacía referencia a la *"Administración Pública centralizada y descentralizada"*, pero se modificó al texto citado, lo cual, con toda seguridad, engloba la totalidad de la Administración.

El artículo 4 regula el *"ámbito de aplicación objetivo"* de la ley, definiendo que esta será aplicable *"al tratamiento de datos personales de personas físicas que consten o estén destinados a constar en soportes físicos, automatizados total o parcialmente, o en ambos soportes, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización"*. Por otro lado, según la redacción del texto original, los supuestos de inaplicabilidad de la norma son 4:

> *"a. Cuando los datos personales estén destinados exclusivamente a actividades en el marco de la vida familiar o doméstica de una persona física, esto es, 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.*
>
> *b. La información anónima, es decir, aquélla que no guarda relación con una persona física identificada o identificable, así como los datos personales sometidos*

[38] **UCCAEP**. Oficio N° DE-086-22. Op. cit.
[39] **Ministerio de Economía, Industria y Comercio.** Oficio N°MEIC-DM-OF-340-2022 de 9 de agosto de 2022, suscrito por la señora Giannina Córdoba Corrales, jefa de despacho.
[40] **UCCAEP**. Oficio N° DE-086-22. Op. cit.

a un proceso de anonimización de tal forma que el titular no pueda ser identificado o reidentificado.

c. A los tratamientos de persona fallecidas, sin perjuicio de lo establecido en el artículo 5 de esta Ley.

d. A los tratamientos sometidos a la normativa sobre protección de materias clasificadas o secretos de Estado."

A estos efectos, es oportuno valorar la solicitud expresa de Access Now y Derechos Digitales, quienes desarrollaron que *"los datos anonimizados, los datos de personas fallecidas o los datos que constituyen secreto de estado pueden ser excepciones para, por ejemplo, la obtención del consentimiento del titular, más no para otras estipulaciones"*[41]. Por consiguiente, se modificó la redacción dentro del texto sustitutivo, y se eliminaron los incisos c y d.

El artículo 5 establece las pautas para el ejercicio de los derechos reconocidos por la Ley, sobre los datos de una persona fallecida. A estos efectos, en el texto sustitutivo, se cambió el concepto *"personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos"*, por *"herederos, previa acreditación de su condición"*, como los legitimados para ejercer estos derechos. Lo anterior, fundamentado en las sugerencias de la Asociación Latinoamericana de Internet, pues era un concepto amplio que podía dar lugar a suplantación de identidad y generaba inseguridad jurídica en cuanto a sus alcances.[42]

El artículo 6 introduce la regulación del *"ámbito de aplicación territorial"* para el tratamiento de datos personales, en cuatro supuestos:

"a. Por un responsable o encargado con establecimiento en la República de Costa Rica.

b. Por un responsable o encargado sin establecimiento en la República de Costa Rica, cuando las actividades del tratamiento estén relacionadas con la oferta de bienes o servicios dirigidos a los habitantes de la República de Costa Rica, o bien, estén relacionadas con el control de su comportamiento, en la medida en que éste tenga lugar en la República de Costa Rica.

c. Por un responsable o encargado que no cuente con establecimiento en la República de Costa Rica, pero le resulte aplicable la legislación nacional, derivado de la celebración de un contrato o en virtud de las normas del derecho internacional privado.

d. Por un responsable o encargado sin establecimiento en territorio costarricense y que utilice o recurra a medios, automatizados o no, situados en ese territorio para tratar datos personales, salvo que dichos medios se utilicen solamente con fines

[41] **Access Now y Derechos Digitales**. Oficio suscrito por los señores Gaspar Pisanu y Michel Roberto de Souza.
[42] **Asociación Latinoamericana de Internet**. Oficio de 29 de julio de 2022. Op. cit.

de tránsito."

En palabras de CAMTIC, el punto d se debería eliminar, pues impone el derecho local a quien contrata un proveedor de servicios o un encargado de tratamiento en el país. Realmente, únicamente debería estar el encargado sujeto a dicha normativa, no el responsable.[43] De forma congruente con lo establecido por este comentario, se eliminó el punto d del inciso 1 de la redacción del texto sustitutivo, lo cual elimina limitaciones innecesarias a servicios como hosting y procesamiento de datos.

El artículo 7 establece las *"excepciones generales al derecho a la protección de datos"*, es decir, aquellos casos en los que se puede limitar este derecho. Es oportuno citar la opinión de Access Now y Derechos Digitales, donde citan con base en el texto original, que se debe modificar la redacción del artículo, sustituyendo el primer inciso *"Cualquier ley que tenga como propósito limitar el derecho a la protección de datos personales contendrá, como mínimo, disposiciones relativas a:"*, por *"No se podrá limitar el derecho a la protección de datos personales mediante ley, salvo de manera excepcional, cuando existan razones que justifiquen su necesidad, sean adecuadas y proporcionales en una sociedad democrática, y respeten los derechos y las libertades fundamentales de los Titulares"*. De esta manera, se garantiza una protección más amplia a este derecho, al estar la limitación sujeta a excepcionalidad, que además deberá conjugarse con ciertas disposiciones mínimas enlistadas en el artículo.[44]

Por otro lado, bajo las mismas recomendaciones y para mayor congruencia con los motivos anteriormente citados, se elimina el inciso 2, que disponía que *"las leyes serán las necesarias, adecuadas y proporcionales en una sociedad democrática, y deberán respetar los derechos y las libertades fundamentales de los titulares", y* se sustituye por el inciso 3, cuya redacción se mantiene entre ambos textos.

El artículo 8 introduce los *"tratamientos de datos por obligación legal, interés público o ejercicio de poderes públicos y cesiones interinstitucionales de datos en el sector público"*. Distinto al texto original, en esta versión se aclara que se refiere al sector público y se sustituye la palabra *"transferencia",* por *"cesión"* a lo largo del texto. Asimismo, en atención a los comentarios de UCCAEP, se incluye que "no deberán ser menores a las garantías y derechos establecidos en esta Ley", las condiciones especiales que pueda imponer esta norma, a la hora de realizar tratamientos de esta naturaleza. En este orden de ideas, se fundamenta que los convenios interinstitucionales deben hacer referencia adicionalmente a "los medios para solicitar el efectivo ejercicio de los derechos del Titular"; cambio que se ve reflejado en el texto sustitutivo.[45]

---

[43] **Cámara de Tecnologías de Información y Comunicación.** (CAMTIC) Oficio de 8 de agosto de 2022. Op. cit.
[44] [44] **Access Now y Derechos Digitales**. Oficio suscrito por los señores Gaspar Pisanu y Michel Roberto de Souza. Op. cit.
[45] **UCCAEP**. Oficio N° DE-086-22. Op. cit.

Por otro lado, en este mismo artículo, se introduce que cuando la cesión deba ser autorizada de previo por la Agencia de Protección de Datos, esta deberá verificar en un plazo no mayor a 10 días hábiles, el cumplimiento de las siguientes condiciones:

> *"i) la cesión sea absolutamente necesaria para cumplir con el fin público invocado y asignado por ley a la entidad receptora;*
> *ii) que los datos a ceder son los estrictamente necesarios y adecuados para ese fin.*
> *iii) que la entidad receptora de los datos cuenta con las medidas de seguridad, protocolos y demás garantías establecidas en esta Ley, para proteger la integridad, disponibilidad y confidencialidad de los datos."*

Se incluye que los convenios institucionales deberán ser comunicados a la Agencia de Protección de Datos y se aclara, en un nuevo inciso 6, que *"no se considerará cesión ni transferencia de datos la remisión de datos personales realizada por un Responsable o Encargado del sector público ante una orden de una autoridad judicial competente en el marco de sus facultades legales, siempre que dicha orden se realice dentro de una investigación o procedimiento específico"*.

El artículo 10 titulado *"tratamiento de datos personales sensibles",* sobrelleva una serie de modificaciones, impulsadas por las sugerencias de distintas entidades:

1) Se adiciona en cuanto al inciso d sobre consentimiento expreso, que este *"podrá derivar de un contrato donde el tratamiento de tales datos sensibles resulta indispensable, siempre que así conste que se haya informado al Titular"*, en virtud de los comentarios de CAMTIC. [46]
2) Por sugerencia del Colegio de Optometristas y el Colegio de Farmacéuticos, se incluyen como excepciones *"la investigación en salud"* y las *"pandemias debidamente declaradas por las autoridades de salud competentes"*. [47]
3) Se incluyen 3 nuevas excepciones a la prohibición del tratamiento de datos sensibles en los incisos i, j, k. Desarrollan:
   "i. El tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del Responsable o del Titular en el ámbito del derecho laboral, de la seguridad social o ayudas sociales, en la medida en que así lo autorice el marco normativo y establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del Titular", motivado por los comentarios de Access Now y Derechos Digitales.[48]

[46] **Cámara de Tecnologías de Información y Comunicación.** Oficio de 8 de agosto de 2022. Op. cit.
[47] **Colegio de Optometristas de Costa Rica**. Oficio N°COCR-174-Ago-2022. **Colegio de Farmacéuticos de Costa Rica.** Oficio N°JD-0184-08-2022. Op. cit.
[48] **Access Now y Derechos Digitales**. Oficio suscrito por los señores Gaspar Pisanu y Michel Roberto de Souza. Op. cit.

"j. El tratamiento sea efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los Titulares", en razón de las sugerencias de UCCAEP, Access Now y Derechos Digitales.[49]

"k. El tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial". Este último a solicitud de la Corte Suprema de Justicia, por las implicaciones que el caso contrario podría tener sobre las bases de datos que operan en la actualidad, y que son de consulta obligada y diaria.[50] Asimismo, la redacción incorporada fue propuesta por Access Now y Derechos Digitales.[51]

Sobre el artículo 11 referente al *"tratamiento de datos personales relativos a condenas e infracciones penales"*, es conveniente hacer referencia a los comentarios de la Corte Suprema de Justicia. Indica que, en el texto original, hacía falta una mención sobre *"cómo tratar este tipo de datos cuando una parte en un proceso penal es funcionario público y los hechos están relacionados con el ejercicio de su cargo; ello en tanto no se puede diferenciar donde la ley no lo hace"*.[52] En relación con este tema, se destacan dos ajustes en el texto sustitutivo: 1. La inclusión del Ministerio de Justicia como sujeto facultado para contar con un registro completo de condenas penales. 2. La aclaratoria, expresada a través de un inciso segundo, de que *"además de los funcionarios judiciales involucrados, los abogados en ejercicio podrán realizar tratamiento de datos personales referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas cuando tengan por objeto tratar la información tratada por sus clientes para el ejercicio de sus funciones, bajo la obligación de secreto profesional".*

La norma originalmente incluía en el artículo 12, la prohibición absoluta de la existencia de datos personales sensibles en bases de datos de acceso público. Dicha disposición, como fue desarrollado en los comentarios de la Asociación Latinoamericana de Internet, era excesiva y podía afectar servicios existentes en la actualidad, con profunda necesidad para la población, como lo sería el Diario Oficial La Gaceta.[53] Afortunadamente, se eliminó del texto sustitutivo.

[49] Ibíd.
[50] **Corte Suprema de Justicia.** Oficio N°SPP155-2022. Op.cit.
[51] **Access Now y Derechos Digitales**. Oficio suscrito por los señores Gaspar Pisanu y Michel Roberto de Souza. Op. cit.
[52] **Corte Suprema de Justicia.** Oficio N°SPP155-2022. Op.cit.
[53] **Asociación Latinoamericana de Internet**. Oficio de 29 de julio de 2022. Op. cit.

3.2. Capítulo II Principios de protección de datos personales

En el ***Capítulo II Principios de protección de datos personales*** se modifican:

- Principios aplicables al tratamiento de datos personales -artículo 13-
- Principio de exactitud -artículo 14-
- Principio de legitimación -artículo 15-
- Principio de lealtad -artículo 18-
- Principio de transparencia -artículo 19-
- Principio de finalidad -artículo 20-
- Principio de exactitud -artículo 22-
- Principio de responsabilidad proactiva -artículo 23-
- Principio de seguridad -artículo 24-
- Notificación de violación a la seguridad de los datos personales -artículo 25-

En el ***Capítulo II Principios de protección de datos personales*** se incorporaron principios que son parte del Reglamento General de Protección de Datos Personales (RGPDP). Se desarrollan los siguientes principios: exactitud[54], legitimación[55], lealtad[56], transparencia[57], limitación de la finalidad[58], minimización[59], exactitud[60], responsabilidad[61], seguridad[62] y confidencialidad[63].

Este listado se encuentra en el artículo 13, el cual originalmente establecía que *"en el tratamiento de datos personales, el responsable observará los principios de exactitud, legitimación, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad"*. Con las reformas introducidas al texto, en este caso, producto de los comentarios de UCCAEP, se generalizó la disposición, eliminando que será el responsable quien observará estos principios, sino *"el tratamiento deberá realizarse conforme a los principios"*[64]. Algunos de dichos principios, sufrieron cambios en su denominación, específicamente el de proporcionalidad (ahora minimización), exactitud (ahora calidad) y finalidad (ahora limitación de la finalidad).

[54] Artículo 14.
[55] Artículo 15.
[56] Artículo 18.
[57] Artículo 19.
[58] Artículo 20.
[59] Artículo 21.
[60] Artículo 22.
[61] Artículo 23.
[62] Artículo 24.
[63] Artículo 26.
[64] **UCCAEP**. Oficio N° DE-086-22. Op. cit.

El artículo 14, regula el *"principio de exactitud"*. Este principio abarca los supuestos en los que la existencia de datos inexactos no es imputable al responsable, teniendo él la obligación de tomar todas las medidas razonables para que se supriman o rectifiquen. En ese sentido, en la redacción del texto sustitutivo, se tomó en consideración la recomendación de UCCAEP, en virtud del cual se incluyó la siguiente oración, a manera de un inciso 2: *"En todos los casos anteriores el Titular tendrá derecho de solicitar rectificación de sus datos personales"*.[65]

El artículo 15 en la regulación del *"principio de legitimación"*, señala los presupuestos bajo los cuales el tratamiento que se realice será legítimo. Siguiendo la línea del ajuste que se realizó en el texto sustitutivo al artículo 13, se modificó el inciso primero para que, en atención a los comentarios de la misma entidad, se cambiara *"El tratamiento de los datos personales será legítimo solo cuando se realice con fundamento en alguna de las siguientes bases de legitimación"*, en vez de *"El responsable solo podrá tratar datos personales cuando se presente alguno de los siguientes supuestos"*. Por otro lado, es importante tomar en consideración los comentarios de Access Now y Derechos Digitales, donde señalan sobre el texto original que "*tanto el párrafo 2 como el párrafo 3 del Artículo 15 utilizan una terminología ambigua que puede dar lugar a confusión y abarcan supuestos que están cubiertos en su totalidad por otras disposiciones de la misma ley"*. En ese sentido, se eliminaron ambos párrafos. Además, sugirieron agregar un nuevo párrafo dos, para delimitar los alcances de los incisos b, c, f y h, que indique que estos *"estarán sujetos al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta Ley y a los criterios de legalidad, proporcionalidad y necesidad".* [66]

El artículo 18 regula el *"principio de lealtad"*, estableciendo que "*1. El Responsable tratará los datos personales en su posesión privilegiando la protección de los intereses del Titular y absteniéndose de tratar éstos a través de medios engañosos o fraudulentos. 2. Para los efectos de esta Ley, se considerarán desleales aquellos tratamientos de datos personales que den lugar a una discriminación injusta o arbitraria contra los Titulares o excedan las expectativas razonables del Titular respecto a sus finalidades"*. Cabe resaltar, que la última frase *"o excedan las expectativas..."*, es producto de las sugerencias de Access Now y Derechos Digitales, quienes argumentaron que también debe considerarse desleal el tratamiento de esta naturaleza, no limitándose a aquellos casos de discriminación injusta o arbitraria.[67]

El artículo 19 referido al *"principio de transparencia*", mantiene en su mayoría el texto original. El único cambio recae en el inciso d, que previamente establecía que el responsable debe, entre otros, proporcionar al titular la información sobre *"Las transferencias, nacionales o internacionales, de datos personales que pretenda*

[65] Ibíd.
[66] **Access Now y Derechos Digitales**. Oficio suscrito por los señores Gaspar Pisanu y Michel Roberto de Souza. Op. cit.
[67] Ibíd.

realizar, incluyendo los destinatarios y las finalidades que motivan la realización de las mismas". En palabras de la Asociación Latinoamericana de Internet, *"Esta obligación resulta complicada en la práctica para el responsable, dado que, en el mundo digital globalizado, y en el cual las transferencias internacionales son innumerables, muchas veces es impracticable brindar el nivel de detalle que requiere el artículo, teniendo en cuenta que los países de destino y los destinatarios pueden variar con frecuencia. Tampoco resultaría beneficioso en términos prácticos para los interesados que los responsables proporcionen listados extensos referidos a las transferencias internacionales. En todo caso, siguiendo la línea del GDPR y otras legislaciones de la región, debería bastar y extenderse la posibilidad de cumplir al informar la existencia de transferencias internacionales o categorías de destinatarios"*.[68] Por lo tanto, se modificó el inciso para en adelante leerse *"d. La existencia de cesiones y/o transferencias internacionales de datos personales, los destinatarios, las categorías de datos y finalidades que motivan la realización de las mismas"*.

El artículo 20 en la regulación del *"principio de finalidad"*, señala que los tratamientos se limitarán al cumplimiento de finalidades determinadas, explícitas y legítimas. Se recomienda incluir en el texto sustitutivo *"o que no resulten"* antes de "análogas y compatibles", en atención a los comentarios de la Asociación Latinoamericana de Internet, en virtud de que *"pueden existir situaciones donde no necesariamente se debe contar con una nueva base legal, como aquellos casos donde la finalidad es análoga o compatible con la finalidad que motivó el tratamiento, es decir, no existen cambios materiales al tratamiento que justifiquen la carga administrativa para ambas partes de obtener nuevamente un consentimiento. Esto coincide con el contenido de varias regulaciones de la región tendientes a proveer de mayor certeza y efectividad jurídica la evidencia de consentimiento respecto de las modificaciones a finalidades de tratamiento*".[69]

El artículo 22, previamente titulado *"principio de calidad"*, regula el *"principio de exactitud",* que establece el deber del responsable de poner en práctica medidas para mantener exactos, completos y actualizados los datos. Asimismo, fue modificado, con base en las sugerencias de las siguientes entidades:

1. Corte Suprema de Justicia: sugirió se aclarare si el tratamiento ulterior de datos personales con fines archivísticos, de investigación o estadísticos, debe ser siempre anonimizado o no, por poder esto afectar el manejo de sus propias bases de datos, como Nexus PJ. Por lo que en el inciso 4 se incluyó *"De igual forma, se entenderán válidas las excepciones contenidas en leyes especiales en materia de archivo, investigación o estadística".*[70]
2. CAMTIC: solicitó incluir una referencia al interés legítimo del responsable en la conservación de los datos, más allá del tiempo requerido para el

[68] **Asociación Latinoamericana de Internet**. Oficio de 29 de julio de 2022. Op. cit.
[69] Ibíd.
[70] **Corte Suprema de Justicia.** Oficio N°SPP155-2022. Op.cit.

cumplimiento de la finalidad requerida.[71] Por lo anterior, se incluyó en el inciso 4 que *"el Responsable podrá conservar los datos más allá del plazo de conservación en cumplimiento de un interés legítimo, para el cumplimiento de la finalidad inicial de su tratamiento y con pleno respeto a los derechos y garantías del Titular*".

3. UCCAEP: por la redacción propuesta, se incluyó al final del inciso 1, que el responsable *"adoptará todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos"*. Adicionalmente, propuso el cambio de nombre previamente descrito.[72]

El artículo 23 incorpora el *"principio de responsabilidad proactiva"*, que enlista los mecanismos que el responsable podrá adoptar, para cumplir con los principios y obligaciones de la norma. Se modificó la redacción de dos de esos mecanismos, establecidos en los incisos b y g, y se agregaron 2 más, en incisos h e i. Esta redacción fue propuesta por UCCAEP, la cual establece:

1. *"d. Implementar medidas para el análisis de los riesgos asociados al tratamiento de datos personales, y en caso de que corresponda, evaluaciones de impacto de datos personales"*. Previamente establecía únicamente sistemas de administración de riesgos asociados al tratamiento de datos personales.
2. *"g. Establecer procedimientos para recibir y responder dudas y quejas de los Titulares"*, adicionando *"en los plazos establecidos en esta Ley"*.
3. *"h. Llevar el registro de tratamiento de datos personales, cuando corresponda conforme lo establecido en esta Ley".*
4. *"i. Designar un delegado de protección de datos personales cuando sea requerido conforme esta Ley*".[73]

El artículo 24 regula el *"principio de seguridad"*, que establece la importancia de medidas para garantizar la confidencialidad, integridad y disponibilidad de los datos. En el texto original, se establecía esto como deber únicamente del responsable. Sin embargo, en el texto sustitutivo se adiciona al encargado. Asimismo, en el listado de factores que debe tomar en cuenta el responsable a la hora de determinar las medidas, se cambia el del inciso a, eliminando, dentro de la consideración del riesgo para los derechos y libertades de los titulares, *", en particular, por el valor potencial cuantitativo y cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión".* Lo anterior en atención a los comentarios de UCCAEP[74]. Por otro lado, también se eliminó el inciso 6.

[71] **Cámara de Tecnologías de Información y Comunicación.** Oficio de 8 de agosto de 2022. Op. cit.
[72] **UCCAEP**. Oficio N° DE-086-22. Op. cit.
[73] Ibíd.
[74] Ibíd.

El artículo 25, referido a las *"notificaciones de violación a la seguridad de los datos personales"*, se ajustó en el sentido de que en el inciso 4, se aclaró que la notificación a la que se hace referencia se debe realizar tanto a los titulares afectados, como a la Agencia de Protección de Datos. Asimismo, se incluyó en el inciso 4 que, si bien el Responsable debe notificar la información que tenga a su disposición, cuando por la gravedad o naturaleza particular del incidente sea imposible identificar todos los elementos anteriores dentro de las 72 horas, debe *"presentar actualizaciones periódicas a la Agencia de Protección de Datos Personales sobre el informe inicial, cada vez que se disponga de información nueva o diferente sobre el incidente, hasta la fecha en que la investigación del incidente haya concluido y que el incidente asociado se haya mitigado y resuelto por completo*". Por lo tanto, se eliminó que deba *"completar y notificar el resto de la información indicada en un plazo no mayor a cinco días hábiles desde que haya tenido conocimiento del incidente"*. La denominación de este artículo se modificó, al cambiarse la palabra *"vulneración"*, por *"violación"*.

3.3. Capítulo III Derechos del titular

En el ***Capítulo III Derechos del titular*** se modifican:

- Derechos de acceso, rectificación, cancelación, oposición (ARCO) y de portabilidad -artículo 27-
- Disposiciones generales sobre ejercicio de los derechos -artículo 28-
- Derecho de acceso -artículo 29-
- Derecho de cancelación o supresión -artículo 31-
- Derecho de oposición -artículo 32-
- Derecho a no ser objeto de decisiones individuales automatizadas -artículo 33-
- Ejercicio de los derechos ARCO y de portabilidad -artículo 36-

En el artículo 27 sobre los *"derechos de Acceso, Rectificación, Cancelación y Oposición y de portabilidad"*, se adiciona un inciso 3, que establece *"Los derechos del Titular son irrenunciables. Será nula de pleno derecho toda estipulación en contrario"*.

En el artículo 28 se establecen las *"disposiciones generales sobre ejercicio de los derechos",* de manera que se desarrolla cómo deben proceder el responsable, encargado y titular, ante una solicitud de ejercicio de derechos. Al respecto, Access Now y Derechos Digitales indicaron, *"Si bien algunos de los derechos incluidos en la ley establecen un plazo para que el responsable cumpla con el pedido del titular del dato otros, como el derecho de acceso, no lo contienen".*[75] Por lo que se incluyó en el inciso 4 un plazo de cinco días hábiles, en el cual responsable deberá

[75] **Access Now y Derechos Digitales**. Oficio suscrito por los señores Gaspar Pisanu y Michel Roberto de Souza. Op. cit.

comunicar la respuesta a una solicitud de ejercicio de derechos, salvo que la ley establezca otro plazo.

El artículo 29 regula el *"derecho de acceso"*, que versa sobre el derecho del titular, previa acreditación de su identidad, de recibir en un plazo de 5 días, confirmación sobre si se están tratando sus datos. Con este texto sustitutivo se incluyó la aclaratoria sobre el plazo que opera y la acreditación de la identidad del titular. Se agregó, además, otra información que debe brindar el responsable al titular, como: bases legales que legitiman las finalidades del tratamiento, el derecho a a presentar una reclamación ante la Agencia y la información sobre las transferencias internacionales de datos que se hayan efectuado o se prevean efectuar, incluyendo los países de destino. En el caso de esta última, se incluyó en el inciso d, pues se eliminó el contenido previamente establecido, que hacía referencia al plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo. Asimismo, por sugerencia de UCCAEP, se incluyó la existencia o no de decisiones automatizadas respecto del tratamiento de sus datos personales, incluida la elaboración de perfiles, como información que debe brindar el responsable.[76]

En el artículo 31 se incluye el *"derecho de cancelación o supresión",* cuyo título fue modificado al adicionar *"supresión"* y eliminar la referencia que previamente se hacía al derecho de olvido. Lo anterior, en razón de que, como lo fundamenta la Asociación Latinoamericana de Internet, se trataba de derechos diferentes. En virtud de los mismos comentarios, se eliminó el inciso 2 que versaba sobre la obligación del responsable de informarle a otros responsables la supresión de datos. Esto se tornaría muy arduo y oneroso para el responsable.[77] Asimismo, en el inciso 2.c, se eliminó *"en el ámbito de salud pública"*, para que más bien, se refiriera al interés público en general. Al inciso 1.e se le agregó el supuesto de que los datos se deban suprimir para cumplir con una orden de autoridad competente.

Finalmente, se adicionó un inciso 2.f, el cual exime al responsable del deber de proceder con la cancelación, cuando *"los datos personales deban ser conservados durante los plazos previstos en disposiciones legales o contractuales, entre el Responsable o Encargado del tratamiento y el Titular de los datos"*.

El artículo 32 estipula los supuestos en los que el titular puede oponerse al tratamiento de sus datos personales, conocido como *"derecho de oposición"*. Se incluyen nuevos supuestos, tales como la publicidad y la prospección comercial, así como se impone al responsable un plazo máximo de 5 días hábiles para responder la solicitud.

[76] **UCCAEP**. Oficio N° DE-086-22. Op. cit.
[77] **Asociación Latinoamericana de Internet**. Oficio de 29 de julio de 2022. Op. cit.

El artículo 33 incluye el *"derecho a no ser objeto de decisiones individuales automatizadas",* el cual consiste en el derecho a no ser objeto de una decisión basada en el tratamiento automatizado de datos, incluida la elaboración de perfiles. Por medio de una redacción propuesta por la Asociación Latinoamericana de Internet*,* además del criterio de que produzcan efectos jurídicos al titular, se introdujo que afecten sus intereses de forma significativa. Además, en atención a los mismos comentarios, en el inciso 3, se insertó como excepción al derecho del titular de recibir una explicación sobre la decisión tomada, *"siempre que no revelen con dicha explicación secretos comerciales"*.[78]

El artículo 36 plantea la forma en la que el titular puede ejercer sus derechos ARCO y de portabilidad e impone al responsable el deber de contar con mecanismos y procedimientos para esos efectos. En relación con el texto anterior, la Asociación Latinoamericana de Internet destacó que el hecho de que se incluyera la regulación por vía reglamentaria de los requerimientos, plazos y condiciones en que el titular puede ejercer sus derechos, provoca incertidumbre para ambas partes.[79] En ese sentido, se eliminó esa disposición del texto. Otra modificación relevante, fue que se eliminó la referencia a que las causales en las que el titular no puede ejercer sus derechos se enlistaban *"de manera enunciativa más no limitativa"*.

3.4. Capítulo IV Responsable y encargado del tratamiento

En el ***Capítulo IV Responsable y encargado del tratamiento*** se modifican:

- Obligaciones del responsable del tratamiento -artículo 37-
- Cesión de datos -artículo 39-
- Formalización de la prestación de servicios del encargado -artículo 41-

El artículo 37 regula expresamente los deberes del responsable del tratamiento, así como los riesgos que pueden producirse a la hora de adoptar medidas, en distintos supuestos. En el texto sustitutivo, se eliminó el inciso 1, que establecía la obligación del responsable de definir las medidas técnicas y organizativas que implementaría, y la obligación concreta de valorar si procedía una evaluación de impacto. En consecuencia, se incluyó un nuevo inciso 1, acompañado de puntos de las letras a-k. Indican lo siguiente:

> *"1. Los Responsables del tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente Ley, sus normas reglamentarias y otras que rijan su actividad:*
>
> *a. Implementar medidas apropiadas, útiles, oportunas, pertinentes y eficaces para garantizar y poder demostrar el adecuado cumplimiento de la presente Ley y sus*

[78] Ibíd.
[79] Ibíd.

normas reglamentarias, especialmente los derechos de los Titulares y la materialización de los principios del tratamiento de datos personales;

b. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de protección de datos, especialmente conocer, actualizar, rectificar, suprimir sus datos personales u oponerse al tratamiento de los mismos;

c. Cumplir debidamente con el deber de informar al Titular sobre la finalidad de la recolección y sus derechos;

d. Tratar los datos personales bajo condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

e. Implementar medidas para garantizar que los datos personales sean veraces, actualizados, completos, exactos y comprobables;

f. Actualizar los datos personales, rectificar la información cuando sea incorrecta y adoptar medidas necesarias para que la misma se mantenga actualizada;

g. Tramitar debidamente las solicitudes presentadas por el Titular, respondiéndolas de manera completa y oportunamente;

h. Realizar la notificación de violaciones de seguridad en los términos y plazos previstos en esta Ley.

i. Cumplir las instrucciones, órdenes o requerimientos que imparta la Agencia de Protección de Datos Personales.

j. Formalizar mediante la suscripción de un acuerdo, contrato o cualquier otro instrumento jurídico la prestación de servicios entre el Responsable y el Encargado, en entre corresponsables.

k. Verificar que los Encargados, o quienes éstos subcontraten, ofrecen garantías suficientes para realizar el tratamiento de datos personales conforme con los requisitos de la presente Ley y garantice la protección de los derechos del Titular. Dicha verificación debe realizarse con anterioridad a la contratación u realización de otro acto jurídico que lo vincule con el Encargado;

l. Exigir al Encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y debido tratamiento de la información del Titular;"

Sobre la redacción original del artículo 39, que regula la cesión de datos, la Asociación Latinoamericana de Internet señalo la necesidad de modificarla, por las siguientes razones:

"Se sugiere aclarar el término comunicación y cesión, ya que una comunicación de datos podría darse en una relación de responsable-encargado, en donde el consentimiento del titular del dato no es necesario o existen otros casos en los que otras bases legales deberían poder utilizarse. No se explica razonablemente porque

el consentimiento se convierte en la única base legal para las comunicaciones a terceros. Además, sería conveniente modificar el inciso 1 para que se haga referencia únicamente a las cesiones de datos y no a las comunicaciones en general, pues las mismas están sujetas a diversos casos."[80]

Por consiguiente, se eliminó la palabra *"comunicación"* a lo largo del texto. Por otro lado, se adicionó en el inciso 2, la obligación de quienes cedan datos, de *"facilitar al Titular de los datos personales cedidos la siguiente información, dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos:"*. Dicha información, es la siguiente:

"a) la identidad y los datos de contacto del Responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;

d) las categorías de datos personales de que se trate;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del Responsable de transferir datos personales a un destinatario en un tercer país.

3. Las disposiciones del apartado anterior no serán aplicables cuando y en la medida en que:

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. En tales casos, el Responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del Titular;

c) la obtención o la comunicación esté expresamente establecida en una ley, o;

d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional emanada en una norma de carácter legal."

[80] Ibíd.

El artículo 41 regula la "*formalización de la prestación de servicios del Encargado",* desarrollando que se dará por medio de la suscripción de un contrato de encargo, cuya formalización es deber del responsable. Al respecto, de acuerdo con las recomendaciones de la UCCAEP, se modificaron los incisos 3.d, 3.e, 3.f y 3.k. A los primeros dos, se les agregó una aclaratoria de que cuando el deber del encargado, en relación con las cláusulas del contrato, consista en informar al responsable, deberá hacerlo sin dilación alguna. Sobre el inciso 3.f, se incluyó que el encargado debe *"garantizar que su personal y cualquier persona autorizada por el Encargado para tratar datos personales del Responsable cuenten con obligaciones contractuales o derivadas de una obligación legal que les obliguen a respetar la confidencialidad de los datos personales tratados"*. Finalmente, se añadió al inciso 3.k que, además del deber del encargado de colaborar con el responsable en lo relativo al cumplimiento de la legislación, debe *"facilitar la información necesaria para demostrar el cumplimiento de las obligaciones en el presente artículo, sea en el marco de una auditoría realizada al Responsable, de un procedimiento de fiscalización por una autoridad competente o cuando dicha obligación derive del contrato de encargo*".[81]

3.5. Capítulo V Transferencias internacionales de datos personales

En el ***Capítulo V Transferencias internacionales de datos personales*** se modifican:

- Reglas generales para las transferencias internacionales de datos personales -artículo 45-

El artículo 45 versa sobre las reglas para llevar a cabo transferencias internacionales de datos personales, así como los supuestos en los que son procedentes. Por consiguiente, y de acuerdo con los comentarios de UCCAEP, se ajustó la estructura del artículo, incluyendo subtítulos en cada inciso que resumen su contenido.[82] También, se incluyó en el inciso c la aclaración de que cuando el país destinatario acredite condiciones mínimas y suficientes para garantizar un nivel de protección de datos personales adecuado, estas *"no podrán ser menores que las reconocidas en la presente Ley"*. Además, incorpora en el inciso d, para el caso de transferencias fundamentadas en garantías adecuadas del exportador, que el exportador debe acreditar el cumplimiento de derechos exigibles y el acceso a acciones legales efectivas.

Por último, se adicionó un inciso 4 que indica *"cuando el Titular de forma libre, voluntaria y por su propia iniciativa, transfiera sus datos a un Responsable situado en una jurisdicción diferente a la del Titular"*.

[81] **UCCAEP**. Oficio N° DE-086-22. Op. cit.
[82] Ibíd.

3.6. Capítulo VI Medidas proactivas en el tratamiento de datos personales

En el ***Capítulo VI Medidas proactivas en el tratamiento de datos personales*** se modifican:

- Privacidad por diseño y privacidad por defecto -artículo 47-
- Oficial de protección de datos personales -artículo 48-
- Intervención del oficial de protección de datos en caso de reclamación ante la Agencia de Protección de Datos -artículo 49-
- Mecanismos de autorregulación -artículo 50-
- Evaluación de impacto a la protección de datos personales -artículo 51-

El artículo 47 regula el deber del responsable de poner en práctica medidas preventivas, programas, servicios o sistemas que permitan aplicar o se ajusten a los principios, derechos y demás obligaciones en la Ley. En ese sentido, se incluyó en el inciso 1 que *"teniendo en cuenta el estado de la técnica, el costo de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entrañe el tratamiento de los datos para los derechos y libertades de los Titulares"*, el responsable aplicará esas medidas desde el diseño. Dicha sugerencia proviene de los comentarios de UCCAEP.[83]

El artículo 48 establece los supuestos en los que el responsable debe nombrar un oficial de protección de datos personales, al igual que el detalle de sus funciones y desarrollo de sus labores. Incorporando algunos de los comentarios de UCCAEP, se realizaron las siguientes modificaciones:

- Se incluyó a la Asamblea Legislativa como una de las entidades en las que el responsable debe nombrar un oficial.
- Se aclaró que dicho nombramiento en el caso de las entidades bancarias y financieras, sujetas a la regulación de SUGEF, será "*de acuerdo a las regulaciones sectoriales que se dicten"*.
- Se eliminó del inciso 3 el deber del responsable de informar en un plazo de 10 días naturales a la Agencia de Protección de Datos las designaciones, nombramientos y ceses de los oficiales. En cambio, se dispuso que *"los Responsables que designen un oficial de protección de datos, sea por mandato legal o de forma voluntaria, deberán poner a disposición del Titular sus datos de contacto en cualquier aviso o política de privacidad de la que disponga"*.
- En el inciso 4 se aclaró que, cuando el oficial desempeñe otras funciones, estas no deberán dar lugar a conflicto de intereses.
- Se eliminó en el inciso 4 que la Agencia tuviera que contar con una lista actualizada de los oficiales, accesible por medios electrónicos.

[83] Ibíd.

- Se agregó un inciso 10 que establece el secreto profesional y deber de confidencialidad que cubre al oficial.[84]

El artículo 49 regula la *"intervención del oficial de protección de datos en caso de reclamación ante la Agencia de Protección de Datos".* Ambos plazos estipulados en los incisos 1 y 2, de dos meses y un mes respectivamente, se cambiaron a cinco días hábiles. El primero hace referencia al plazo del oficial para comunicar al afectado la decisión que se hubiera adoptado, contados desde la recepción de la reclamación. El segundo se refiere al plazo que tiene el oficial para responder, cuando la Agencia le remita la reclamación.

El artículo 50 establece que el responsable y encargado pueden adherirse a mecanismos de autorregulación vinculantes para promover la aplicación correcta de la Ley y procedimientos de resolución de conflictos entre el responsable y el titular. Previamente, el texto original incluía esta facultad únicamente para el responsable, pero fue modificado tomando como base los comentarios de UCCAEP. Asimismo, en el inciso 3 se adicionó, que las reglas que defina la Agencia en relación con el reconocimiento de los mecanismos de autorregulación son los *"elaborados por las asociaciones y otras organizaciones, nacionales o internacionales, de alcance general o sectoriales"*.[85]

El artículo 51 regula la *"evaluación de impacto a la protección de datos personales"*, la cual se llevará a cabo por parte del responsable, en casos de tratamientos que probablemente entrañen un alto riesgo de afectación a la protección de datos personales. Con el texto sustitutivo y de acuerdo con los comentarios de UCCAEP, se incluyó en el inciso 3.b, como supuesto dentro de los cuales debe realizarse la evaluación, el tratamiento de datos *"relativos a condenas e infracciones penales previstos en esta Ley"*.[86] Además, se eliminó el antiguo inciso 6 y se sustituyó por el contenido del inciso 7, en el cual se cambió la *"autoridad de control"* por la *"Agencia de Protección de Datos"*.

3.7. Capítulo VII Disposiciones aplicables a tratamientos concretos

En el ***Capítulo VII Disposiciones aplicables a tratamientos concretos*** se modifican:

- Tratamiento con fines de videovigilancia -artículo 52-
- Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo -artículo 53-
- Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral -artículo 54-

[84] Ibíd.
[85] Ibíd.
[86] Ibíd.

- Datos relativos al comportamiento crediticio del sector financiero y no financiero -artículo 55-
- Tratamiento de datos en la investigación en salud -artículo 56-

El artículo 52 establece el *"tratamiento con fines de videovigilancia"*. En cuanto al inciso 8, la Asociación Latinoamericana de Internet, desarrolló: *"Asimismo, el numeral 8 señala que se prohíbe, sin excepción, el uso de sistemas de identificación biométrica en tiempo real en espacios públicos para cualquier finalidad, especialmente policiales o de investigación criminal. En todo caso, se debe considerar este adelanto tecnológico y la aplicabilidad en el beneficio en la agilización de procesos investigativos, especialmente en delitos relacionados con el salvaguardo de la integridad física de las personas, se recomienda analizar la posibilidad de desarrollar y regular los casos en que podría ser aplicable"*.[87]

En consecuencia, se ajustó el inciso 8, eliminando dicha disposición restrictiva. En cambio, se incluyó que *"se prohíbe el uso de sistemas de identificación biométrica en tiempo real en espacios públicos a través de cámaras o sistemas de videovigilancia que tengan por finalidad la identificación indiscriminada o masiva de las personas"*.

El artículo 53 regula el *"derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo"*, indicando en qué supuestos el empleador puede tratar imágenes obtenidas a través de esos sistemas, y en cuáles su instalación no es permitida. En el texto sustitutivo, se cambió la redacción *"trabajadores o los empleados públicos"*, por *"trabajadores del sector público o privado"*, lo cual define con mayor claridad el ámbito de aplicación de esta norma. Asimismo, de acuerdo con los comentarios de UCCAEP, se incluyeron las salas de lactancia como uno de los supuestos en los que no se admite la instalación de estos sistemas.[88]

Al artículo 54, sobre el *"derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral"*, se le realizó el mismo cambio que al artículo pasado, en cuanto se cambió *"trabajadores o empleados públicos"*, por *"trabajadores del sector público o privado"*. Lo anterior, evita que haya un margen de interpretación sobre el ámbito de aplicación de la norma.

El artículo 55, versa sobre los *"datos relativos al comportamiento crediticio del sector financiero y no financiero"*. Previamente estaba titulado *"sistemas y proveedores de información crediticia"*. Su redacción en el texto inicial fue objeto de diversas críticas, por lo que es uno de los pocos artículos que fueron modificados en su totalidad. La redacción anterior, se enfocaba en que los datos relativos al comportamiento crediticio se regían por las normas que dicte SUGEF, permitiendo a las entidades de esta naturaleza acceder a ellos, sin comprometer los derechos y garantías en la

[87] **Asociación Latinoamericana de Internet**. Oficio de 29 de julio de 2022. Op. cit.
[88] **UCCAEP**. Oficio N° DE-086-22. Op. cit.

Ley. Indudablemente, era necesaria una redacción más amplia que brinde una protección más extensa y clara al derecho de protección de datos personales. En consecuencia, se incluyó la siguiente redacción en el texto sustitutivo:

> *"1. Los datos personales relativos al comportamiento crediticio tratados por el Centro de Información Crediticia (CIC) se regirán por las normas dictadas por la Superintendencia General de Entidades Financieras, de modo que el acceso a dichos datos permita a las entidades financieras y de crédito valorar el nivel de riesgo de crédito de sus clientes, respetando las garantías, principios y derechos concedidos en esta Ley. Esto sin perjuicio del tratamiento que sobre datos crediticios puedan hacer otros Responsables del sector no financiero, en los términos indicados en el presente artículo.*
>
> *2. Queda expresamente autorizado el tratamiento de datos personales destinado a informar sobre la solvencia patrimonial o crediticia, incluyendo aquellos datos relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial y/o crediticio que permitan evaluar los riesgos de contratación, la conducta comercial y/o la capacidad de pago del Titular. Lo anterior, en los casos en que dichos datos personales sean obtenidos de fuentes de acceso público, y/o procedentes de informaciones facilitadas por el acreedor con base en su interés legítimo prevalente, o en las circunstancias previstas en la presente Ley.*
>
> *3. Cuando se realice una cesión de datos personales para el fin indicado en el párrafo anterior, el acreedor, en calidad de Responsable de los datos, deberá mantener un registro del Titular de los datos cedidos, que podrá ser requerido por la Agencia de Protección de Datos en el marco de una investigación o procedimiento sancionatorio.*
>
> *4. Los datos personales relativos al comportamiento crediticio que sean significativos para evaluar la solvencia económica o financiera podrán tratarse hasta por cuatro años, desde el vencimiento del plazo original de la operación de crédito. El plazo se reduce a dos años cuando el deudor cancele o extinga la obligación, plazo a contar a partir de la fecha en que lo hace, debiendo constar esta información en el informe crediticio.*
>
> *5. Cuando se cancele una obligación incumplida registrada en una base de datos de solvencia, o exista una orden judicial o administrativa que así lo ordene, el acreedor de la obligación deberá en un plazo máximo de cinco días hábiles de acontecido el hecho, comunicarlo al Responsable de la base de datos de solvencia. Una vez recibida la comunicación por el Responsable de la base de datos de solvencia, éste dispondrá de un plazo máximo de tres días hábiles para proceder a la actualización del dato, asentando su nueva situación en el informe crediticio.*
>
> *6. Los Responsables de las bases de datos sobre solvencia o insolvencia patrimonial deberán en todo momento velar por realizar valoraciones objetivas de la información, sin que esta pueda prestarse para ningún tipo de discriminación. Dichas condiciones serán supervisadas por la Agencia de Protección de Datos."*

El artículo 56 define los criterios por los cuales se rige el tratamiento de datos en la investigación de salud. Con el texto sustitutivo, se eliminaron los incisos b y e, de manera que se protegen los derechos de los titulares de una manera más rigurosa. Al respecto, el Colegio de Profesionales en Informática y Computación, consideró que esos incisos no eran aceptables. Los motivos se exponen a continuación:

El inciso b contenía una autorización excesiva, ya que, faculta los estudios científicos sin consentimiento de los afectados, con base en "situaciones de excepcional relevancia y gravedad para la salud pública". Deja a interpretación del funcionario público la aplicación de la norma. Sobre el inciso e, es de alto riesgo lo dispuesto en el punto iii), que deja abierta la posibilidad de excepcionar los derechos de los titulares, cuando la investigación tenga "otros objetivos importantes de interés público general". Se puede prestar para que cualquier interés particular calce bajo esta definición. En ambos casos, se promovía que se excepcionaran los derechos o garantías del titular para este tipo de tratamiento, por lo que su eliminación era oportuna.

Finalmente, de acuerdo con los comentarios de la misma entidad, para mayor claridad en el inciso g, se hace referencia a que el comité ético, es aquel previsto en la Ley 9234 Ley Reguladora de Investigación Biomédica.[89]

3.8. Capítulo VIII Agencia de Protección de Datos

En el ***Capítulo VIII Agencia de Protección de Datos*** se modifican:

- Disposiciones generales - artículo 61-
- Régimen económico presupuestario -artículo 62-
- Funciones -artículo 63-
- Potestades -artículo 64-
- Dirección de la Agencia de Protección de Datos -artículo 65-

El artículo 61 menciona las disposiciones generales relacionadas con la Agencia de Protección de Datos y su estructura. El antiguo inciso 1, pasó a ser el 2, y en su lugar, se incluyó que la Agencia *"es la autoridad nacional de control encargada de la regulación y protección de los datos personales de los habitantes de la República"*. Además, en el inciso 3, se adiciona una mención al MICITT, para referirse a que ante este no se pueden impugnar las resoluciones de la Agencia, ni podrá este avocar sus competencias. Dichas modificaciones recogen parte de los cambios propuestos por UCCAEP.[90]

[89] **Colegio de Profesionales en Informática y Computación.** Oficio AL-014-JD-CPIC-2022 de 11 de agosto de 2022, suscrito por Hilda Isabel Delgado Montes, asesora legal.
[90] **UCCAEP**. Oficio N° DE-086-22. Op. cit.

El artículo 62 regula el régimen económico presupuestario de la Agencia, lo cual abarca los componentes del presupuesto y las entidades encargadas de su fiscalización y auditoría. Al inciso a, se le incluyó al final del texto que "*la denominación salario base utilizada en esta Ley debe entenderse como la contenida en el artículo 2 de la Ley No. 7337 de 5 de mayo de 1993"*. Adicionalmente, se aclaró que, sean nacionales o internacionales, no se pueden aceptar donaciones de empresas que se dediquen a la comercialización de datos. Lo anterior, de forma congruente con los comentarios enviados por UCCAEP.[91]

El artículo 63 enlista las funciones de la Agencia de Protección de Datos. Con el nuevo texto, se modifican algunas y se adicionan 2. En cuanto al inciso c, se cambia para que la función consista en *"emitir criterio"*, no *"asesorar"*. El inciso f establecía como función resolver las reclamaciones de los titulares u organismos y llevar a cabo una investigación al respecto. Actualmente, se cambió su contenido por *"Investigar, resolver y sancionar, de oficio o a ante denuncia, cualquier infracción atribuida a una persona física o jurídica, del sector público o privado, e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable"*.

Asimismo, siguiendo la línea de los comentarios de CAMTIC[92] y UCCAEP[93], se incluyeron dos funciones al final del artículo. La primera, se refiere a *"emitir dictámenes no vinculantes a solicitud de interesados, con el objeto de brindar criterios generales sobre el cumplimiento de las obligaciones y ejercicio de derechos contemplados en esta Ley y los reglamentos que la desarrollen"*. El segundo, adiciona "*Gestionar y administrar sus recursos y presupuesto, para lo que podrá aprobar los contratos de obras y servicios, de acuerdo con el ordenamiento jurídico vigente"*.

El artículo 64 establece las potestades de la Agencia, que podrá ejercer para llevar a cabo sus funciones de investigación. Se incluyó una potestad, relativa a que la Agencia pueda dictar medidas cautelares en sede administrativa para garantizar el derecho de protección de datos. Esto, relacionado con los comentarios de UCCAEP.[94] En el último párrafo se incluyó que, en el caso de auditorías preventivas, puede actuar sin comprobación previa de indicios.

El artículo 65 regula la *"dirección de la Agencia de Protección de Datos".* En ese sentido, menciona cómo será el nombramiento de la Dirección y el Adjunto, la duración de este y las formas en las que podrá cesar. Fue modificado en los siguientes términos:

- Se adicionaron las causales de impedimento para ser nombrado como Director y/o Adjunto, las cuales se refieren a que no podrán ser nombrados

[91] Ibíd.
[92] **Cámara de Tecnologías de Información y Comunicación.** Oficio de 8 de agosto de 2022. Op. cit.
[93] **UCCAEP**. Oficio N° DE-086-22. Op. cit.
[94] Ibíd.

en estos puestos, quienes sean parientes "hasta tercer grado de consanguinidad o afinidad del presidente de la República, los vicepresidentes, los ministros y viceministros o con vínculo civil por afinidad hasta el mismo grado".

- En el inciso 5.b se aclara que cuando el Director o Adjunto, cesen de su cargo por incapacidad física sobrevenida para el ejercicio de su función, esta deberá ser por un plazo superior a 6 meses.
- En el inciso 5.c se adiciona que cuando el Director o Adjunto, cesen de su cargo por condena firme por delito doloso, esto podrá ser incluso en grado de tentativa.

3.9. Capítulo X Régimen sancionador

En el ***Capítulo X Régimen sancionador*** se modifican:

- Sujetos responsables -artículo 72-
- Infracciones -artículo 73-
- Infracciones consideradas muy graves - artículo 74-
- Interrupción de la prescripción de la infracción - artículo 77-
- Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento -artículo 79-

El artículo 72 regula quiénes están sujetos al régimen sancionador establecido en este capítulo. En el texto original, se mencionaban el responsable y el encargado. Sin embargo, con el texto sustitutivo se hace una aclaratoria en cuanto al segundo, indicando que este estará sujeto al régimen sancionador *"en el cuanto su responsabilidad no se derive de instrucciones giradas por el Responsable, o del incumplimiento de este a las disposiciones de esta Ley o su reglamento"*. De esta manera, se sigue lo recomendado por CAMTIC, quien expuso en sus comentarios que no tiene sentido sancionar al encargado por las acciones que este realice amparado en las instrucciones del responsable.[95]

El artículo 73 fija los montos de las sanciones por actos y conductas contrarias a la Ley. Su redacción anterior, generó preocupación de entidades, tales como el Colegio de Optometristas y el Colegio de Farmacéuticos, quienes destacaron que los montos eran elevados. Especialmente, fue inquietante la magnitud del volumen de ventas como criterio para determinar la sanción en caso de personas jurídicas, pues tratándose, por ejemplo, de los colegios profesionales, tienen una realidad económica que dista por mucho de empresas de ventas.

[95] **Cámara de Tecnologías de Información y Comunicación.** Oficio de 8 de agosto de 2022. Op. cit.

Por consiguiente, se ajustaron los montos de las multas en el texto sustitutivo, disminuyéndolas. En adelante, son las siguientes:

> "a. Para las faltas leves, una multa hasta de entre cinco y diez salarios base.
>
> b. Para las faltas graves, una multa de diez a cincuenta salarios base.
>
> c. Para las faltas gravísimas, una multa de cincuenta hasta cien salarios base, y, en caso de personas físicas o jurídicas que cometieran la infracción en el ejercicio de una actividad lucrativa, el monto superior entre cien salarios base y hasta un dos por ciento del volumen de ventas que hubiere reportado durante el periodo fiscal inmediato anterior a la comisión de la infracción."

De esta manera, se implementa en cambio, el criterio en las faltas gravísimas, de *"personas físicas o jurídicas que cometieran la infracción en el ejercicio de una actividad lucrativa"*, de la mano de una determinación del monto inferior a la expuesta en el texto original. Además, el volumen de ventas se redujo de 4% a 2%.

El artículo 74 define los supuestos en los que se comete una infracción clasificada como muy grave. En comparación con el texto original, se eliminaron en los incisos k y l, la referencia a los artículos 45 y 64 de la ley, respectivamente. Lo anterior, en concordancia con los comentarios de UCCAEP.[96] Asimismo, se eliminó el inciso n, que abarcaba la no facilitación del acceso del personal de la autoridad de protección de datos, a los datos, información o equipos cuando sean requeridos por esta, para el ejercicio de sus poderes de investigación.

El artículo 77 regula la *"interrupción de la prescripción de la infracción"*. Su contenido versa sobre el plazo durante el cual, si el expediente sancionador está paralizado, se interrumpe el plazo de prescripción de la infracción. Dicho plazo, previamente era de doce meses, pero se cambió a seis.

El artículo 79 menciona el *"régimen aplicable a determinadas categorías de responsables o encargados del tratamiento"*. Se eliminó la redacción original del inciso 3, que establecía la facultad de la Agencia de proponer la iniciación de actuaciones disciplinarias contra los funcionarios implicados, cuando existan indicios suficientes para ello. En cambio, se introdujo que *"los funcionarios públicos que incurran en algunas de las infracciones establecidas en los artículos 74, 75 y 76 y se haya demostrado la culpa o dolo en su accionar u omisión, serán sancionados con la suspensión de su cargo por hasta noventa días, sin goce de salario, sin perjuicio de otras sanciones previstas en el régimen disciplinario aplicable al funcionario"*.

[96] **UCCAEP**. Oficio N° DE-086-22. Óp.. cit.

3.9. Capítulo XI Derecho de indemnización

En el ***Capítulo XI Derecho de indemnización*** se modifican:

- Reparación del daño -artículo 81-

El artículo 81 regula la reparación del daño al titular que sufra daños y perjuicios por violación de su derecho a la protección de datos personales. El inciso 2 desarrolla que el ejercicio de las acciones judiciales prescribe en tres años a partir de la existencia del daño. Previamente, este plazo era de un año.

3.7. Disposiciones de transitorias

Se modificó la redacción del Transitorio II, lo cual resultó en el desplazamiento de su anterior texto, al Transitorio III. Su contenido se refiere a que *"la PRODHAB continuará desarrollando sus funciones hasta que estas puedan ser asumidas de forma coordinada por la Agencia de Protección de Datos Personales creada en esta Ley, una vez que al menos su dirección haya sido designada y cuente con capacidad operativa para funcionar, lo que determinará la dirección mediante resolución que deberá ser publicada en el Diario La Gaceta y comunicada al público en general. Dicha transición deberá completarse en un periodo máximo de un año a partir de la entrada en vigor de esta Ley. Todos los procedimientos administrativos que estuvieran en trámite ante PRODHAB serán trasladados a la Agencia de Protección de Datos Personales a partir de que esta entre en funcionamiento, y serán continuados en el estado que estuvieren y hasta su efectiva finalización"*.

3.8. Conclusiones

Como se evidenció a lo largo del repaso de los artículos del texto sustitutivo, esta norma es fundamental para la regulación del derecho de protección de datos de las personas en Costa Rica, que garantiza congruencia con los estándares internacionales que rigen la materia. Es claro que de forma efectiva amplía la esfera de protección de las personas, sus derechos e intereses, respecto del manejo de sus datos, especialmente en una sociedad cada vez más digitalizada y automatizada. Además, contrapuesto a esto, se encuentran una amplia gama de obligaciones de los responsables y encargados, que facilitan dicha protección.

En ese sentido, la norma es acorde con los principios y parámetros contenidos en el Reglamento General de Protección de Datos Personales de la Unión Europea[97] y los Estándares de Protección de Datos Personales de la Red Iberoamericana de

[97] Reglamento General de Protección de Datos Personales (RGPDP) número 2016/679, el cual entró en vigor en la Unión Europea el 25 de mayo de 2018.

Protección de Datos Personales[98]. Inclusive, en algunas instancias, sus disposiciones son claras adaptaciones de estos instrumentos.

Sobre todo, se considera compatible en aspectos, tales como:

- Definiciones. Al respecto, llama la atención la clasificación de las categorías de datos personales.
- Principios relativos al tratamiento.
- Derechos de los titulares de forma general, pero específicamente los derechos ARCO y de portabilidad.
- Los mecanismos para garantizar la seguridad de los datos.
- La regulación aplicable a los responsables y encargados del tratamiento.

En consideración con las reformas planteadas, es conveniente impulsar la reorientación de la asignación de recursos humanos, financieros, tecnológicos y otros, para una adecuada gestión, no solo de la Agencia de Protección de Datos, sino de los datos objeto de tratamiento en la Administración Pública.

Asimismo, son imprescindibles las opiniones y valoraciones de los diferentes sectores, de manera que estos puedan brindar sus perspectivas y recomendaciones; que, a su vez, sean analizadas por el órgano legislativo competente para así lograr el objetivo que se desea alcanzar con la presente iniciativa.

IV.- ASPECTOS DE TÉCNICA LEGISLATIVA

4.1. Redacción del proyecto de ley

La redacción de la propuesta de ley debe guardar un estilo sumamente parco, desprovisto de palabras innecesarias, donde se establezca una absoluta precisión y la mayor claridad posible. El texto legal debe tener carácter rigurosamente preceptivo; deben omitirse disposiciones que sólo constituyen motivación del texto, enuncian intenciones o son simples recomendaciones.[99] De allí, que el presente texto es acorde con una adecuada técnica legislativa, que cumple con todos los criterios anteriormente mencionados.

Su redacción presenta coherencia y uniformidad a la interpretación que se haga de él. Incluso, se evidencia claridad en cada disposición, que permite una idónea comprensión de los alcances de lo que se pretende regular.

[98] Estándares de Protección de Datos Personales para los Estados Iberoamericanos, del 20 de junio de 2017. Los cuales pueden ser consultado en la siguiente dirección web: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf
[99] Pérez Bourbon, Héctor. Manual de Técnica Legislativa. - 1a ed. - Buenos Aires: Konrad Adenauer Stiftung, 2007, pág. 102.

4.2. Estructura de la ley

Es oportuno considerar los siguientes aspectos sobre la estructura de la ley:

- El objeto de la **estructura** es hacer fácilmente accesible el conocimiento del contenido de la ley y de las normas en ella contenidas.[100]
- La **redacción**, tiende a asegurar que el texto de la ley será interpretado del mismo modo por todos aquéllos que deban utilizarlo.
- La **dinámica legislativa** asegura la correcta inserción en el orden jurídico de las normas contenidas en la ley.[101]
- La **lógica** de los sistemas normativos, procuran evitar las lagunas, contradicciones y redundancias en el orden jurídico.[102]

La finalidad de las reglas sobre estructura consiste en facilitar el acceso del conocimiento del objeto y del alcance de la ley y de las normas en ella contenidas.[103]

El cuerpo del texto sustitutivo del presente proyecto de ley está compuesto por 83 artículos y seis disposiciones transitorias. El cual se encuentra estructurado de la siguiente forma:

---

[100] *"Una buena estructura permite construir un índice de la ley, mediante el cual el usuario, sea profesional o no, puede encontrar rápidamente la norma o el grupo de normas que necesita."* Ibid, pág. 34.

[101] *"La sanción de una nueva ley implicará, necesariamente, una adecuación en el orden jurídico vigente a ese momento: deberán modificarse o derogarse otras normas.*
Un correcto manejo de las reglas referidas a la dinámica legislativa permite una mayor certeza en cuanto a cuáles son las normas que mantienen su vigencia y cuáles las que la han perdido." Ibid, pág. 34.

[102] *"Estos cuatro pilares de la técnica legislativa (estructura, redacción, dinámica y lógica), no obstante, si bien pueden analizarse y estudiarse por separado, confluyen todos ellos al momento de tener que redactar un texto normativo.*
Ello hace que no sea sencillo, en algunos casos, encontrar la ubicación correcta de las reglas que se plantean. En efecto, podrá apreciarse que algunas de ellas vinculadas, por ejemplo, a redacción, tienen decisiva influencia en la estructura o en la dinámica.
Por tal motivo, se ha tratado de señalar, en cada caso, qué otras reglas deben consultarse."
(Estas aclaraciones han sido extraídas, de modo prácticamente textual, de Reglas Prácticas de Técnica Legislativa, de Héctor Pérez Bourbon y otros, pp. 21 y 22.) Ibid, págs. 34 y 35.

[103] *"5. Como consecuencia de lo anterior, las reglas sobre estructura que se indican en este Manual deben ser dejadas a un lado si su cumplimiento conspira contra la clara inteligencia del contenido de la ley.*
6. Al desarrollar la estructura de la ley, debe tenerse muy presente quién será su principal usuario. Si bien todas las leyes deben ser claras en su comprensión, debe ponerse especial cuidado en ello cuando están dirigidas al público en general. En tales casos puede ser necesario que deban reiterarse normas contenidas en otras leyes u otros textos normativos, aun a riesgo de caer en redundancias, pero facilitando el acceso del lego a la totalidad de la normativa sobre la materia en cuestión (ver reglas 207 y 208).
7. En las leyes cuyos principales usuarios serán los profesionales o especialistas, del derecho o de otras disciplinas, esas reiteraciones deben evitarse; asimismo, en estos casos es admisible un cierto grado de dificultad en su comprensión, proveniente de la utilización de términos técnicos (ver reglas 207 y 208).
Un requisito ineludible para lograr el cumplimiento de las leyes es que sean comprendidas por la población. En este aspecto, una buena estructura facilita enormemente la comprensión de la ley.
Sin embargo, las reglas a aplicar en este tema deben ser preponderantemente prácticas y dirigidas al objetivo principal: la fácil accesibilidad al contenido y a la comprensión de la ley. Por ese motivo se han dejado a un lado conceptos que, aunque teóricamente puedan considerarse mejores desde el punto de vista técnico, irían en contra de ese objetivo.
Un ejemplo es el del ámbito temporal de aplicación de la ley. Desde una perspectiva teórica, lo razonable sería que se colocara junto con el ámbito material, el personal y el territorial; no obstante, en prácticamente toda la legislación argentina, el artículo sobre entrada en vigor de la ley se coloca al final. Vano sería entonces pretender una ubicación teóricamente más razonable de dicho artículo si por esa causa quedara ubicado donde nadie lo encontrara sino después de una búsqueda exhaustiva.
Por ello también es que se señala la necesidad de tener presente, en todo momento, quién será el principal usuario. Una ley que regule, por ejemplo, el instituto de Iniciativa Popular, que será utilizada por el común de la ciudadanía, debe ser más fácil de comprender que un código procesal cuyo usuario principal será, seguramente, un profesional del derecho." Ibid, págs. 35 y 36.

Capítulo I Disposiciones generales

- *Artículos 1 a 12*

Capítulo II Principios de protección de datos personales

- *Artículos 13 a 26*

Capítulo III Derechos del titular

- *Artículos 27 a 36*

Capítulo IV Responsable y Encargado del tratamiento

- *Artículos 37 a 44*

Capítulo V Transferencias internacionales de datos personales

- *Artículo 45*

Capítulo VI Medidas proactivas en el tratamiento de datos personales

- *Artículos 46 a 51*

Capítulo VII Disposiciones aplicables a tratamientos concretos

- *Artículos 52 a 60*

Capítulo VIII Agencia de Protección de Datos

- *Artículos 61 a 65*

Capítulo IX Procedimiento en caso de posible vulneración a la normativa de protección de datos

- *Artículos 66 a 71*

Capítulo X Régimen sancionador

- *Artículos 72 a 80*

Capítulo XI Derecho de indemnización

- *Artículos 81 a 83*

Transitorios (I, II, III, IV, V y VI)

Como puede observarse, la estructura de la ley se desarrolla en once capítulos, los cuales están numerados de forma adecuada y con denominaciones que son atinentes al contenido desarrollado por cada uno. Dicho de otro modo, hay congruencia entre el fondo de cada artículo y el tema objeto de los capítulos.

Por otra parte, la ausencia de secciones da mayor claridad de lo que se pretende regular en cada capítulo, al igual que un acceso a la información simplificado.

4.3. Título del proyecto de ley

El título de una ley tiene las siguientes características:

> *"El texto debe ser introducido por un título general que precise el objeto de la ley.*
> *El título debe ser breve, concreto y reflejar objetivamente el contenido de la ley.*
> *Debe evitarse dar a una ley un título ya asignado a otra ley anterior que continúa en vigor.*
> *El título de la ley es el que el cuerpo legislativo aprueba al momento de su sanción; los títulos puestos por publicaciones, oficiales o no, no reemplazan el título oficial de la ley.*

El primer acercamiento que tiene el lector al texto de la ley es, precisamente, el título de la ley. Por ese motivo es importante que la ley tenga un título que le dé suficiente información acerca de qué trata.
Por otra parte, es necesario señalar que muchas veces al publicarse el texto legal se le adiciona un título o nombre; ese nombre o título sólo será el nombre o título de la ley si fue así aprobado por el cuerpo legislativo."[104]

El título en toda ley o proyecto de ley cumple la función de definir o especificar el contenido o finalidad de ésta. Resulta claro que el título del presente proyecto ilustra de forma concreta su contenido, de acuerdo con una correcta técnica legislativa, evitando excederse en palabras innecesarias.

V.- ASPECTOS DE PROCEDIMIENTO

5.1. Votación

De conformidad con lo establecido en el artículo 24 de la Constitución Política, la presente iniciativa de ley requiere para su aprobación de **dos terceras partes del total de los miembros de la Asamblea Legislativa**.

Asimismo, teniendo presente la opinión emitida por la Corte Suprema de Justicia, donde señaló que la norma se refiere a la organización o funcionamiento del Poder Judicial[105], conforme el artículo 167 de la Constitución Política, se requerirá para apartarse del criterio de la Corte Suprema de Justicia el voto de las **dos terceras partes del total de los miembros de la Asamblea**.

5.2. Delegación

La presente iniciativa **no es delegable a una Comisión con Potestad Legislativa Plena**, puesto que la propuesta requiere para su aprobación de **dos terceras partes del total de los miembros de la Asamblea**.

5.3. Consultas

- Obligatorias:
  - Corte Suprema de Justicia.
- Facultativas:
  - Agencia Protección de datos de los Habitantes.
  - Asociación Latinoamericana de internet.

[104] Ibid, pág. 36.
[105] *"De esta manera, para los efectos de lo establecido en los numerales 167 de la Constitución Política y 59 inciso 1) de la Ley Orgánica del Poder Judicial, debo indicar que el proyecto de ley denominado: Ley de Protección de Datos Personales,* ***sí incide directamente en el funcionamiento y organización del Poder Judicial."*** **Corte Suprema de Justicia.** Oficio N° SP-155-2022 op. cit.

- Caja Costarricense de Seguro Social.
- Cámara de Industrias de Costa Rica.
- Cámara de Tecnologías de Información y Comunicación.
- Colegio de Ingenieros Químicos de Costa Rica.
- Colegio de Profesionales en Informática y Computación.
- Colegio de Profesionales en Sociología de Costa Rica.
- Colegio de Terapeutas.
- Comisión Nacional del Consumidor.
- Contraloría General de la República.
- Defensoría de los Habitantes.
- Fundación Privacidad y Datos PRIDAT.
- Ministerio de Ciencia y Tecnología.
- Ministerio de Economía, Industria y Comercio.
- Ministerio de Justicia.
- Procuraduría General de la República.
- Sala Tercera de la Corte Suprema de Justicia.
- Superintendencia de Telecomunicaciones.
- Tribunal Supremo de Elecciones.
- UCCAEP.

No se omite manifestar que en la sesión ordinaria N°16 de 10 de noviembre de 2022, de la Comisión Permanente Especial de Ciencia, Tecnología y Educación, se aprobó moción de consulta al texto sustitutivo.

VI.- FUENTES

6.1. Constitucionales

- **Constitución Política de la República de Costa Rica,** del 19 de noviembre de 1949.

- Acuerdo N°399 de 29 de noviembre de 1961. **Reglamento de la Asamblea Legislativa.**

6.2. Leyes y Reglamentos

- Ley N°6227. **Ley General de la Administración Pública**, de 2 mayo de 1978.

- Ley N°8968, **Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales** del 5 de setiembre de 2011.

6.3. Pronunciamientos administrativos

6.4. Otras

- **Reglamento General de Protección de Datos** (UE) número 2016/679, del 27 de abril de 2016.
- **Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de España**, número 3/2018, del 5 de diciembre de 2018.
- **Estándares de Protección de Datos Personales para los Estados Iberoamericanos**, del 20 de junio de 2017.

VII.- ANEXOS

CUADRO COMPARATIVO ENTRE EL TEXTO BASE DEL PROYECTO DE LEY 23097 Y EL TEXTO SUSTITUTIVO aprobado en la Comisión Permanente Especial de Ciencia, Tecnología y Educación, en la sesión ordinaria N°16 del 10 de noviembre de 2022.

Para efectos de determinar la conexidad de la propuesta de texto sustitutivo, se detalla una tabla comparativa entre el texto original y el texto sustitutivo; donde en letra tachada se precisa lo que se elimina y en letra negrita lo que se modifica, para efectos de determinar con claridad las enmiendas realizadas.

LEY DE PROTECCIÓN DE DATOS PERSONALES	
TEXTO INICIAL	**TEXTO SUSTITUTIVO**[106]
CAPÍTULO I DISPOSICIONES GENERALES	CAPÍTULO I DISPOSICIONES GENERALES
ARTÍCULO 1- Objeto 1.La presente Ley tiene por objeto: a. Establecer un conjunto de principios y derechos de protección de datos personales con la finalidad de garantizar un debido tratamiento de los datos personales de los habitantes. b. Elevar el nivel de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales, el cual responda a las necesidades y exigencias internacionales que demanda el derecho a la protección de datos personales en una sociedad en la cual las tecnologías de la información y del conocimiento cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana. c. Garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física mediante el establecimiento de reglas comunes que aseguren el debido tratamiento de sus datos personales. c. Facilitar el flujo internacional de los datos personales, con la finalidad de coadyuvar al crecimiento social y económico ~~de la región.~~	ARTÍCULO 1- Objeto 1. La presente Ley tiene por objeto: a. Establecer un conjunto de principios y derechos de protección de datos personales con la finalidad de garantizar un debido tratamiento de los datos personales de los habitantes**, independientemente de su nacionalidad.** b. Elevar el nivel de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales, el cual responda a las necesidades y exigencias internacionales que demanda el derecho a la protección de datos personales en una sociedad en la cual las tecnologías de la información y del conocimiento cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana. c. Garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física mediante el establecimiento de reglas comunes que aseguren el debido tratamiento de sus datos personales. d. Facilitar el flujo internacional de los datos personales, con la finalidad de coadyuvar al crecimiento social y económico **del país.**

[106] Comisión Permanente Especial de Ciencia, Tecnología y Educación, en la sesión ordinaria N°16 del 10 de noviembre de 2022.

e. Impulsar el desarrollo de mecanismos para la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, autoridades de control no pertenecientes a la región y autoridades y entidades internacionales en la materia.	e. Impulsar el desarrollo de mecanismos para la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, autoridades de control no pertenecientes a la región y autoridades y entidades internacionales en la materia.
ARTÍCULO 2- Definiciones 1. Para los efectos de la presente Ley se entenderá por: a. Anonimización: la aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o reidentificación de una persona física sin esfuerzos desproporcionados. b. Base de datos: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado o descentralizado. c. Cesión ~~o comunicación~~ de datos: toda revelación de datos realizada a una persona distinta del titular. d. Consentimiento: manifestación de la voluntad, libre, específica, inequívoca e informada, del titular a través de la cual acepta ~~y autoriza~~ mediante una acción declaración o una clara acción afirmativa, el tratamiento de los datos personales que le conciernen. e. Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas ~~o conductuales~~ de una persona física que permitan o confirmen ~~la~~ identificación única ~~de dicha persona~~, como imágenes faciales o datos dactiloscópicos. f. Datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.	ARTÍCULO 2- Definiciones 1. Para los efectos de la presente Ley se entenderá por: **a.** Anonimización: la aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o reidentificación de una persona física sin esfuerzos **o plazos** desproporcionados**, teniendo en cuenta factores como los costos y el tiempo necesario para la identificación o reidentificación de la persona a la luz de la tecnología disponible en el momento del tratamiento.** **b.** Base de datos: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado o descentralizado**, independientemente de que los datos se encuentren respaldados en soportes físicos o electrónicos.** c. Cesión de datos: toda revelación de datos realizada a una persona**, entidad u organización** distinta del **T**itular. d. Consentimiento: manifestación de la voluntad, libre, específica, inequívoca e informada del **T**itular **de los datos personales o su representante,** a través de la cual acepta**,** mediante una declaración o una clara acción afirmativa, el tratamiento de los datos personales que le conciernen. e. Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas de una persona física que permitan o confirmen **su** identificación única, **tales** como imágenes faciales o datos dactiloscópicos**, entre otros**.

g. Datos personales: cualquier información concerniente a una persona física 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.	f. Datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.
	g. Datos personales: cualquier información concerniente a una persona física 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.
h. Datos personales sensibles: aquellos que se refieran a la esfera íntima de su titular~~, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste~~. ~~De manera enunciativa,~~ se consideran sensibles los datos personales que ~~puedan~~ revel~~ar aspectos como~~ origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física.	h. Datos personales sensibles: aquellos que se refieran a la esfera íntima de su titular. **S**e consideran sensibles los datos personales que revel**en el** origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física.
i. Datos relativos a la salud: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;	i. Datos relativos a la salud: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria **en el ámbito público o privado**, que revelen información sobre su estado de salud;
j. Encargado: prestador de servicios, que, con el carácter de persona física o jurídica o autoridad pública, ajena a la organización del responsable, trata datos personales a nombre y por cuenta de éste.	j. Encargado: prestador de servicios, que, con el carácter de persona física o jurídica o autoridad pública, ajena a la organización del **R**esponsable, trata datos personales a nombre y por cuenta de éste.
k. Exportador: persona física o jurídica de carácter privado, autoridad pública, servicios, organismo o prestador de servicios que efectúe transferencias internacionales de datos personales, conforme a lo dispuesto en esta Ley.	k. Exportador: persona física o jurídica de carácter privado, autoridad pública, servicios, organismo o prestador de
l. Fuentes de acceso público: bases de datos ~~públicas~~ que pueden ser accedidas por cualquier persona,	

~~siempre y cuando una ley especial les haya dado ese carácter de manera expresa, o dicho acceso público sea razonablemente necesario para cumplir los fines previstos en esa ley especial y para los cuales se conformó la base de datos.~~ Se entienden como fuentes de acceso público, entre otras que puedan existir, las bases de datos de personas jurídicas, bienes inmuebles, bienes muebles, catastro y propiedad industrial del Registro Nacional, los registros de nacimientos, matrimonios y defunciones del Registro Civil, ~~y~~ las bases de datos que acrediten la condición de colegiado a un colegio profesional.	servicios que efectúe transferencias internacionales de datos personales, conforme a lo dispuesto en esta Ley. **l.** Fuentes de acceso público: bases de datos que pueden ser accedidas por cualquier persona. Se entienden como fuentes de acceso público, entre otras que puedan existir, **las siguientes: 1)** bases de datos de personas jurídicas, bienes inmuebles, bienes muebles, catastro y propiedad industrial del Registro Nacional, **2)** los registros de nacimientos, matrimonios y defunciones del Registro Civil, **3)** las bases de datos que acrediten la condición de colegiado a un colegio profesional**, 4) el diario oficial La Gaceta y el Boletín Judicial, independientemente del soporte físico o digital en el que se publiquen, 5) Las publicaciones realizadas en medios masivos de comunicación, entendiendo por tales los provenientes de la prensa, cualquiera sea el soporte en el que figuren o el canal a través del cual se practique la comunicación, 6) Las guías, publicaciones, anuarios, directorios y similares que tengan la finalidad comunicar públicamente la pertenencia de determinadas personas a organizaciones gremiales, asociaciones, colegios profesionales u otras organizaciones de la sociedad civil, en el tanto cuenten con el consentimiento del Titular y se cumpla la finalidad para la que dicho consentimiento fue otorgado por el Titular. El funcionamiento de las bases de datos de acceso público respetará los términos de la presente Ley, en especial en cuanto a los principios de legitimación y minimización.**
~~m.~~ Grupo ~~empresarial: grupo constituido por una empresa que ejerce el control y sus empresas controladas.~~	
n. Elaboración de perfiles: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.	
o. Normas corporativas vinculantes: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento para transferencias, cesiones o un conjunto de transferencias y cesiones de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo ~~empresarial~~ o una unión de empresas dedicadas a una actividad económica conjunta.	m. Grupo **económico: agrupación de sociedades o empresas, de hecho o de derecho, que se manifiesta mediante una unidad de decisión, es decir, la reunión de todos o una parte sustancial de los elementos de mando o dirección empresarial por medio de un centro de operaciones,**
p. Responsable: persona física o jurídica de carácter privado, autoridad pública, servicios u organismo que, solo o en conjunto con otros, determina los fines, medios, alcance y demás cuestiones	

relacionadas con un tratamiento de datos personales.	**y que se exterioriza mediante dos movimientos básicos: el criterio de unidad de dirección, ya sea por subordinación o por colaboración entre sus miembros, o el criterio de dependencia económica de sus miembros, sin importar que su personalidad jurídica se vea afectada, o que su patrimonio sea objeto de transferencia.**
q. Seudoanonimización: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.	n. Elaboración de perfiles: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.
r. Sistema de identificación biométrica: sistema o software que se desarrolla empleando: a) estrategias de aprendizaje automático, incluidos el aprendizaje supervisado, el no supervisado, el realizado por refuerzo, o el aprendizaje automático; b) estrategias basadas en la lógica y el conocimiento; o c) estrategias estadísticas y análogas; destinado a identificar a personas físicas a distancia comparando sus datos biométricos con los que figuran en una base de datos de referencia, y sin que el usuario del sistema sepa de antemano si la persona en cuestión se encontrará en dicha base de datos y podrá ser identificada. Se entenderá que se utiliza un sistema de identificación biométrica "en tiempo real" cuando la recogida de los datos biométricos, la comparación y la identificación se producen sin una demora significativa. Este término engloba no solo la identificación instantánea, sino también demoras mínimas limitadas, a fin de evitar su elusión.	o. Normas corporativas vinculantes: las políticas de protección de datos personales asumidas por un **R**esponsable o **E**ncargado del tratamiento para transferencias, cesiones o un conjunto de transferencias y cesiones de datos personales a un **R**esponsable o **E**ncargado en uno o más países terceros, dentro de un grupo **económico** o una unión de empresas dedicadas a una actividad económica conjunta.
s. Tercero: persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o ~~interesado~~, del responsable del tratamiento, del Responsable, Encargado y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento. Podrán ser también terceros los entes sin personalidad	p. Responsable: persona física o jurídica de carácter privado, autoridad pública, servicios u organismo que, solo o en conjunto con otros, determina los fines, medios, alcance y demás cuestiones relacionadas con un tratamiento de datos personales. q. Seudoanonimización: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado 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

jurídica que actúen en el tráfico como sujetos diferenciados. t. Titular: persona física a quien le conciernen los datos personales. ~~u. Transferencia de datos: se refiere a la transmisión o entrega de datos personales o bases de datos de un responsable o encargado del tratamiento a un nuevo responsable o corresponsable del tratamiento, que podrá definir de forma independiente o conjunta las finalidades y medios del tratamiento de los datos recibidos.~~ v. Tratamiento: cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre datos personales, relacionadas, de manera enunciativa más no limitativa, con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales.	se atribuyan a una persona física identificada o identificable. r. Sistema de identificación biométrica: sistema o software que se desarrolla empleando: a) estrategias de aprendizaje automático, incluidos el aprendizaje supervisado, el no supervisado, el realizado por refuerzo, o el aprendizaje automático; b) estrategias basadas en la lógica y el conocimiento; o c) estrategias estadísticas y análogas; destinado a identificar a personas físicas a distancia comparando sus datos biométricos con los que figuran en una base de datos de referencia, y sin que el usuario del sistema sepa de antemano si la persona en cuestión se encontrará en dicha base de datos y podrá ser identificada. Se entenderá que se utiliza un sistema de identificación biométrica "en tiempo real" cuando la recogida de los datos biométricos, la comparación y la identificación se producen sin una demora significativa. Este término engloba no solo la identificación instantánea, sino también demoras mínimas limitadas, a fin de evitar su elusión. s. Tercero: persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o **Titular del dato**, del **R**esponsable del tratamiento, del Responsable, Encargado y de las personas autorizadas para tratar los datos bajo la autoridad directa del **R**esponsable del tratamiento o del **E**ncargado del tratamiento. Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados. t. Titular: persona física a quien le conciernen los datos personales. u. Tratamiento: cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre datos personales, relacionadas, de manera enunciativa más no limitativa, con la

	obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, **cesión,** transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales. **v. Violación de la seguridad de los datos personales: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos personales.**
ARTÍCULO 3- Ámbito de aplicación subjetivo Esta Ley será aplicable a las personas físicas o jurídicas de carácter privado, y a la ~~a~~dministración ~~p~~ública ~~centralizada y descentralizada~~, que realicen tratamiento de datos personales en el ejercicio de sus actividades y funciones.	ARTÍCULO 3- Ámbito de aplicación subjetivo Esta Ley será aplicable a las personas físicas o jurídicas de carácter privado, y a la **Administración Pública en sentido amplio**, que realicen tratamiento de datos personales en el ejercicio de sus actividades y funciones.
ARTÍCULO 4- Ámbito de aplicación objetivo 1. Esta Ley será aplicable al tratamiento de datos personales de personas físicas que consten o estén destinados a constar en soportes físicos, automatizados total o parcialmente, o en ambos soportes, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización. 2. Esta Ley no será aplicable en los siguientes supuestos: a. Cuando los datos personales estén destinados exclusivamente a actividades en el marco de la vida familiar o doméstica de una persona física, esto es, 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. b. La información anónima, es decir, aquélla que no guarda relación con una persona física identificada o	ARTÍCULO 4- Ámbito de aplicación objetivo 1. Esta Ley será aplicable al tratamiento de datos personales de personas físicas que consten o estén destinados a constar en soportes físicos, automatizados total o parcialmente, o en ambos soportes, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización. 2. Esta Ley no será aplicable en los siguientes supuestos: a. Cuando los datos personales estén destinados exclusivamente a actividades en el marco de la vida familiar o doméstica de una persona física, esto es, 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. b. La información anónima, es decir, aquélla que no guarda relación con una persona física identificada o identificable, así como los datos

identificable, así como los datos personales sometidos a un proceso de anonimización de tal forma que el titular no pueda ser identificado o reidentificado. ~~c. A los tratamientos de persona fallecidas, sin perjuicio de lo establecido en el artículo 5 de esta Ley.~~ ~~d. A los tratamientos sometidos a la normativa sobre protección de materias clasificadas o secretos de Estado.~~	personales sometidos a un proceso de anonimización de tal forma que el **T**itular no pueda ser identificado o reidentificado.
ARTÍCULO 5-Datos de personas fallecidas 1. ~~Las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos~~ podrán dirigirse al responsable o encargado del tratamiento con objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión. 2. Como excepción, ~~las personas a las que se refiere el párrafo anterior~~ no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente por escrito o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante. 3. Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión. 4. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales. 5. En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de salvaguardia, si tales facultades se entendieran comprendidas en las medidas de salvaguardia prestadas por el designado.	ARTÍCULO 5-Datos de personas fallecidas 1. **En caso de fallecimiento del Titular de los datos, los derechos que reconoce la presente Ley pueden ser ejercidos por sus herederos, que, previa acreditación de su condición,** podrán dirigirse al **R**esponsable o **E**ncargado del tratamiento con objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión 2. Como excepción, **los herederos** no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente por escrito o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante. 3. Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión. 4. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales. 5. En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de salvaguardia, si tales facultades se entendieran comprendidas en las medidas de salvaguardia prestadas por el designado.

ARTÍCULO 6- Ámbito de aplicación territorial 1. Esta Ley resultará aplicable al tratamiento de datos personales efectuado: a. Por un responsable o encargado con establecimiento en la República de Costa Rica. b. Por un responsable o encargado sin establecimiento en la República de Costa Rica, cuando las actividades del tratamiento estén relacionadas con la oferta de bienes o servicios dirigidos a los habitantes de la República de Costa Rica, o bien, estén relacionadas con el control de su comportamiento, en la medida en que éste tenga lugar en la República de Costa Rica. c. Por un responsable o encargado que no cuente con establecimiento en la República de Costa Rica, pero le resulte aplicable la legislación nacional, derivado de la celebración de un contrato o en virtud de las normas del derecho internacional privado. ~~d. Por un responsable o encargado sin establecimiento en territorio costarricense y que utilice o recurra a medios, automatizados o no, situados en ese territorio para tratar datos personales, salvo que dichos medios se utilicen solamente con fines de tránsito.~~ 2. Para los efectos de la presente Ley, se entenderá por establecimiento el lugar de la administración central o principal del responsable o encargado, el cual deberá determinarse en función de criterios objetivos e implicar el ejercicio efectivo y real de actividades de gestión que determinen las principales decisiones en cuanto a los fines y medios del tratamiento de datos personales que lleve a cabo, a través de modalidades estables. 3. La presencia y utilización de medios técnicos y tecnologías para el tratamiento de datos personales o las actividades de tratamiento no constituirán, en sí mismas, un establecimiento principal y no serán considerados como criterios determinantes para la definición del establecimiento principal del responsable o encargado.	ARTÍCULO 6- Ámbito de aplicación territorial 1. Esta Ley resultará aplicable al tratamiento de datos personales efectuado: a. Por un **R**esponsable o **E**ncargado con establecimiento en la República de Costa Rica. b. Por un **R**esponsable o **E**ncargado sin establecimiento en la República de Costa Rica, cuando las actividades del tratamiento estén relacionadas con la oferta de bienes o servicios dirigidos a los habitantes de la República de Costa Rica, o bien, estén relacionadas con el control de su comportamiento, en la medida en que éste tenga lugar en la República de Costa Rica. c. Por un **R**esponsable o **E**ncargado que no cuente con establecimiento en la República de Costa Rica, pero le resulte aplicable la legislación nacional, derivado de la celebración de un contrato o en virtud de las normas del derecho internacional privado. 2. Para los efectos de la presente Ley, se entenderá por establecimiento el lugar de la administración central o principal del **R**esponsable o **E**ncargado, el cual deberá determinarse en función de criterios objetivos e implicar el ejercicio efectivo y real de actividades de gestión que determinen las principales decisiones en cuanto a los fines y medios del tratamiento de datos personales que lleve a cabo, a través de modalidades estables. 3. La presencia y utilización de medios técnicos y tecnologías para el tratamiento de datos personales o las actividades de tratamiento no constituirán, en sí mismas, un establecimiento principal y no serán considerados como criterios determinantes para la definición del establecimiento principal del **R**esponsable o **E**ncargado. 4. Cuando el tratamiento de datos personales lo realice un grupo **económico**, el establecimiento principal de la empresa que ejerce el control deberá considerarse el establecimiento principal del grupo **económico**, excepto cuando los fines y medios del tratamiento los determine efectivamente otra de las empresas del grupo.

4. Cuando el tratamiento de datos personales lo realice un grupo ~~empresarial~~, el establecimiento principal de la empresa que ejerce el control deberá considerarse el establecimiento principal del grupo ~~empresarial~~, excepto cuando los fines y medios del tratamiento los determine efectivamente otra de las empresas del grupo.	
ARTÍCULO 7- Excepciones generales al derecho a la protección de datos personales ~~1.~~ Cualquier ley que tenga como propósito limitar el derecho a la protección de datos personales contendrá, como mínimo, disposiciones relativas a: a. La finalidad del tratamiento. b. Las categorías de datos personales de que se trate. c. El alcance de las limitaciones establecidas. d. Las garantías adecuadas para evitar accesos o transferencias ilícitas o desproporcionadas. e. La determinación del responsable o responsables. f. Los plazos de conservación de los datos personales. g. Los posibles riesgos para los derechos y libertades de los titulares. h. El derecho de los titulares a ser informados sobre la limitación, salvo que resulte perjudicial o incompatible a los fines de ésta. ~~2. Las leyes serán las necesarias, adecuadas y proporcionales en una sociedad democrática, y deberán respetar los derechos y las libertades fundamentales de los titulares.~~ ~~3.~~ Ninguna limitación del derecho fundamental a la protección de datos personales podrá vaciar de contenido este derecho, por lo que se respetará el cumplimiento de las garantías, principios y derechos del titular que no sea necesario limitar o restringir para acometer el fin público	ARTÍCULO 7.- Excepciones generales al derecho a la protección de datos personales 1. **No se podrá** limitar el derecho a la protección de datos personales **mediante ley, salvo de manera excepcional, cuando existan razones que justifiquen su necesidad, sean adecuadas y proporcionales en una sociedad democrática, y respeten los derechos y las libertades fundamentales de los Titulares.** **2.** Ninguna limitación del derecho fundamental a la protección de datos personales podrá vaciar de contenido este derecho, por lo que se respetará el cumplimiento de las garantías, principios y derechos del **T**itular que no sea necesario limitar o restringir para acometer el fin público perseguido. El deber de información deberá ser garantizado en todo momento. El incumplimiento de este inciso dará pie a responsabilidad disciplinaria de los funcionarios implicados y a responsabilidad administrativa del Estado, sin perjuicio de las demás sanciones previstas en el régimen sancionatorio de esta Ley o de las responsabilidades penales establecidas en el Código Penal. **3. Cualquier Ley que tenga como propósito limitar el derecho a la protección de datos personales** contendrá, como mínimo, disposiciones relativas a: a. La finalidad del tratamiento. b. Las categorías de datos personales de que se trate. c. El alcance de las limitaciones establecidas. d. Las garantías adecuadas para evitar accesos**, cesiones** o transferencias ilícitas o desproporcionadas.

perseguido. El deber de información deberá ser garantizado en todo momento. El incumplimiento de este inciso dará pie a responsabilidad disciplinaria de los funcionarios implicados y a responsabilidad administrativa del Estado, sin perjuicio de las demás sanciones previstas en el régimen sancionatorio de esta Ley o de las responsabilidades penales establecidas en el Código Penal.	e. La determinación del **R**esponsable o **R**esponsables. f. Los plazos de conservación de los datos personales. g. Los posibles riesgos para los derechos y libertades de los **T**itulares. h. El derecho de los Titulares a ser informados sobre la limitación, salvo que resulte perjudicial o incompatible a los fines de ésta.
ARTÍCULO 8- Tratamientos de datos por obligación legal, interés público o ejercicio de poderes públicos y ~~transferencias~~ interinstitucionales 1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable cuando así lo prevea una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras similares. 2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable cuando derive de una competencia atribuida por una norma con rango de ley. 3. Las ~~transferencias~~ de datos personales que se efectúen entre entes públicos en el marco de una obligación legal, interés público o ejercicio de poderes públicos, así como todo tratamiento realizado con los datos ~~transferidos~~, serán lícitas en la medida en que se cumplan las siguientes condiciones acumulativas: a) Que una ley especial lo autorice expresamente, o que ~~la transferencia~~ sea estrictamente necesaria para cumplir con los fines de interés público asignados por Ley a la entidad receptora de los datos. En el caso de esta segunda alternativa, la ~~transferencia~~ solo se llevará a cabo previa autorización de la	ARTÍCULO 8.- Tratamientos de datos por obligación legal, interés público o ejercicio de poderes públicos y **cesiones** interinstitucionales **de datos en el sector público** 1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al **R**esponsable cuando así lo prevea una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras similares**, que no deberán ser menores a las garantías y derechos establecidos en esta Ley.** 2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al **R**esponsable cuando derive de una competencia atribuida por una norma con rango de ley. 3. Las **cesiones** de datos personales que se efectúen entre entes públicos en el marco de una obligación legal, interés público o ejercicio de poderes públicos, así como todo tratamiento realizado con los datos **cedidos**, serán lícitas en la medida en que se cumplan las siguientes condiciones acumulativas: a) Que una ley especial lo autorice expresamente, o que **la cesión** sea estrictamente necesaria para cumplir con los fines de interés público asignados por **l**ey a la

Agencia de Protección de Datos, quien deberá verificar que: i) la ~~transferencia~~ sea absolutamente necesaria para cumplir con el fin público invocado y asignado por Ley a la entidad receptora; ii) que los datos a ceder son los estrictamente necesarios y adecuados para ese fin. iii) que la entidad receptora de los datos cuenta con las medidas de seguridad, protocolos y demás garantías establecidas en esta Ley, para proteger la integridad, disponibilidad y confidencialidad de los datos. b) Que el ente que ~~transfiere~~ los datos los haya obtenido con fundamento en una de las bases legales previstas en el artículo ~~14~~ y en el ejercicio de sus competencias asignadas por ley. c) Que el ente receptor utilice los datos pretendidos para una finalidad que se encuentre dentro del marco de sus competencias legales vigentes. d) Que los datos involucrados en la ~~transferencia~~ sean únicamente los adecuados y estrictamente necesarios para acometer la finalidad pública, de conformidad con el principio de minimización. Se prohíbe la cesión masiva e indiscriminada de bases de datos. En cualquiera de los anteriores supuestos, las transferencias deberán ponerse en conocimiento de todos los titulares de los datos involucrados de manera segura y sin comprometer su confidencialidad, dentro de los siguientes quince días a la ejecución de la ~~transferencia~~. Además, la ~~transferencia~~ debe documentarse en un convenio interinstitucional que deberá ser publicado y puesto a disposición de la ciudadanía para su escrutinio, resguardando la confidencialidad de los datos personales involucrados en la transferencia. Este convenio deberá contener disposiciones específicas respecto de las condiciones que rigen la licitud del tratamiento por parte de las personas responsables; la descripción clara de la categoría de personas cuyos datos se ~~procesarán~~, sin exponer datos que puedan	entidad receptora de los datos. En el caso de esta segunda alternativa, la **cesión** solo se llevará a cabo previa autorización de la Agencia de Protección de Datos, quien deberá verificar, **en un plazo no mayor a 10 días hábiles, el cumplimiento de las siguientes condiciones acumulativas:** i) la **cesión** sea absolutamente necesaria para cumplir con el fin público invocado y asignado por ley a la entidad receptora; ii) que los datos a ceder son los estrictamente necesarios y adecuados para ese fin. iii) que la entidad receptora de los datos cuenta con las medidas de seguridad, protocolos y demás garantías establecidas en esta Ley, para proteger la integridad, disponibilidad y confidencialidad de los datos. b) Que el ente que **cede** los datos los haya obtenido con fundamento en una de las bases legales previstas en el artículo **15** y en el ejercicio de sus competencias asignadas por ley. c) Que el ente receptor utilice los datos pretendidos para una finalidad que se encuentre dentro del marco de sus competencias legales vigentes. d) Que los datos involucrados en la **cesión** sean únicamente los adecuados y estrictamente necesarios para acometer la finalidad pública, de conformidad con el principio de minimización **de datos**. Se prohíbe la cesión o **transferencia masiva** e indiscriminada de bases de datos. **4.** En cualquiera de los anteriores supuestos, las **cesiones** deberán ponerse en conocimiento de todos los **T**itulares de los datos involucrados de manera segura y sin comprometer su confidencialidad, dentro de los siguientes quince días a la ejecución de la **cesión**. Además, la **cesión** debe documentarse en un convenio interinstitucional que deberá **ser comunicado a la Agencia de Protección de Datos Personales**, publicado y puesto a disposición de la ciudadanía para su escrutinio, resguardando la confidencialidad de los datos personales involucrados en la **cesión**. Este convenio deberá contener disposiciones específicas respecto de las condiciones que rigen la licitud del tratamiento por parte de las personas responsables; la descripción clara de

identificar a las personas; los tipos de datos objeto de tratamiento, especialmente si contienen categorías de datos sensibles; la finalidad específica del tratamiento; los plazos de conservación de los datos; un detalle de las operaciones y los procedimientos del tratamiento; incluidas las medidas técnicas, físicas y organizativas de seguridad que se establecerán para proteger la información; y un medio de contacto para obtener más información sobre la ~~transferencia.~~ Las transferencias no serán de conocimiento público ni deberán ser puestas en conocimiento de los titulares cuando tengan por objeto la investigación de un posible delito o para fines policiales, ni en aquellos casos donde la revelación de la transferencia a los titulares pueda comprometer seriamente el objetivo de interés público perseguido con la transferencia.	la categoría de personas cuyos datos se **tratarán**, sin exponer datos que puedan identificar a las personas; los tipos de datos objeto de tratamiento, especialmente si contienen categorías de datos sensibles; la finalidad específica del tratamiento; los plazos de conservación de los datos; un detalle de las operaciones y los procedimientos del tratamiento; incluidas las medidas técnicas, físicas y organizativas de seguridad que se establecerán para proteger la información; y un medio de contacto para obtener más información sobre la **cesión, así como los medios para solicitar el efectivo ejercicio de los derechos del Titular.** **5.** Las transferencias o **cesiones** no serán de conocimiento público ni deberán ser puestas en conocimiento de los **T**itulares cuando tengan por objeto la investigación de un posible delito o para fines policiales, ni en aquellos casos donde la revelación de la transferencia **o cesión** a los **T**itulares pueda comprometer seriamente el objetivo de interés público perseguido con la transferencia **o cesión**. **6. No se considerará cesión ni transferencia de datos la remisión de datos personales realizada por un Responsable o Encargado del sector público ante una orden de una autoridad judicial competente en el marco de sus facultades legales, siempre que dicha orden se realice dentro de una investigación o procedimiento específico.**
ARTÍCULO 9- Tratamiento de datos personales de niñas, niños y adolescentes 1. En el tratamiento de datos personales concernientes a niñas, niños y adolescentes se privilegiará la protección del interés superior de éstos, conforme a la Convención sobre los Derechos del Niño y demás instrumentos internacionales que busquen su bienestar y protección integral. 2. Se promoverá en la formación académica de las niñas, niños y adolescentes, el uso responsable, adecuado y seguro de las tecnologías de la información y comunicación y los eventuales riesgos a los que se enfrentan en ambientes digitales respecto del tratamiento indebido de sus datos personales, así como el respeto de sus derechos y libertades.	ARTÍCULO 9.- Tratamiento de datos personales de niñas, niños y adolescentes 1. En el tratamiento de datos personales concernientes a niñas, niños y adolescentes se privilegiará la protección del interés superior de éstos, conforme a la Convención sobre los Derechos del Niño y demás instrumentos internacionales que busquen su bienestar y protección integral. 2. Se promoverá en la formación académica de las niñas, niños y adolescentes, el uso responsable, adecuado y seguro de las tecnologías de la información y comunicación y los eventuales riesgos a los que se enfrentan en ambientes digitales respecto del tratamiento indebido de sus datos personales, así como el respeto de sus derechos y libertades.

3. Los padres, madres, tutores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.	3. Los padres, madres, tutores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.
ARTÍCULO 10- Tratamiento de datos personales sensibles 1. Por regla general, queda prohibido el tratamiento de datos personales sensibles, que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, salvo que se presente cualquiera de los siguientes supuestos: a. Los mismos sean ~~estrictamente~~ necesarios para el ejercicio y cumplimiento de ~~las~~ atribuciones y obligaciones ~~expresamente~~ previstas en las normas ~~que regulan~~ su actuación. b. Se dé cumplimiento a un mandato legal. c. Sea necesario para proteger intereses vitales del titular o de otra persona física, en el supuesto de que el titular no esté capacitado, física o jurídicamente, para dar su consentimiento; d. Se cuente con el consentimiento expreso del titular ~~con~~ uno o más fines especificados. e. Sean necesarios por razones de seguridad nacional, seguridad pública, orden público, salud pública o salvaguarda de derechos y libertades de terceros, ~~fundados~~ en ley especial, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y	ARTÍCULO 10.- Tratamiento de datos personales sensibles 1. Por regla general, queda prohibido el tratamiento de datos personales sensibles, que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, salvo que se presente cualquiera de los siguientes supuestos: **a.** Los mismos sean **razonablemente** necesarios para el ejercicio y cumplimiento de atribuciones y obligaciones previstas en **una** norma **legal o en un contrato libremente consentido por el Titular de los datos.** b. Se dé cumplimiento a un mandato legal. c. Sea necesario para proteger intereses vitales del **T**itular o de otra persona física, en el supuesto de que el **T**itular no esté capacitado, física o jurídicamente, para dar su consentimiento; **d.** Se cuente con el consentimiento expreso del **T**itular **para** uno o más fines especificados**, consentimiento que podrá derivar de un contrato donde el tratamiento de tales datos sensibles resulta indispensable, siempre que así conste que se haya informado al Titular.** e. Sean necesarios por razones de seguridad nacional, seguridad pública,

específicas para proteger los intereses y derechos fundamentales del titular. f. Sea necesarios para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base de la legislación aplicable a la materia o en virtud de un contrato con un profesional de la salud sujeto a la obligación de secreto profesional, o bajo su responsabilidad. g. Sean necesarios por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, con fundamento en una legislación que establezca medidas adecuadas y específicas para proteger los derechos y libertades del titular, en particular el secreto profesional~~,~~ h. Sean con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, con fundamento en una ley especial que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular. 2. Exclusivamente mediante ley aplicable en la materia podrá establecerse excepciones, garantías y condiciones adicionales para asegurar el debido tratamiento de los datos personales sensibles.	orden público, salud pública o salvaguarda de derechos y libertades de terceros, **fundadas** en ley especial, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del **T**itular. f. Sea necesarios para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, **investigación en salud**, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base de la legislación aplicable a la materia o en virtud de un contrato con un profesional de la salud sujeto a la obligación de secreto profesional, o bajo su responsabilidad. g. Sean necesarios por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, **como pandemias debidamente declaradas por las autoridades de salud competentes**, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, con fundamento en una legislación que establezca medidas adecuadas y específicas para proteger los derechos y libertades del **T**itular, en particular el secreto profesional. h. Sean con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, con fundamento en una ley especial que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del **T**itular. **i. El tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del**

	Responsable o del Titular en el ámbito del derecho laboral, de la seguridad social o ayudas sociales, en la medida en que así lo autorice el marco normativo y establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del Titular. **j. El tratamiento sea efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los Titulares;** **k. El tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.** 2. Exclusivamente mediante ley aplicable en la materia podrá establecerse excepciones, garantías y condiciones adicionales para asegurar el debido tratamiento de los datos personales sensibles.
ARTÍCULO 11- Tratamiento de datos personales relativos a condenas e infracciones penales 1. El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas. Solo podrá llevarse un registro completo de condenas penales bajo el control del Poder Judicial.	ARTÍCULO 11.- Tratamiento de datos personales relativos a condenas e infracciones penales 1. El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas. Solo podrá llevarse un registro completo de condenas penales bajo el control del Poder Judicial **y/o el Ministerio de Justicia.** **2. Además de los funcionarios judiciales involucrados, los abogados en ejercicio podrán realizar tratamiento de datos personales referidos a condenas e infracciones penales, así como a**

	procedimientos y medidas cautelares y de seguridad conexas cuando tengan por objeto tratar la información tratada por sus clientes para el ejercicio de sus funciones, bajo la obligación de secreto profesional.
ARTÍCULO 12- Tratamiento de datos personales obtenidos de fuentes de acceso público Los datos obtenidos de fuentes de acceso público solo podrán ser tratados para los fines establecidos por **L**ey, y de conformidad con el principio de minimización, por lo que solo serán incluidos en estas bases los datos estrictamente necesarios, adecuados y pertinentes para cumplir la finalidad pública. Los titulares gozarán de todos los derechos, principios y garantías establecidos en esta Ley respecto de sus datos personales que consten en fuentes de acceso público, los cuales solo podrán ser limitados, mas no extinguidos, en la medida en que la limitación sea estrictamente necesaria, idónea y proporcional para garantizar los fines de interés público de la base de datos pública. ~~Bajo ninguna circunstancia un dato personal sensible podrá ser incorporado en una base de datos de acceso público.~~	ARTÍCULO 12.-Tratamiento de datos personales obtenidos de fuentes de acceso público Los datos obtenidos de fuentes de acceso público solo ~~podrán~~ ser tratados para los fines establecidos por **l**ey, y de conformidad con el principio de minimización, por lo que solo serán incluidos en estas bases los datos estrictamente necesarios, adecuados y pertinentes para cumplir la finalidad pública. Los **T**itulares gozarán de todos los derechos, principios y garantías establecidos en esta **L**ey respecto de sus datos personales que consten en fuentes de acceso público, los cuales solo podrán ser limitados, mas no extinguidos, en la medida en que la limitación sea estrictamente necesaria, idónea y proporcional para garantizar los fines de interés público de la base de datos pública.
CAPÍTULO II PRINCIPIOS DE PROTECCIÓN DE DATOS PERSONALES	CAPÍTULO II PRINCIPIOS DE PROTECCIÓN DE DATOS PERSONALES
ARTÍCULO 13- Principios aplicables al tratamiento de datos personales ~~1.~~ ~~En~~ el tratamiento de datos personales~~, el responsable observará~~ los principios de exactitud, legitimación, lealtad, transparencia, finalidad, ~~proporcionalidad, calidad~~, responsabilidad, seguridad y confidencialidad.	ARTÍCULO 13.- Principios aplicables al tratamiento de datos personales **E**l tratamiento de datos personales **deberá realizarse conforme a** los principios de exactitud, legitimación, lealtad, transparencia, **limitación de la** finalidad, **minimización, exactitud**, responsabilidad, seguridad y confidencialidad.
ARTÍCULO 14- Principio de exactitud 1. Los datos serán exactos, y si fuere necesario, actualizados. No será imputable al responsable ~~del tratamiento~~, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos: a. Hubiesen sido obtenidos por el responsable directamente del afectado.	ARTÍCULO 14.- Principio de exactitud 1. Los datos serán exactos, y si fuere necesario, actualizados. No será imputable al **R**esponsable, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos:

b. Hubiesen sido obtenidos por el responsable de un encargado que los ~~recogió~~ en nombre propio para su transmisión al responsable. c. Fuesen sometidos a tratamiento por el responsable por haberlos recibido de otro responsable en virtud del ejercicio del afectado del derecho a la portabilidad previsto en esta Ley. d. Fuesen obtenidos de un registro público por el responsable.	a. Hubiesen sido obtenidos por el Responsable directamente del afectado. b. Hubiesen sido obtenidos por el **R**esponsable de un **E**ncargado que los **recolectó** en nombre propio para su transmisión al Responsable. c. Fuesen sometidos a tratamiento por el **R**esponsable por haberlos recibido de otro **R**esponsable en virtud del ejercicio del afectado del derecho a la portabilidad previsto en esta Ley. d. Fuesen obtenidos de un registro público por el **R**esponsable. **2. En todos los casos anteriores el Titular tendrá derecho de solicitar rectificación de sus datos personales.**
ARTÍCULO 15- Principio de legitimación 1. ~~El responsable~~ solo ~~podrá tratar datos personales~~ cuando se ~~presente alguno de los siguientes supuestos:~~ a. El titular otorgue su consentimiento para una o varias finalidades específicas. b. El tratamiento sea necesario para el cumplimiento de una orden judicial, resolución o mandato fundado y motivado de autoridad pública competente. c. El tratamiento sea necesario para el ejercicio de facultades propias de las autoridades públicas ~~o~~ se realice en virtud de una habilitación legal. d. El tratamiento sea necesario para el reconocimiento o defensa de los derechos del titular ante una autoridad pública. e. El tratamiento sea necesario para la ejecución de un contrato o precontrato en el que el titular sea parte. f. El tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al responsable.	ARTÍCULO 15.- Principio de legitimación 1. **El tratamiento de los datos personales será legítimo** solo cuando se **realice con fundamento en alguna de las siguientes bases de legitimación:** a. El **T**itular otorgue su consentimiento para una o varias finalidades específicas. b. El tratamiento sea necesario para el cumplimiento de una orden judicial, resolución o mandato fundado y motivado de autoridad pública competente. c. El tratamiento sea necesario para el ejercicio de facultades propias de las autoridades públicas **y** se realice en virtud de una habilitación legal. d. El tratamiento sea necesario para el reconocimiento o defensa de los derechos del **T**itular ante una autoridad pública. e. El tratamiento sea necesario para la ejecución de un contrato o precontrato en el que el **T**itular sea parte.

g. El tratamiento sea necesario para proteger intereses vitales del titular o de otra persona física. h. El tratamiento sea necesario por razones de interés público establecidas o previstas en ley. i. El tratamiento sea necesario 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 que requiera la protección de datos personales, en particular cuando el titular sea niño, niña o adolescente. Lo anterior, no resultará aplicable a los tratamientos de datos personales realizados por las autoridades públicas en el ejercicio de sus funciones. ~~2. Tratándose de este último inciso, se entenderá amparado por el interés legítimo el tratamiento de datos personales de contacto que sea imprescindible para la localización de personas físicas que prestan sus servicios al responsable, con la finalidad de mantener cualquier tipo de relación con ésta.~~ ~~3. El tratamiento de datos personales que realicen las autoridades públicas se sujetará a las facultades o atribuciones que la ley les confiera expresamente.~~	f. El tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al **R**esponsable. g. El tratamiento sea necesario para proteger intereses vitales del **T**itular o de otra persona física. h. El tratamiento sea necesario por razones de interés público establecidas o previstas en **una** ley. i. El tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el **R**esponsable o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del **T**itular que requiera la protección de datos personales, en particular cuando el **Ti**tular sea niño, niña o adolescente. Lo anterior, no resultará aplicable a los tratamientos de datos personales realizados por las autoridades públicas en el ejercicio de sus funciones. **2. Los supuestos establecidos en los incisos b, c, f y h estarán sujetos al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta Ley y a los criterios de legalidad, proporcionalidad y necesidad.**
ARTÍCULO 16- Condiciones para el consentimiento 1. Cuando sea necesario obtener el consentimiento del titular, el responsable demostrará de manera indubitable que el titular otorgó su consentimiento, ya sea a través de una declaración o una acción afirmativa clara. 2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas. 3. Si el consentimiento del titular se da en el contexto de una declaración escrita que	ARTÍCULO 16.- Condiciones para el consentimiento 1. Cuando sea necesario obtener el consentimiento del **T**itular, el **R**esponsable demostrará de manera indubitable que el **T**itular otorgó su consentimiento, ya sea a través de una declaración o una acción afirmativa clara. 2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas. 3. Si el consentimiento del **T**itular se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de

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 de la presente Ley. 4. No podrá supeditarse la ejecución de un contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual. 5. Siempre que sea requerido el consentimiento para el tratamiento de los datos personales, el titular podrá revocarlo en cualquier momento, para lo cual el responsable establecerá mecanismos sencillos, ágiles, eficaces y gratuitos. La revocación del consentimiento no afectará la licitud del tratamiento basada en el consentimiento previo a su revocación. 6. Cuando los datos y/o el consentimiento se recaben a través de internet, aplicaciones móviles u otros medios electrónicos, el responsable podrá cumplir su deber de información en capas, suministrando al interesado, en la misma sección donde se recolecta el consentimiento, un vínculo funcional que remita al interesado al sitio donde almacena el responsable la información exigida en el artículo 6 de esta Ley.	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 de la presente Ley. 4. No podrá supeditarse la ejecución de un contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual. 5. Siempre que sea requerido el consentimiento para el tratamiento de los datos personales, el **T**itular podrá revocarlo en cualquier momento, para lo cual el **R**esponsable establecerá mecanismos sencillos, ágiles, eficaces y gratuitos. La revocación del consentimiento no afectará la licitud del tratamiento basada en el consentimiento previo a su revocación. 6. Cuando los datos y/o el consentimiento se recaben a través de internet, aplicaciones móviles u otros medios electrónicos, el **R**esponsable podrá cumplir su deber de información en capas, suministrando al interesado, en la misma sección donde se recolecta el consentimiento, un vínculo funcional que remita al interesado al sitio donde almacena el **R**esponsable la información exigida en el artículo 6 de esta Ley.
ARTÍCULO 17- Consentimiento para el tratamiento de datos personales de niñas, niños y adolescentes 1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de quince años. Se exceptúan los supuestos en que la ley exija la ~~asistencia~~ de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento. 2. El tratamiento de los datos de los menores de quince años, fundado en el	**ARTÍCULO 17.- Consentimiento para el tratamiento de datos personales de niñas, niños y adolescentes** 1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de quince años. Se exceptúan los supuestos en que la ley exija la **participación** de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento. 2. El tratamiento de los datos de los menores de quince años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria

consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, conforme lo previsto en la legislación respectiva.	potestad o tutela, conforme lo previsto en la legislación respectiva.
ARTÍCULO 18- Principio de lealtad 1. El responsable tratará los datos personales en su posesión privilegiando la protección de los intereses del titular y absteniéndose de tratar éstos a través de medios engañosos o fraudulentos. 2. Para los efectos de esta Ley, se considerarán desleales aquellos tratamientos de datos personales que den lugar a una discriminación injusta o arbitraria contra los titulares.	ARTÍCULO 18.- Principio de lealtad 1. El **R**esponsable tratará los datos personales en su posesión privilegiando la protección de los intereses del **T**itular y absteniéndose de tratar éstos a través de medios engañosos o fraudulentos. 2. Para los efectos de esta Ley, se considerarán desleales aquellos tratamientos de datos personales que den lugar a una discriminación injusta o arbitraria contra los **T**itulares **o excedan las expectativas razonables del Titular respecto a sus finalidades.**
ARTÍCULO 19- Principio de transparencia 1. Cuando se obtengan directamente de un titular, datos personales relativos a él, el responsable informará al titular en el momento en que estos se obtengan sobre la existencia misma y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto. 2. El responsable proporcionará al titular, al menos, la siguiente información: a. Su identidad y datos de contacto. b. Los datos de contacto del oficial de protección de datos, de haberlo. c. Las finalidades del tratamiento a que serán sometidos sus datos personales y la base jurídica del tratamiento. d. Las transferencias~~, nacionales o~~ internacionales, de datos personales ~~que pretenda realizar,~~ incluyendo los destinatarios y ~~las~~ finalidades que motivan la realización de las mismas. e. La existencia, forma y mecanismos o procedimientos a través de los cuales podrá ejercer los derechos de acceso, rectificación, cancelación, oposición y portabilidad.	ARTÍCULO 19.- Principio de transparencia 1. Cuando se obtengan directamente de un **T**itular, datos personales relativos a él, el **R**esponsable informará al **T**itular en el momento en que estos se obtengan sobre la existencia misma y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto. 2. El **R**esponsable proporcionará al **T**itular, al menos, la siguiente información: a. Su identidad y datos de contacto. b. Los datos de contacto del oficial de protección de datos, de haberlo. c. Las finalidades del tratamiento a que serán sometidos sus datos personales y la base jurídica del tratamiento. d. La **existencia de cesiones y/o** transferencias internacionales de datos personales, los destinatarios, **las categorías de datos** y finalidades que motivan la realización de las mismas. e. La existencia, forma y mecanismos o procedimientos a través de los cuales podrá ejercer los derechos de acceso, rectificación, cancelación, oposición y portabilidad.

f. El plazo durante el cual se conservarán los datos personales, o cuando no sea posible, los criterios utilizados para determinar ese plazo. g. En su caso, el origen de los datos personales cuando el responsable no los hubiere obtenido directamente del titular. h. El derecho del titular a presentar una reclamación ante la Agencia de Protección de Datos. 3. La información proporcionada al titular tendrá que ser suficiente y fácilmente accesible, así como redactarse y estructurarse en un lenguaje claro, sencillo y de fácil comprensión para los titulares a quienes va dirigida, especialmente si se trata de niñas, niños y adolescentes. 4. Cuando los datos sean obtenidos del titular, el responsable del tratamiento podrá dar cumplimiento al deber de información facilitando al titular la información básica contenida en los incisos a, b y d del inciso 2 de este artículo, e indicándole una dirección electrónica o proporcionándole un vínculo funcional u otro medio que permita acceder de forma sencilla e inmediata a la restante información. 5. Todo responsable contará con políticas transparentes de los tratamientos de datos personales que realice.	f. El plazo durante el cual se conservarán los datos personales, o cuando no sea posible, los criterios utilizados para determinar ese plazo. g. En su caso, el origen de los datos personales cuando el **R**esponsable no los hubiere obtenido directamente del **T**itular. h. El derecho del **T**itular a presentar una reclamación ante la Agencia de Protección de Datos. 3. La información proporcionada al **T**itular tendrá que ser suficiente y fácilmente accesible, así como redactarse y estructurarse en un lenguaje claro, sencillo y de fácil comprensión para los **T**itulares a quienes va dirigida, especialmente si se trata de niñas, niños y adolescentes. 4. Cuando los datos sean obtenidos del **T**itular, el **R**esponsable del tratamiento podrá dar cumplimiento al deber de información facilitando al **Ti**tular la información básica contenida en los incisos a, b y d del inciso 2 de este artículo, e indicándole una dirección electrónica o proporcionándole un vínculo funcional u otro medio que permita acceder de forma sencilla e inmediata a la restante información. 5. Todo **Responsable** contará con políticas transparentes de los tratamientos de datos personales que realice.
ARTÍCULO 20- Principio de finalidad 1. Todo tratamiento de datos personales se limitará al cumplimiento de finalidades determinadas, explícitas y legítimas. 2. El responsable no podrá tratar los datos personales en su posesión para finalidades distintas a aquéllas que motivaron el tratamiento original de éstos, a menos que concurra alguna de las causales que habiliten un nuevo tratamiento de datos conforme al principio de legitimación.	ARTÍCULO 20.- Principio de finalidad 1. Todo tratamiento de datos personales se limitará al cumplimiento de finalidades determinadas, explícitas y legítimas. 2. El **R**esponsable no podrá tratar los datos personales en su posesión para finalidades distintas**, análogas o compatibles** a aquéllas que motivaron el tratamiento original de éstos, a menos que concurra alguna de las causales que habiliten un nuevo tratamiento de datos conforme al principio de legitimación.

3. El tratamiento ulterior de datos personales con fines archivísticos, de investigación científica e histórica o con fines estadísticos, todos ellos, en favor del interés público, no se considerará incompatible con las finalidades iniciales.	3. El tratamiento ulterior de datos personales con fines archivísticos, de investigación científica e histórica o con fines estadísticos, todos ellos, en favor del interés público, no se considerará incompatible con las finalidades iniciales.
ARTÍCULO 21- Principio de minimización 1- El responsable tratará únicamente los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento.	ARTÍCULO 21.- Principio de minimización 1. El **R**esponsable tratará únicamente los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento.
ARTÍCULO 22- Principio de ~~calidad~~ 1- El responsable adoptará las medidas necesarias para mantener exactos, completos y actualizados los datos personales en su posesión, de tal manera que no se altere la veracidad de éstos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento. 2- Cuando los datos personales hubieren dejado de ser necesarios para el cumplimiento de las finalidades que motivaron su tratamiento, el responsable los suprimirá o eliminará de sus archivos, registros, bases de datos, expedientes o sistemas de información, o en su caso, los someterá a un procedimiento de anonimización. 3- En la supresión de los datos personales, el responsable implementará métodos y técnicas orientadas a la eliminación definitiva y segura de éstos. 4- Los datos personales únicamente serán conservados durante el plazo necesario para el cumplimiento de las finalidades que justifiquen su tratamiento o aquéllas relacionadas con exigencias legales aplicables al responsable. No obstante, la ley podrá establecer excepciones respecto al plazo de conservación de los datos personales, ~~con pleno respeto a los derechos y garantías del titular.~~	ARTÍCULO 22.- Principio de **exactitud** 1. El **R**esponsable adoptará las medidas necesarias para mantener exactos, completos y actualizados los datos personales en su posesión, de tal manera que no se altere la veracidad de éstos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento **y adoptará todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos.** 2. Cuando los datos personales hubieren dejado de ser necesarios para el cumplimiento de las finalidades que motivaron su tratamiento, el **R**esponsable los suprimirá o eliminará de sus archivos, registros, bases de datos, expedientes o sistemas de información, o en su caso, los someterá a un procedimiento de anonimización. 3. En la supresión de los datos personales, el **R**esponsable implementará métodos y técnicas orientadas a la eliminación definitiva y segura de éstos. 4. Los datos personales únicamente serán conservados durante el plazo necesario para el cumplimiento de las finalidades que justifiquen su tratamiento o aquéllas relacionadas con exigencias legales aplicables al **R**esponsable. **No obstante, el Responsable podrá conservar los datos más allá del plazo de conservación en cumplimiento de un interés legítimo, para el cumplimiento de la finalidad inicial de su tratamiento y con pleno respeto a los derechos y garantías del Titular. Asimismo,** la ley podrá establecer excepciones respecto al plazo de conservación de los datos

	personales**. De igual forma, se entenderán válidas las excepciones contenidas en leyes especiales en materia de archivo, investigación o estadística.**
ARTÍCULO 23- Principio de responsabilidad 1. El responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en esta Ley, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al titular y a la Agencia de Protección de Datos, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines. 2. Lo anterior, aplicará cuando los datos personales sean tratados por parte de un encargado a nombre y por cuenta del responsable, así como al momento de realizar transferencias de datos personales. 3. Entre los mecanismos que el responsable podrá adoptar para cumplir con el principio de responsabilidad se encuentran, de manera enunciativa más no limitativa, los siguientes: a. Destinar recursos para la instrumentación de programas y políticas de protección de datos personales. b. Implementar ~~sistemas de administración~~ de riesgos asociados al tratamiento de datos personales. c. Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable. d. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales. e. Revisar periódicamente las políticas y programas de seguridad de datos	ARTÍCULO 23.- Principio de responsabilidad **proactiva** 1. El **R**esponsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en esta Ley, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al **T**itular y a la Agencia de Protección de Datos, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines. 2. Lo anterior, aplicará cuando los datos personales sean tratados por parte de un **E**ncargado a nombre y por cuenta del **R**esponsable, así como al momento de realizar cesiones o transferencias de datos personales. 3. Entre los mecanismos que el **R**esponsable podrá adoptar para cumplir con el principio de responsabilidad se encuentran, de manera enunciativa más no limitativa, los siguientes: a. Destinar recursos para la instrumentación de programas y políticas de protección de datos personales. b. Implementar **medidas para el análisis** de **los** riesgos asociados al tratamiento de datos personales, **y en caso de que corresponda, evaluaciones de impacto de datos personales.** c. Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del **R**esponsable. d. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales.

personales para determinar las modificaciones que se requieran. f. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales. g. Establecer procedimientos para recibir y responder dudas y quejas de los titulares. 4. El responsable revisará y evaluará permanentemente los mecanismos que para tal afecto adopte voluntariamente para cumplir con el principio de responsabilidad, con el objeto de medir su nivel de eficacia en cuanto al cumplimiento de la legislación nacional aplicable.	e. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran. f. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales. **g.** Establecer procedimientos para recibir y responder dudas y quejas de los **T**itulares **en los plazos establecidos en esta Ley.** **h. Llevar el registro de tratamiento de datos personales, cuando corresponda conforme lo establecido en esta Ley.** **i. Designar un delegado de protección de datos personales cuando sea requerido conforme esta Ley.** 4. El **R**esponsable revisará y evaluará permanentemente los mecanismos que para tal afecto adopte voluntariamente para cumplir con el principio de responsabilidad, con el objeto de medir su nivel de eficacia en cuanto al cumplimiento de la legislación nacional aplicable.
ARTÍCULO 24- Principio de seguridad 1. El responsable establecerá y mantendrá, con independencia del tipo de tratamiento que efectúe, medidas de carácter administrativo, físico y técnico suficientes para ~~garantizar~~ la confidencialidad, integridad y disponibilidad de los datos personales. 2. Para la determinación de las medidas referidas en el numeral anterior, el responsable considerará los siguientes factores: ~~a.~~ El riesgo para los derechos y libertades de los titulares~~, en particular, por el valor potencial cuantitativo y cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.~~ b. El estado de la técnica.	ARTÍCULO 24.- Principio de seguridad 1. El **Responsable y el Encargado** establecerá**n** y mantendrá, con independencia del tipo de tratamiento que efectúe, medidas de carácter administrativo, físico y técnico suficientes para **mantener** la confidencialidad, integridad y disponibilidad de los datos personales. 2. Para la determinación de las medidas referidas en el numeral anterior, el **R**esponsable considerará los siguientes factores: a. El riesgo para los derechos y libertades de los **T**itulares. b. El estado de la técnica. c. Los costos de aplicación.

c. Los costos de aplicación. d. La naturaleza de los datos personales tratados, en especial si se trata de datos personales sensibles. e. El alcance, contexto y las finalidades del tratamiento. f. Las transferencias internacionales de datos personales que se realicen o pretendan realizar. g. El número de titulares. h. Las posibles consecuencias que se derivarían de una ~~vulneración~~ para los titulares. i. Las ~~vulneraciones~~ previas ocurridas en el tratamiento de datos personales.	d. La naturaleza de los datos personales tratados, en especial si se trata de datos personales sensibles. e. El alcance, contexto y las finalidades del tratamiento. f. Las transferencias internacionales de datos personales que se realicen o pretendan realizar. g. El número de **T**itulares. h. Las posibles consecuencias que se derivarían de una **violación de la seguridad de los datos personales para los T**itulares. i. Las **violación de la seguridad de los datos personales** previas ocurridas en el tratamiento de datos personales.
3. El responsable llevará a cabo una serie de acciones que garanticen el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de las medidas de seguridad aplicables al tratamiento de los datos personales, de manera periódica, para garantizar un nivel de seguridad adecuado al riesgo, que podrá incluir entre otros: a. La seudonimización y el cifrado de los datos personales. b. La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resilencia 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. Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.	3. El **R**esponsable llevará a cabo una serie de acciones que garanticen el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de las medidas de seguridad aplicables al tratamiento de los datos personales, de manera periódica, para garantizar un nivel de seguridad adecuado al riesgo, que podrá incluir entre otros: a. La seudonimización y el cifrado de los datos personales. b. La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resilencia 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. Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.
4. El responsable y el encargado del tratamiento tomarán medidas para garantizar	4. El **R**esponsable y el **E**ncargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la

que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud de disposición legal aplicable. 5. Bajo ninguna circunstancia podrá una entidad u órgano de la Administración Pública o del Estado, invocando el ejercicio de potestades públicas o la satisfacción de intereses públicos, desaplicar o limitar el principio de seguridad aquí descrito. ~~6. Sin perjuicio de las obligaciones y medidas impuestas en este artículo, la Agencia de Protección de Datos establecerá un estándar mínimo de ciberseguridad para el sector público, o acordará adoptar alguno ya existente en la materia, el cual será de acatamiento obligatorio para la totalidad de la Administración Pública. El cumplimiento del estándar mínimo no exime a las entidades públicas de su obligación de disponer de mayores medidas de seguridad en función de los criterios establecidos en el inciso 2 de este artículo y del nivel de riesgo aplicable a cada institución. El Reglamento a ésta Ley dispondrá las características, elementos y medidas técnicas, físicas y lógicas de ciberseguridad mínimas que deberán cumplir las entidades públicas, el mecanismo de control que se utilizará para verificar el cumplimiento de dicho estándar, y la periodicidad con que deberá demostrarse dicho cumplimiento.~~	autoridad del **R**esponsable o del **E**ncargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del **R**esponsable, salvo que esté obligada a ello en virtud de disposición legal aplicable. 5. Bajo ninguna circunstancia podrá una entidad u órgano de la Administración Pública o del Estado, invocando el ejercicio de potestades públicas o la satisfacción de intereses públicos, desaplicar o limitar el principio de seguridad aquí descrito.
ARTÍCULO 25- Notificación de ~~vulneraciones~~ a la seguridad de los datos personales 1. Cuando el responsable tenga conocimiento de una ~~vulneración~~ de seguridad de datos personales ocurrida en cualquier fase del tratamiento, entendida como cualquier daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los datos personales, ~~aún~~ cuando ocurra de manera accidental, notificará a la Agencia de Protección de Datos Personales en un plazo de 72 horas, desde que se tuviera conocimiento efectivo ~~y, a los titulares afectados dicho acontecimiento~~, sin dilación alguna. 2. Lo anterior, no resultará aplicable cuando el responsable pueda demostrar, atendiendo al principio de responsabilidad	ARTÍCULO 25.- Notificación de **violación** a la seguridad de los datos personales 1. Cuando el **R**esponsable tenga conocimiento de una **violación** de seguridad de datos personales ocurrida en cualquier fase del tratamiento, entendida como cualquier daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los datos personales, **aun** cuando ocurra de manera accidental, notificará a la Agencia de Protección de Datos Personales **y a los Titulares afectados** en un plazo de 72 horas, desde que se tuviera conocimiento efectivo, sin dilación alguna. 2. Lo anterior, no resultará aplicable cuando el **R**esponsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la

proactiva, la improbabilidad de la ~~vulneración~~ de seguridad ocurrida, o bien, que ésta no represente un riesgo para los derechos y las libertades de los titulares involucrados.	improbabilidad de la **violación** de seguridad ocurrida, o bien, que ésta no represente un riesgo para los derechos y las libertades de los **T**itulares involucrados.
3. La notificación que realice el responsable a los titulares afectados estará redactada en un lenguaje claro y sencillo, posibilitando acreditar el envío de la notificación referida.	3. La notificación que realice el **R**esponsable a los **T**itulares afectados estará redactada en un lenguaje claro y sencillo, posibilitando acreditar el envío de la notificación referida.
4. La notificación a que se refieren los numerales anteriores contendrá, al menos, la siguiente información: a. La naturaleza del incidente. b. Los datos personales comprometidos. c. Las acciones correctivas realizadas de forma inmediata. d. Las recomendaciones al titular sobre las medidas que éste pueda adoptar para proteger sus intereses. e. Los medios ~~disponibles al~~ titular para obtener mayor información al respecto.	4. La notificación a que se refieren los numerales anteriores, t**anto a la Agencia de Protección de Datos como a los Titulares afectados,** contendrá, al menos, la siguiente información: a. La naturaleza del incidente. b. Los datos personales **que pueden considerarse** comprometidos. c. Las acciones correctivas realizadas de forma inmediata. d. Las recomendaciones al **T**itular sobre las medidas que éste pueda adoptar para proteger sus intereses. e. Los medios **a disposición del T**itular para obtener mayor información al respecto.
4. Cuando por la gravedad o naturaleza particular del incidente sea imposible identificar todos los elementos anteriores dentro de las 72 horas establecidas en el inciso primero, el responsable deberá notificar la información de la que tenga conocimiento a ese momento, debiendo ~~completar y notificar el resto de la información indicada en un plazo no mayor a cinco días hábiles desde que haya tenido conocimiento del incidente.~~	4. Cuando por la gravedad o naturaleza particular del incidente sea imposible identificar todos los elementos anteriores dentro de las 72 horas establecidas en el inciso primero, el **R**esponsable deberá notificar la información de la que tenga conocimiento a ese momento, **debiendo presentar actualizaciones periódicas a la Agencia de Protección de Datos Personales sobre el informe inicial, cada vez que se disponga de información nueva o diferente sobre el incidente, hasta la fecha en que la investigación del incidente haya concluido y que el incidente asociado se haya mitigado y resuelto por completo.**
5. El responsable ~~auditará y~~ documentará toda ~~vulneración~~ de seguridad de los datos personales ocurrida en cualquier fase del tratamiento, identificando, de manera enunciativa más no limitativa, la fecha en que ocurrió; el motivo de la ~~vulneración~~; los hechos relacionados con ella y sus efectos y las medidas correctivas implementadas de forma inmediata y definitiva, la cual estará a disposición de la Agencia de Protección de Datos.	5. El **R**esponsable documentará toda **violación** de seguridad de los datos personales ocurrida en cualquier fase del tratamiento, identificando, de manera enunciativa más no limitativa, la fecha en que ocurrió; el motivo de la **violación**; los hechos relacionados con ella y sus efectos y las medidas correctivas implementadas de
6. El reglamento que se dicte a la presente ley establecerá los efectos de las notificaciones	

de ~~vulneraciones~~ de seguridad que realice el responsable a la autoridad de control, en lo que se refiere a los procedimientos, forma y condiciones de su intervención, con el propósito del salvaguardar los intereses, derechos y libertades de los **t**itulares afectados.	forma inmediata y definitiva, la cual estará a disposición de la Agencia de Protección de Datos. 6. El reglamento que se dicte a la presente **L**ey establecerá los efectos de las notificaciones de **violaciones** de seguridad que realice el **R**esponsable a la autoridad de control, en lo que se refiere a los procedimientos, forma y condiciones de su intervención, con el propósito del salvaguardar los intereses, derechos y libertades de los **T**itulares afectados.
ARTÍCULO 26- Principio de confidencialidad 1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad. Este deber será complementario de los deberes de secreto profesional de conformidad con la normativa aplicable. 2. El responsable o encargado establecerán controles o mecanismos para que quienes intervengan en cualquier fase del tratamiento de los datos personales mantengan y respeten la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el titular.	ARTÍCULO 26.- Principio de confidencialidad 1. Los **R**esponsables y **E**ncargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad. Este deber será complementario de los deberes de secreto profesional de conformidad con la normativa aplicable. 2. El **R**esponsable o **E**ncargado establecerán controles o mecanismos para que quienes intervengan en cualquier fase del tratamiento de los datos personales mantengan y respeten la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el **T**itular.
CAPÍTULO III DERECHOS DEL TITULAR	CAPÍTULO III DERECHOS DEL TITULAR
ARTÍCULO 27- Derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) y de portabilidad 1. En todo momento el titular o su representante podrán solicitar al responsable, el acceso, rectificación, cancelación, oposición y portabilidad de los datos personales que le conciernen. 2. El ejercicio de cualquiera de los derechos referidos en el numeral anterior no es requisito previo, ni impide el ejercicio de otro.	ARTÍCULO 27.- Derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) y de portabilidad 1. En todo momento el **T**itular o su representante podrán solicitar al **R**esponsable, el acceso, rectificación, cancelación, oposición y portabilidad de los datos personales que le conciernen. 2. El ejercicio de cualquiera de los derechos referidos en el numeral anterior no es requisito previo, ni impide el ejercicio de otro. **3. Los derechos del Titular son irrenunciables. Será nula de pleno derecho toda estipulación en contrario.**

ARTÍCULO 28- Disposiciones generales sobre ejercicio de los derechos 1. Los derechos reconocidos en ~~en~~ este Capítulo, ~~p~~podrán ejercerse directamente o por medio de representante legal o voluntario, debiendo estar estos debidamente acreditados. Cuando el responsable tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado. 2. El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado. 3. El encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule. 4. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable. 5. En cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de quince años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente Ley. 6. Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos.	ARTÍCULO 28.- Disposiciones generales sobre ejercicio de los derechos 1. Los derechos reconocidos en este Capítulo **se ejercerán por medio escrito, y serán comunicados al Responsable en los medios que hubiese puesto a disposición del Titular, por medio del oficial de protección de datos (de haberlo), o, en su defecto, en su domicilio social o establecimiento comercial abierto al público. Podrán** ejercerse directamente o por medio de representante legal o voluntario, debiendo estar estos debidamente acreditados. Cuando el **R**esponsable tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado. 2. El **R**esponsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado. 3. El **E**ncargado podrá tramitar, por cuenta del **R**esponsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule. 4. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el **Responsable. Salvo que otro plazo se estableciera en esta Ley, la respuesta a una solicitud de ejercicio de derechos por parte de un afectado deberá comunicarse en un plazo de cinco días hábiles posteriores a su recepción, al medio señalado por el afectado.** 5. En cualquier caso, los **T**itulares de la patria potestad podrán ejercitar en nombre y representación de los menores de quince años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente Ley. 6. Serán gratuitas las actuaciones llevadas a cabo por el **R**esponsable del tratamiento para

	atender las solicitudes de ejercicio de estos derechos.
ARTÍCULO 29- Derecho de acceso 1.- El titular tendrá derecho ~~a~~ obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales q~~ue le conciernen~~ y, en tal caso, derecho de acceso a los datos personales y a la siguiente información: a. ~~Los~~ fin~~es~~ del tratamiento. b. Las categorías de datos personales de que se trate. ~~c.~~ Los destinatarios o las categorías de destinatarios a los que se ~~transfirieron~~ o ~~serán transferidos~~ los datos personales, ~~en particular destinatarios en terceros países u organizaciones internacionales.~~ d. ~~De ser posible,~~ el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo. e. La existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al titular, o a oponerse a dicho tratamiento. f. Cuando los datos personales no se hayan obtenido del titular, cualquier información disponible sobre su origen. 2. Cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud. 3. El derecho de acceso se entenderá otorgado si el responsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación	ARTÍCULO 29.- Derecho de acceso 1. El **Titular, previa acreditación de su identidad**, tendrá derecho **de** obtener del **R**esponsable del tratamiento **en el plazo de cinco días hábiles**, confirmación de si se están tratando o no **sus** datos personales, y en tal caso, derecho de acceso **en el mismo plazo indicado** a los datos personales y a la siguiente información: **a. Las** fin**alidades** del tratamiento **y las bases legales que las legitiman.** b. Las categorías de datos personales de que se trate. c. Los destinatarios o las categorías de destinatarios a los que se **cedieron** o **se prevean ceder** los datos personales. **d. Información sobre las transferencias internacionales de datos que se hayan efectuado o se prevean efectuar, incluyendo los países de destino.** **e. El plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo.** **f.** La existencia del derecho a solicitar del **R**esponsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al **T**itular, o a oponerse a dicho tratamiento **o a presentar una reclamación ante la Agencia de Protección de Datos Personales.** g. Cuando los datos personales no se hayan obtenido del **T**itular, cualquier información disponible sobre su origen. **h. La existencia o no de decisiones automatizadas respecto del tratamiento de sus datos personales, incluida la elaboración de perfiles.**

por el responsable al afectado del modo en que este podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho. 4. El responsable ~~del tratamiento~~ facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá ~~percibir~~ por cualquier otra copia solicitada por el titular un canon razonable basado en los costos administrativos. Cuando el titular presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común. 5. Se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello. En dicho caso, el responsable podrá denegar la solicitud por ese motivo hasta que transcurra dicho plazo.	2. Cuando el **R**esponsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el **R**esponsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud. 3. El derecho de acceso se entenderá otorgado si el **R**esponsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por el **R**esponsable al afectado del modo en que este podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho. 4. El **R**esponsable facilitará una copia de los datos personales objeto de tratamiento. El **R**esponsable podrá **cobrar un monto razonable** por cualquier otra copia solicitada por el **T**itular un canon razonable basado en los costos administrativos. Cuando el **T**itular presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común. 5. Se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello. En dicho caso, el **R**esponsable podrá denegar la solicitud por ese motivo hasta que transcurra dicho plazo.
ARTÍCULO 30- Derecho de rectificación 1. El titular tendrá el derecho a obtener del responsable, en el plazo máximo de cinco días hábiles, la rectificación o corrección de sus datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados. Al ejercer este derecho el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.	ARTÍCULO 30.- Derecho de rectificación 1. El **T**itular tendrá el derecho a obtener del **R**esponsable, en el plazo máximo de cinco días hábiles, la rectificación o corrección de sus datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados. Al ejercer este derecho el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.
ARTÍCULO 31- Derecho de cancelación ~~(derecho al olvido)~~	ARTÍCULO 31.- Derecho de cancelación **o supresión**

1. El titular tendrá derecho a obtener del responsable del tratamiento y en el plazo de cinco días hábiles, la cancelación de ~~los~~ datos personales ~~que le conciernan~~, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes: ~~a.~~ Los datos personales ya no sean necesarios en relación con los fines para los que fueron ~~recogidos o tratados de otro modo.~~ b. El titular ~~retire~~ el consentimiento en que se basa el tratamiento, y este no se ~~base en otro fundamento jurídico.~~ ~~c.~~ El titular ~~se oponga al tratamiento~~ con arreglo al artículo 32 ~~apartado 1~~, y no prevalezcan otros motivos legítimos para el tratamiento, ~~o el titular se oponga al tratamiento con arreglo al artículo 32, apartado 2.~~ d. Los datos personales hayan sido tratados ilícitamente. ~~e.~~ Los datos personales deban suprimirse para el cumplimiento de una obligación legal ~~establecida en una ley especial que se aplique al responsable del tratamiento.~~ 2. ~~Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el costo 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 supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.~~ 3. ~~Los~~ apartado~~s~~ 1 y ~~2~~ no se aplicarán cuando el tratamiento sea necesario: a. Para ejercer el derecho a la libertad de expresión e información. b. Para el cumplimiento de una obligación legal que requiera el tratamiento de	1. El **T**itular tendrá derecho a obtener del **R**esponsable del tratamiento y en el plazo de cinco días hábiles, la cancelación de **sus** datos personales, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes: **a.** Los datos personales ya no sean necesarios en relación con los fines para los que fueron **recolectados.** **b.** El **T**itular **revoque** el consentimiento en que se basa el tratamiento, y este no se **ampare en otra base legal.** c. El **T**itular **haya ejercido su derecho de oposición** con arreglo al artículo 32, y no prevalezcan otros motivos legítimos para el tratamiento. d. Los datos personales hayan sido tratados ilícitamente. **e.** Los datos personales deban suprimirse para el cumplimiento de una obligación legal **o por orden de una autoridad competente.** **2. El apartado 1 no se aplicarán cuando el tratamiento sea necesario:** a. Para ejercer el derecho a la libertad de expresión e información. b. Para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por ley especial que se aplique al **R**esponsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al **R**esponsable. c. Por razones de interés público. d. Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento.

datos impuesta por ley especial que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable. ~~c.~~ Por razones de interés público ~~en el ámbito de la salud pública.~~ d. Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento. e. Para la formulación, el ejercicio o la defensa de reclamaciones.	e. Para la formulación, el ejercicio o la defensa de reclamaciones. **f. Cuando los datos personales deban ser conservados durante los plazos previstos en disposiciones legales o contractuales, entre el Responsable o Encargado del tratamiento y el Titular de los datos.**
ARTÍCULO 32- Derecho de oposición 1. El titular podrá oponerse en cualquier momento al tratamiento de sus datos personales, cuando dicho tratamiento se fundamente en las causales de los incisos h) e i) del artículo 15 (1) de esta Ley, cuando: a. Tenga una razón legítima derivada de su situación particular, misma que deberá justificar en su solicitud de oposición. b. El tratamiento de sus datos personales tenga por objeto la mercadotecnia directa, incluida la elaboración de perfiles, en la medida que esté relacionada con dicha actividad. 2. El responsable del tratamiento dejará de tratar los datos personales, salvo que 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. 3. Tratándose del inciso 1 (b) anterior, cuando el titular se oponga al tratamiento con fines de mercadotecnia directa, sus datos personales dejarán de ser tratados para dichos fines.	ARTÍCULO 32.- Derecho de oposición 1. El **T**itular podrá oponerse en cualquier momento al tratamiento de sus datos personales, cuando dicho tratamiento se fundamente en las causales de los incisos h) e i) del artículo 15 (1) de esta Ley, cuando: a. Tenga una razón legítima derivada de su situación particular, misma que deberá justificar en su solicitud de oposición. b. El tratamiento de sus datos personales tenga por objeto la **publicidad, la prospección comercial o la** mercadotecnia directa, incluida la elaboración de perfiles, en la medida que esté relacionada con dicha actividad. 2. El **R**esponsable del tratamiento **deberá responder la solicitud en el plazo máximo de cinco días hábiles, y** dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del **T**itular, o para la formulación, el ejercicio o la defensa de reclamaciones. 3. Tratándose del inciso 1 (b) anterior, cuando el **T**itular se oponga al tratamiento con fines de mercadotecnia directa, sus datos personales dejarán de ser tratados para dichos fines.

ARTÍCULO 33- Derecho a no ser objeto de decisiones individuales automatizadas 1. El titular tendrá derecho a no ser objeto de ~~decisiones~~ que le produzcan efectos jurídicos o ~~le~~ afecten de manera significativa, ~~que se basen únicamente en tratamientos automatizados~~ destinad~~o~~s a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento. 2. Lo dispuesto en el numeral anterior no resultará aplicable cuando el tratamiento automatizado de datos personales sea necesario para la celebración o la ejecución de un contrato entre el titular y el responsable o bien, se base en el consentimiento demostrable del titular. 3. No obstante, cuando el tratamiento automatizado sea necesario para la relación contractual o el titular hubiere manifestado su consentimiento, éste tendrá derecho a obtener una intervención humana significativa; recibir una explicación sobre la decisión tomada; expresar su punto de vista e impugnar la decisión. 4. El responsable no podrá llevar a cabo tratamientos automatizados de datos personales que tengan como efecto la discriminación de los titulares ~~por su origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, género, así como datos genéticos o datos biométricos.~~	ARTÍCULO 33.- Derecho a no ser objeto de decisiones individuales automatizadas 1. El **T**itular tendrá derecho a no ser objeto de **una decisión basada en el tratamiento automatizado de datos, incluida la elaboración de perfiles**, que le produzca efectos jurídicos o afecten **sus intereses** de manera significativa, destinad**a**s a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica **o crediticia**, estado de salud, preferencias sexuales, fiabilidad o comportamiento. 2. Lo dispuesto en el numeral anterior no resultará aplicable cuando el tratamiento automatizado de datos personales sea necesario para la celebración o la ejecución de un contrato entre el **T**itular y el **R**esponsable o bien, se base en el consentimiento demostrable del **T**itular. 3. No obstante, cuando el tratamiento automatizado sea necesario para la relación contractual o el **T**itular hubiere manifestado su consentimiento, éste tendrá derecho a obtener una intervención humana significativa; recibir una explicación sobre la decisión tomada, **siempre que no se revelen con dicha explicación secretos comerciales; así como** expresar su punto de vista e impugnar la decisión. 4. El **R**esponsable no podrá llevar a cabo tratamientos automatizados de datos personales que tengan como efecto la discriminación de los **T**itulares, **particularmente cuando se basen en datos sensibles, según son definidos en esta Ley.**
ARTÍCULO 34- Derecho a la portabilidad de los datos personales 1. Cuando se traten datos personales por vía electrónica o medios automatizados, el titular tendrá derecho a obtener una copia de los datos personales que hubiere proporcionado al responsable o que sean objeto de tratamiento, en un formato electrónico estructurado, de uso común y lectura mecánica, que le permita seguir utilizándolos y transferirlos a otro responsable, en caso de que lo requiera.	ARTÍCULO 34.- Derecho a la portabilidad de los datos personales 1. Cuando se traten datos personales por vía electrónica o medios automatizados, el **T**itular tendrá derecho a obtener una copia de los datos personales que hubiere proporcionado al **R**esponsable o que sean objeto de tratamiento, en un formato electrónico estructurado, de uso común y lectura mecánica, que le permita seguir utilizándolos y transferirlos a otro **R**esponsable, en caso de que lo requiera.

2. El titular podrá solicitar que sus datos personales se transfieran directamente de responsable a responsable cuando sea técnicamente posible. 3. El derecho a la portabilidad de los datos personales no afectará negativamente a los derechos y libertades de otros. 4. Sin perjuicio de otros derechos del titular, el derecho a la portabilidad de los datos personales no resultará procedente cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.	2. El **T**itular podrá solicitar al **R**esponsable que sus datos personales se transfieran directamente de **R**esponsable a **R**esponsable cuando sea técnicamente posible. 3. El derecho a la portabilidad de los datos personales no afectará negativamente a los derechos y libertades de otros. 4. Sin perjuicio de otros derechos del **T**itular, el derecho a la portabilidad de los datos personales no resultará procedente cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el **R**esponsable con base en los datos personales proporcionados por el **T**itular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.
ARTÍCULO 35- Derecho a la limitación del tratamiento de los datos personales 1. El titular tendrá derecho a que el tratamiento de datos personales se limite a su almacenamiento durante el periodo que medie entre una solicitud de rectificación u oposición hasta su resolución por el responsable. 2. El titular tendrá derecho a la limitación del tratamiento de sus datos personales cuando éstos sean innecesarios para el responsable, pero los necesite para formular una reclamación.	ARTÍCULO 35.- Derecho a la limitación del tratamiento de los datos personales 1. El **T**itular tendrá derecho a que el tratamiento de datos personales se limite a su almacenamiento durante el periodo que medie entre una solicitud de rectificación u oposición hasta su resolución por el **R**esponsable. 2. El **T**itular tendrá derecho a la limitación del tratamiento de sus datos personales cuando éstos sean innecesarios para el **R**esponsable, pero los necesite para formular una reclamación.
ARTÍCULO 36- Ejercicio de los derechos ARCO y de portabilidad 1. El responsable establecerá medios y procedimientos sencillos, expeditos, accesibles y gratuitos que permitan al titular ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad. 2. ~~Por vía reglamentaria se establecerán los requerimientos, plazos, términos y condiciones en que los titulares podrán ejercer sus~~ derechos de acceso, rectificación, cancelación, oposición y portabilidad, ~~así como las causales de improcedencia al ejercicio de los mismos como podrían ser, de manera enunciativa más no limitativa~~:	ARTÍCULO 36.- Ejercicio de los derechos ARCO y de portabilidad 1. El **R**esponsable establecerá medios y procedimientos sencillos, expeditos, accesibles y gratuitos que permitan al **T**itular ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad. 2. **Será improcedente el ejercicio de los** derechos de acceso, rectificación, cancelación, oposición y portabilidad **en los siguientes casos:** a. Cuando el tratamiento sea necesario para el cumplimiento de un objetivo importante de interés público.

a. Cuando el tratamiento sea necesario para el cumplimiento de un objetivo importante de interés público. b. Cuando el tratamiento sea necesario para el ejercicio de las funciones propias de las autoridades públicas. c. Cuando el responsable acredite tener motivos legítimos para que el tratamiento prevalezca sobre los intereses, los derechos y las libertades del titular. d. Cuando el tratamiento sea necesario para el cumplimiento de una disposición legal. e. Cuando los datos personales sean necesarios para el mantenimiento o cumplimiento de una relación jurídica o contractual. 3. Cuando las solicitudes de ejercicio de derechos sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable podrá: a. Cobrar un ~~canon~~ razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada. b. Negarse a actuar respecto de la solicitud. 4. En todo caso, el responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.	b. Cuando el tratamiento sea necesario para el ejercicio de las funciones propias de las autoridades públicas **expresamente establecidas en la ley.** c. Cuando el **R**esponsable acredite tener motivos legítimos para que el tratamiento prevalezca sobre los intereses, los derechos y las libertades del **T**itular. d. Cuando el tratamiento sea necesario para el cumplimiento de una disposición legal. e. Cuando los datos personales sean necesarios para el mantenimiento o cumplimiento de una relación jurídica o contractual. 3. Cuando las solicitudes de ejercicio de derechos sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el **R**esponsable podrá: a. Cobrar un **cargo** razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada. b. Negarse a actuar respecto de la solicitud. 4. En todo caso, el **R**esponsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.
CAPÍTULO IV RESPONSABLE Y ENCARGADO DEL TRATAMIENTO	CAPÍTULO IV RESPONSABLE Y ENCARGADO DEL TRATAMIENTO
ARTÍCULO 37- Obligaciones ~~generales~~ del responsable ~~y encargado~~ del tratamiento ~~1- Los responsables y encargados determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con la presente ley y sus normas de desarrollo. En particular valorarán si procede~~	ARTÍCULO 37.- Obligaciones del **R**esponsable del tratamiento **1. Los Responsables del tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente Ley, sus normas reglamentarias y otras que rijan su actividad:**

~~la realización de la evaluación de impacto en la protección de datos a que se refiere el artículo 51 de esta Ley.~~ 2- Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos: a. Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados. b. Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales. c. Cuando se produjese el tratamiento no meramente incidental o accesorio de datos sensibles, en los términos que son definidos en esta Ley, o de los datos relacionados con la comisión de infracciones administrativas. d. Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos. e. Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.	**a. Implementar medidas apropiadas, útiles, oportunas, pertinentes y eficaces para garantizar y poder demostrar el adecuado cumplimiento de la presente Ley y sus normas reglamentarias, especialmente los derechos de los Titulares y la materialización de los principios del tratamiento de datos personales;** **b. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de protección de datos, especialmente conocer, actualizar, rectificar, suprimir sus datos personales u oponerse al tratamiento de los mismos;** **c. Cumplir debidamente con el deber de informar al Titular sobre la finalidad de la recolección y sus derechos;** **d. Tratar los datos personales bajo condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;** **e. Implementar medidas para garantizar que los datos personales sean veraces, actualizados, completos, exactos y comprobables;** **f. Actualizar los datos personales, rectificar la información cuando sea incorrecta y adoptar medidas necesarias para que la misma se mantenga actualizada;** **g. Tramitar debidamente las solicitudes presentadas por el Titular, respondiéndolas de manera completa y oportunamente;** **h. Realizar la notificación de violaciones de seguridad en los términos y plazos previstos en esta Ley.** **i. Cumplir las instrucciones, órdenes o requerimientos que imparta la Agencia de Protección de Datos Personales.** **j. Formalizar mediante la suscripción de un acuerdo, contrato o cualquier otro instrumento jurídico la prestación de servicios entre el Responsable y el Encargado, en entre corresponsables.** **k. Verificar que los Encargados, o quienes**

f. Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales. g. Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección por parte de la Agencia de Protección de Datos. h. Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.	**éstos subcontraten, ofrecen garantías suficientes para realizar el tratamiento de datos personales conforme con los requisitos de la presente Ley y garantice la protección de los derechos del Titular. Dicha verificación debe realizarse con anterioridad a la contratación u realización de otro acto jurídico que lo vincule con el Encargado;** **l. Exigir al Encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y debido tratamiento de la información del Titular;** 2. Para la adopción de las medidas a que se refiere el apartado anterior los **R**esponsables del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos: a. Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados. b. Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales. c. Cuando se produjese el tratamiento no meramente incidental o accesorio de datos sensibles, en los términos que son definidos en esta Ley, o de los datos relacionados con la comisión de infracciones administrativas. d. Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su

	solvencia financiera, su localización o sus movimientos. e. Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad. f. Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales. g. Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección por parte de la Agencia de Protección de Datos. h. Cualesquiera otros que a juicio del **R**esponsable o del **E**ncargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.
ARTÍCULO 38- Corresponsables del tratamiento 1.- Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por la presente Ley, atendiendo a las actividades que efectivamente desarrolle cada uno de los corresponsables del tratamiento, en particular en cuanto al ejercicio de los derechos del titular y a sus respectivas obligaciones de transparencia a que se refiere el artículo 19 de esta Ley. Dicho acuerdo podrá designar un punto de contacto para los titulares. 2. El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los titulares. Se pondrán a	ARTÍCULO 38.- Corresponsables del tratamiento 1. Cuando dos o más **R**esponsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por la presente Ley, atendiendo a las actividades que efectivamente desarrolle cada uno de los corresponsables del tratamiento, en particular en cuanto al ejercicio de los derechos del **T**itular y a sus respectivas obligaciones de transparencia a que se refiere el artículo 19 de esta Ley. Dicho acuerdo podrá designar un punto de contacto para los **T**itulares. 2. El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los **T**itulares. Se pondrán a disposición del **T**itular los aspectos esenciales del acuerdo.

disposición del titular los aspectos esenciales del acuerdo. 3. Independientemente de los términos del acuerdo a que se refiere el apartado 1, los titulares podrán ejercer los derechos que les reconoce la presente Ley frente a, y en contra de, cada uno de los responsables.	3. Independientemente de los términos del acuerdo a que se refiere el apartado 1, los **T**itulares podrán ejercer los derechos que les reconoce la presente Ley frente a, y en contra de, cada uno de los **R**esponsables.
ARTÍCULO 39- ~~Comunicaciones o~~ cesiones de datos 1- Los datos de carácter personal objeto del tratamiento sólo podrán ser ~~comunicados~~ a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario ~~con el previo consentimiento del interesado.~~ 2- ~~El consentimiento exigido en el apartado anterior no será preciso:~~ ~~a. Cuando la cesión está autorizada en una ley.~~ ~~b. Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con bases de datos de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.~~ ~~c. Cuando la comunicación que deba efectuarse tenga por destinatario al Ministerio Público, los Tribunales de Justicia o a la Contraloría General de la República, en el ejercicio de las funciones que tiene atribuidas.~~ ~~d. Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. Las cesiones entre administraciones públicas que impliquen transferencia de datos personales, seguirán las reglas establecidas en el artículo 8 de la presente Ley.~~	ARTÍCULO 39.- Cesión de datos 1. Los datos de carácter personal objeto del tratamiento sólo podrán ser **cedidos** a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, **en alguno de los supuestos previstos en el artículo 15.1 de esta Ley, y siempre que dicha cesión sea informada al Titular.** **2.** Aquel a quien se **cedan** los datos personal**es** se obliga, por el solo hecho de la cesión, a la observancia de las disposiciones de la presente Ley, **y a facilitar al Titular de los datos personales cedidos la siguiente información, dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos:** **a) la identidad y los datos de contacto del Responsable y, en su caso, de su representante;** **b) los datos de contacto del delegado de protección de datos, en su caso;** **c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;** **d) las categorías de datos personales de que se trate;** **e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;** **f) en su caso, la intención del Responsable de transferir datos personales a un destinatario en un tercer país.**

~~e. Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a una base de datos o para realizar los estudios epidemiológicos en los términos establecidos en la legislación nacional sobre sanidad y salud pública.~~ ~~3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar.~~ ~~4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.~~ ~~5.~~ Aquel a quien se ~~comuniquen~~ los datos de carácter personal se obliga, por el solo hecho de la ~~comunicación,~~ a la observancia de las disposiciones de la presente Ley.	**3. Las disposiciones del apartado anterior no serán aplicables cuando y en la medida en que:** **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. En tales casos, el Responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del Titular;** **c) la obtención o la comunicación esté expresamente establecida en una ley, o;** **d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional emanada en una norma de carácter legal.**
ARTÍCULO 40- Encargado de tratamiento 1. El encargado realizará las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido del mismo, así como limitará sus actuaciones a los términos fijados por el responsable. 2. El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará transferencia de datos siempre que se cumpla lo establecido en la presente Ley y en sus normas de desarrollo. 3. Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los ~~afectados~~ aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo siguiente. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público. Tendrá asimismo la consideración de responsable del	ARTÍCULO 40.- Encargado de tratamiento 1. El **E**ncargado realizará las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido del mismo, así como limitará sus actuaciones a los términos fijados por el **R**esponsable. 2. El acceso por parte de un **E**ncargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al **R**esponsable no se considerará **cesión ni** transferencia de datos siempre que se cumpla lo establecido en la presente Ley y en sus normas de desarrollo. 3. Tendrá la consideración de **R**esponsable del tratamiento y no la de **E**ncargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los **Titulares** aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo siguiente. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público. Tendrá asimismo la consideración de

tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades. 4. El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado. No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista. 5.- El encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento. 6.- En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración Pública, ~~las municipalidades o instituciones descentralizadas,~~ siempre que sea mediante la adopción de un~~a norma reguladora de dichas competencias~~, que deberá incorporar el contenido exigido por el artículo siguiente.	**R**esponsable del tratamiento quien figurando como **E**ncargado utilizase los datos para sus propias finalidades. 4. El **R**esponsable del tratamiento determinará si, cuando finalice la prestación de los servicios del **E**ncargado, los datos personales deben ser destruidos, devueltos al **R**esponsable o entregados, en su caso, a un nuevo **E**ncargado. No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al **R**esponsable, que garantizará su conservación mientras tal obligación persista. 5. El **E**ncargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el **R**esponsable del tratamiento. 6. En el ámbito del sector público podrán atribuirse las competencias propias de un **E**ncargado del tratamiento a un determinado órgano de la Administración Pública, siempre que sea mediante la adopción de un **acto administrativo** que deberá incorporar el contenido exigido por el artículo siguiente.
ARTÍCULO 41- Formalización de la prestación de servicios del encargado 1. La prestación de servicios entre el responsable y encargado se formalizará mediante la suscripción de un contrato de encargo. 2. El contrato de encargo 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 encargado. 3. El contrato o instrumento jurídico establecerá, al menos, las siguientes cláusulas generales relacionadas con los servicios que preste el encargado:	ARTÍCULO 41.- Formalización de la prestación de servicios del **E**ncargado 1. La prestación de servicios entre el **R**esponsable y **E**ncargado se formalizará mediante la suscripción de un contrato de encargo~~, cuya formalización será responsabilidad del Responsable~~. 2. El contrato de encargo establecerá, al menos, el objeto, alcance, contenido, duración, naturaleza y finalidad del tratamiento; el tipo de datos personales; las categorías de **T**itulares, así como las obligaciones y responsabilidades del **R**esponsable y **E**ncargado. 3. El contrato o instrumento jurídico establecerá, al menos, las siguientes cláusulas generales relacionadas con los servicios que preste el Encargado:

a. Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable. b. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. c. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables. d. Informar al responsable cuando ocurra una ~~vulneración a~~ los datos personales que trata por sus instrucciones. e. Informar al responsable cuando un titular ejercite sus derechos en materia de protección de datos a través del encargado. f. Guardar confidencialidad respecto de los datos personales tratados. g. Suprimir, devolver o comunicar a un nuevo encargado designado por el responsable los datos personales objeto de tratamiento, una vez cumplida la relación jurídica con el responsable o por instrucciones de éste, excepto que una disposición legal exija la conservación de los datos personales, o bien, que el responsable autorice la comunicación de éstos a otro encargado. h. Abstenerse de transferir los datos personales, salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad de control. i. Permitir al responsable o autoridad de control inspecciones y verificaciones en sitio. Estas verificaciones podrán hacerse a través de las certificaciones de seguridad de la información con las que cuente el encargado. j. Generar, actualizar y conservar la documentación que sea necesaria y que le permita acreditar sus obligaciones.	a. Realizar el tratamiento de los datos personales conforme a las instrucciones del **R**esponsable. b. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el **R**esponsable. c. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables. d. Informar **sin dilación alguna** al **R**esponsable cuando ocurra una **violación de la seguridad de** los datos personales que trata por sus instrucciones. e. Informar **sin dilación alguna** al **R**esponsable cuando un **T**itular ejercite sus derechos en materia de protección de datos a través del **E**ncargado. **f.** Guardar confidencialidad respecto de los datos personales tratados **y garantizar que su personal y cualquier persona autorizada por el Encargado para tratar datos personales del Responsable cuenten con obligaciones contractuales o derivadas de una obligación legal que les obliguen a respetar la confidencialidad de los datos personales tratados.** g. Suprimir, devolver o comunicar a un nuevo **E**ncargado designado por el **R**esponsable los datos personales objeto de tratamiento, una vez cumplida la relación jurídica con el **R**esponsable o por instrucciones de éste, excepto que una disposición legal exija la conservación de los datos personales, o bien, que el **R**esponsable autorice la comunicación de éstos a otro **E**ncargado. h. Abstenerse de transferir los datos personales, salvo en el caso de que el **R**esponsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad de control.

k. Colaborar con el responsable en todo lo relativo al cumplimiento de la legislación aplicable en la materia. 4. Cuando el encargado incumpla las instrucciones del responsable y decida por sí mismo sobre el alcance, contenido, medios y demás cuestiones del tratamiento de los datos personales asumirá la calidad de responsable.	i. Permitir al **R**esponsable o autoridad de control inspecciones y verificaciones en sitio. Estas verificaciones podrán hacerse a través de las certificaciones de seguridad de la información con las que cuente el **E**ncargado. j. Generar, actualizar y conservar la documentación que sea necesaria y que le permita acreditar sus obligaciones. **k.** Colaborar con el **R**esponsable en todo lo relativo al cumplimiento de la legislación aplicable en la materia**, así como facilitar la información necesaria para demostrar el cumplimiento de las obligaciones en el presente artículo, sea en el marco de una auditoría realizada al Responsable, de un procedimiento de fiscalización por una autoridad competente o cuando dicha obligación derive del contrato de encargo.** 4. Cuando el **E**ncargado incumpla las instrucciones del **R**esponsable y decida por sí mismo sobre el alcance, contenido, medios y demás cuestiones del tratamiento de los datos personales asumirá la calidad de **R**esponsable.
ARTÍCULO 42- Subcontratación de servicios 1. El encargado podrá, a su vez, subcontratar servicios que impliquen el tratamiento de datos personales, siempre y cuando exista una autorización previa por escrito, específica o general del responsable, o bien, se estipule expresamente en el contrato o instrumento jurídico suscrito entre este último y el encargado. 2. El subcontratado asumirá el carácter de encargado. 3. El encargado formalizará la prestación de servicios del subcontratado a través de un contrato, debiendo aportar las garantías recogidas en el artículo 41 de la presente ley. 4. Cuando el subcontratado incumpla sus obligaciones y responsabilidades respecto al tratamiento de datos personales que lleve a	ARTÍCULO 42.- Subcontratación de servicios 1. El **E**ncargado podrá, a su vez, subcontratar servicios que impliquen el tratamiento de datos personales, siempre y cuando exista una autorización previa por escrito, específica o general del **R**esponsable, o bien, se estipule expresamente en el contrato o instrumento jurídico suscrito entre este último y el **E**ncargado. 2. El subcontratado asumirá el carácter de **E**ncargado. 3. El **E**ncargado formalizará la prestación de servicios del subcontratado a través de un contrato, debiendo aportar las garantías recogidas en el artículo 41 de la presente **L**ey. 4. Cuando el subcontratado incumpla sus obligaciones y responsabilidades respecto al tratamiento de datos personales que lleve a

cabo conforme a lo instruido por el encargado, asumirá la calidad de responsable.	cabo conforme a lo instruido por el **E**ncargado, asumirá la calidad de **R**esponsable.
ARTÍCULO 43- Registro de actividades de tratamiento 1. Cada responsable llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación: a. El nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del oficial de protección de datos. b. Los fines del tratamiento. c. Una descripción de las categorías de titulares y de las categorías de datos personales. d. Las categorías de destinatarios a quienes se ~~transfirieron~~ o ~~transferirán~~ los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales. ~~e.~~ En su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional ~~y, en el caso de las transferencias indicadas en el artículo 44, apartado 1, inciso d), la documentación de garantías adecuadas.~~ f. Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos. g. Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 24. 2. Cada encargado llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:	ARTÍCULO 43.- Registro de actividades de tratamiento 1. Cada **R**esponsable llevará un registro de las actividades de tratamiento **de datos personales** efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación: a. El nombre y los datos de contacto del **R**esponsable y, en su caso, del corresponsable, del representante del **R**esponsable, y del oficial de protección de datos. b. Los fines del tratamiento. c. Una descripción de las categorías de **T**itulares y de las categorías de datos personales. d. Las categorías de destinatarios a quienes se **cedieron** o **cederán** los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales. e. En su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional. f. Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos. g. Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 24. 2. Cada **E**ncargado llevará un registro de todas las categorías de actividades de tratamiento **de datos personales** efectuadas por cuenta de un **R**esponsable que contenga: a. El nombre y los datos de contacto del **E**ncargado o **E**ncargados y de cada **R**esponsable por cuenta del cual actúe

a. El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y del oficial de protección de datos, de haberlo. ~~b. Las categorías de tratamientos efectuados por cuenta de cada responsable.~~ c. En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional. d. Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 24. 3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico. 4. El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la Agencia de Protección de Datos cuando ésta lo solicite. 5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 50 personas ~~o~~ se encuentre registrada y al día como PYME ante el Ministerio de Economía Industria y Comercio, ~~,~~ a menos que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los titulares, no sea ocasional, o incluya datos sensibles.	el **E**ncargado, y del oficial de protección de datos, de haberlo. b. En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional. c. Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 24. 3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico. 4. El **R**esponsable o el **E**ncargado del tratamiento y, en su caso, el representante del **R**esponsable o del **E**ncargado pondrán el registro a disposición de la Agencia de Protección de Datos cuando ésta lo solicite. 5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 50 personas **y** se encuentre registrada y al día como PYME ante el Ministerio de Economía Industria y Comercio, a menos que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los **T**itulares, no sea ocasional, o incluya datos sensibles.
ARTÍCULO 44- Bloqueo de los datos 1. El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión. 2. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y	ARTÍCULO 44.- Bloqueo de los datos 1. El **R**esponsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión. 2. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando 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, el Ministerio Público o las Administraciones Públicas competentes, en particular de la Agencia de Protección de Datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas. Transcurrido ese plazo deberá procederse a la destrucción de los datos. 3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior. 4. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo. 5. La Agencia de Protección de Datos podrá fijar excepciones a la obligación de bloqueo establecida en este artículo, en los supuestos en que, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente elevado de afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los afectados, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el responsable del tratamiento.	tribunales, el Ministerio Público o las Administraciones Públicas competentes, en particular de la Agencia de Protección de Datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas. Transcurrido ese plazo deberá procederse a la destrucción de los datos. 3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior. 4. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo. 5. La Agencia de Protección de Datos podrá fijar excepciones a la obligación de bloqueo establecida en este artículo, en los supuestos en que, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente elevado de afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los afectados, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el **R**esponsable del tratamiento.
CAPÍTULO V TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES	CAPÍTULO V TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES
ARTÍCULO 45- Reglas generales para las transferencias internacionales de datos personales 1. Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional, si el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las	ARTÍCULO 45.- Reglas generales para las transferencias internacionales de datos personales 1. **Regla general sobre transferencias internacionales de datos:** Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional, si el **R**esponsable y el **E**ncargado del tratamiento cumplen las condiciones

transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán e interpretarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por la presente Ley no se vea menoscabado.	establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán e interpretarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por la presente Ley no se vea menoscabado.
2. El responsable y encargado podrán realizar transferencias internacionales de datos personales en cualquiera de los siguientes supuestos: a. Cuando el responsable cuente con el consentimiento informado del titular de los datos. b. Cuando la transferencia sea exigida legalmente o en un tratado internacional del que la República de Costa Rica sea parte~~, para la investigación y persecución de los delitos, así como la administración de justicia o por razones de seguridad nacional.~~ c. Cuando el país, parte de su territorio, sector, actividad u organización internacional destinatario de los datos personales hubiere sido reconocido con un nivel adecuado de protección de datos personales por parte de la Agencia de Protección de Datos, o bien, el país destinatario acredite condiciones mínimas y suficientes para garantizar un nivel de protección de datos personales adecuado. d. Cuando el exportador ofrezca garantías suficientes del tratamiento de los datos personales en el país destinatario, y acredite el cumplimiento de ~~las~~ condiciones mínimas y ~~suficientes aplicables a la materia.~~ Se considerarán como garantías suficientes las siguientes: i) Que el exportador y destinatario suscriban cláusulas contractuales o cualquier otro instrumento jurídico que ofrezca garantías suficientes del cumplimiento de la presente Ley y que permita demostrar el alcance del tratamiento de los datos personales, las	2. **Casos en los que la transferencia internacional de datos es procedente:** El **R**esponsable y **E**ncargado podrán realizar transferencias internacionales de datos personales en cualquiera de los siguientes supuestos: a. **Consentimiento del Titular:** Cuando el **R**esponsable cuente con el consentimiento informado del **T**itular de los datos. b. **Transferencia fundamentada en un tratado internacional:** Cuando la transferencia sea exigida legalmente o en un tratado internacional del que la República de Costa Rica sea parte. c. **Transferencia fundamentada en una decisión de adecuación:** Cuando el país, parte de su territorio, sector, actividad u organización internacional destinatario de los datos personales hubiere sido reconocido con un nivel adecuado de protección de datos personales por parte de la Agencia de Protección de Datos, o bien, el país destinatario acredite condiciones mínimas y suficientes para garantizar un nivel de protección de datos personales adecuado**, que no podrán ser menores que las reconocidas en la presente Ley**. d. **Transferencias fundamentadas en garantías adecuadas del exportador:** Cuando el exportador ofrezca garantías suficientes del tratamiento de los datos personales en el país destinatario, y acredite el cumplimiento de condiciones mínimas **suficientes, derechos exigibles y el acceso a acciones legales efectivas.** Se considerarán como garantías suficientes **el**

obligaciones y responsabilidades asumidas por las partes y los derechos de los titulares. ii) Que el exportador y destinatario adopten un esquema de autorregulación vinculante, normas corporativas vinculantes o un mecanismo de certificación, siempre y cuando ~~éste~~ sea acorde con las disposiciones previstas en esta Ley. ~~e. Que se encuentre prevista en una ley o tratado internacional del que la República de Costa Rica sea parte.~~ 3. En todos los casos de transferencias regidas por el presente artículo, el acuerdo o mecanismo que instrumente la transferencia, deberá asegurar que el importador de los datos personales se encuentre sujeto a la jurisdicción de una o varias autoridades de supervisión independientes -tales como una autoridad de protección de datos y los tribunales que pudieran resultar competentes en el país de destino- de manera que los titulares ~~o interesados~~ cuenten con acciones legales efectivas -administrativas y judiciales- para proteger sus derechos. Asimismo, el acuerdo o mecanismo que instrumente la transferencia deberá reconocer que la parte exportadora se encuentra sujeta a la jurisdicción de la Agencia de Protección de Datos y de los tribunales de Costa Rica que resulten competentes.	**cumplimiento de alguna de** las siguientes: i) Que el exportador y destinatario suscriban cláusulas contractuales o cualquier otro instrumento jurídico que ofrezca garantías suficientes del cumplimiento de la presente Ley y que permita demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes y los **principios y** derechos de los **T**itulares. ii) Que el exportador y destinatario adopten un esquema de autorregulación vinculante, normas corporativas vinculantes**, código de conducta** o un mecanismo de certificación **local o internacionalmente reconocidos,** siempre y cuando **estos** sea**n** acorde con las disposiciones previstas en esta Ley. **3.** En todos los casos de transferencias regidas por el presente artículo, el acuerdo o mecanismo que instrumente la transferencia, deberá asegurar que el importador de los datos personales se encuentre sujeto a la jurisdicción de una o varias autoridades de supervisión independientes -tales como una autoridad de protección de datos y los tribunales que pudieran resultar competentes en el país de destino- de manera que los **T**itulares cuenten con acciones legales efectivas -administrativas y judiciales- para proteger sus derechos. Asimismo, el acuerdo o mecanismo que instrumente la transferencia deberá reconocer que la parte exportadora se encuentra sujeta a la jurisdicción de la Agencia de Protección de Datos y de los tribunales de Costa Rica que resulten competentes. **4. Cuando el Titular de forma libre, voluntaria y por su propia iniciativa, transfiera sus datos a un Responsable situado en una jurisdicción diferente a la del Titular.**
CAPÍTULO VI MEDIDAS PROACTIVAS EN EL TRATAMIENTO DE DATOS PERSONALES	CAPÍTULO VI MEDIDAS PROACTIVAS EN EL TRATAMIENTO DE DATOS PERSONALES
ARTÍCULO 46- Reconocimiento de medidas proactivas 1- Se establecen como medidas que promueven el mejor cumplimiento de la legislación y que coadyuvan a fortalecer y elevar los controles de protección de datos	ARTÍCULO 46.- Reconocimiento de medidas proactivas 1. Se establecen como medidas que promueven el mejor cumplimiento de la legislación y que coadyuvan a fortalecer y elevar los controles de protección de datos personales implementados

personales implementados por el responsable, las que a continuación se indican en el presente Capítulo.	por el **R**esponsable, las que a continuación se indican en el presente Capítulo.
ARTÍCULO 47- Privacidad por diseño y privacidad por defecto 1. El responsable aplicará, desde el diseño, en la determinación de los medios del tratamiento de los datos personales, durante el mismo y antes de recabar los datos personales, medidas preventivas de diversa naturaleza que permitan aplicar de forma efectiva los principios, derechos y demás obligaciones previstas en esta Ley. 2. El responsable garantizará que sus programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen un tratamiento de datos personales, cumplan por defecto o se ajusten a los principios, derechos y demás obligaciones previstas en esta Ley. Específicamente, con el fin de que únicamente sean objeto de tratamiento el mínimo de datos personales y se limite la accesibilidad de éstos, sin la intervención del titular, a un número indeterminado de personas.	ARTÍCULO 47.- Privacidad por diseño y privacidad por defecto 1. **Teniendo en cuenta el estado de la técnica, el costo de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entrañe el tratamiento de los datos para los derechos y libertades de los Titulares, el R**esponsable aplicará, desde el diseño, en la determinación de los medios del tratamiento de los datos personales, durante el mismo y antes de recabar los datos personales, medidas preventivas de diversa naturaleza que permitan aplicar de forma efectiva los principios, derechos y demás obligaciones previstas en esta Ley. 2. El **R**esponsable garantizará que sus programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen un tratamiento de datos personales, cumplan por defecto o se ajusten a los principios, derechos y demás obligaciones previstas en esta Ley. Específicamente, con el fin de que únicamente sean objeto de tratamiento el mínimo de datos personales y se limite la accesibilidad de éstos, sin la intervención del **T**itular, a un número indeterminado de personas.
ARTÍCULO 48- Oficial de protección de datos personales 1. El responsable designará a un oficial de protección de datos personales cuando se trate de las siguientes entidades: a. Instituciones públicas de la administración central o descentralizada. b. El Poder Judicial y el Tribunal Supremo de Elecciones. c. Colegios profesionales. d. Empresas de seguridad privada.	ARTÍCULO 48.- Oficial de protección de datos personales 1. El **R**esponsable designará a un oficial de protección de datos personales cuando se trate de las siguientes entidades: a. Instituciones públicas de la administración central o descentralizada. b. El Poder Judicial, **la Asamblea Legislativa** y el Tribunal Supremo de Elecciones. c. Colegios profesionales. d. Empresas de seguridad privada. e. Los centros sanitarios que mantengan historias clínicas de los pacientes, exceptuando los profesionales de la

e. Los centros sanitarios que mantengan historias clínicas de los pacientes, exceptuando los profesionales de la salud que, aun manteniendo historias clínicas, ejerzan su actividad a título individual. f. Entidades bancarias y financieras, sujetas a la regulación de la Superintendencia General de Entidades Financieras. g. Las entidades responsables de bases de datos de evaluación de solvencia patrimonial y crédito. h. Los responsables que lleven a cabo tratamientos de datos personales que tengan por objeto una observación habitual y sistemática de la conducta del titular. i. Los responsables que realicen tratamientos de datos personales donde sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, considerando, entre otros factores y de manera enunciativa más no limitativa, las categorías de datos personales tratados, en especial cuando se trate de datos sensibles; las transferencias que se efectúen; el número de titulares; el alcance del tratamiento; las tecnologías de información utilizadas o las finalidades de éstos. 2. El responsable que no se encuentre en alguna de las causales previstas en el numeral anterior, podrá designar a un oficial de protección de datos personales si así lo estima conveniente. 3. Los responsables deberán ~~informar en un plazo de diez días naturales a la Agencia de Protección de Datos las designaciones, nombramientos y ceses de los oficiales de protección de datos tanto en los supuestos en que se encuentren obligados a su designación como en el caso en que sea voluntaria.~~ 4. Los oficiales de protección de datos podrán ejercer su función a tiempo completo o parcial, dependiendo del volumen de tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los titulares. El oficial de protección de datos podrá ser una persona física o jurídica, interna o externa a la	salud que, aun manteniendo historias clínicas, ejerzan su actividad a título individual. **f.** Entidades bancarias y financieras, sujetas a la regulación de la Superintendencia General de Entidades Financieras**, de acuerdo a las regulaciones sectoriales que se dicten.** g. Las entidades **R**esponsables de bases de datos de evaluación de solvencia patrimonial y crédito. h. Los **R**esponsables o **E**ncargados que lleven a cabo tratamientos de datos personales que tengan por objeto una observación habitual y sistemática de la conducta del **T**itular. i. Los **R**esponsables o **E**ncargados que realicen tratamientos de datos personales donde sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los **T**itulares, considerando, entre otros factores y de manera enunciativa más no limitativa, las categorías de datos personales tratados, en especial cuando se trate de datos sensibles; las transferencias que se efectúen; el número de **T**itulares; el alcance del tratamiento; las tecnologías de información utilizadas o las finalidades de éstos. 2. El **R**esponsable que no se encuentre en alguna de las causales previstas en el numeral anterior, podrá designar a un oficial de protección de datos personales si así lo estima conveniente. 3. Los **R**esponsables **que designen un oficial de protección de datos, sea por mandato legal o de forma voluntaria,** deberán **poner a disposición del Titular sus datos de contacto en cualquier aviso o política de privacidad de la que disponga.** 4. Los oficiales de protección de datos podrán ejercer su función a tiempo completo o parcial, dependiendo del volumen de tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los **T**itulares**, y siempre que las otras funciones que desempeñen no den lugar a un conflicto de interés.** El oficial de protección de datos

organización, y deberá acreditar conocimientos especializados en el derecho y la práctica de protección de datos. ~~La Agencia de Protección de Datos mantendrá una lista actualizada de los oficiales de protección de datos que será accesible por medios electrónicos.~~	podrá ser una persona física o jurídica, interna o externa a la organización, y deberá acreditar conocimientos especializados en el derecho y la práctica de protección de datos.
5. El responsable estará obligado a respaldar al oficial de protección de datos personales en el desempeño de sus funciones, facilitándole los recursos necesarios para su desempeño y para el mantenimiento de sus conocimientos especializados y la actualización de éstos.	5. El **R**esponsable **o el Encargado** estará**n** obligado**s** a respaldar al oficial de protección de datos personales en el desempeño de sus funciones, facilitándole los recursos necesarios para su desempeño y para el mantenimiento de sus conocimientos especializados y la actualización de éstos.
6. El oficial de protección de datos personales tendrá, al menos, las siguientes funciones: a. Asesorar al responsable respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales. b. Coordinar, al interior de la organización del responsable, las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la legislación aplicable en la materia. c. Supervisar al interior de la organización del responsable el cumplimiento de la legislación aplicable en la materia.	6. El oficial de protección de datos personales tendrá, al menos, las siguientes funciones: a. **Informar y asesorar** al **R**esponsable **o el Encargado** respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales. b. Coordinar, al interior de la organización del **R**esponsable, las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la legislación aplicable en la materia. **c.** Supervisar al interior de la organización del **Responsable y del Encargado** el cumplimiento de la legislación aplicable en la materia **y de sus políticas.**
7. Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el oficial de protección de datos no podrá ser removido ni sancionado por el responsable por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del oficial de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.	7. Cuando se trate de una persona física integrada en la organización del **R**esponsable o **E**ncargado del tratamiento, el oficial de protección de datos no podrá ser removido ni sancionado por el **R**esponsable por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del oficial de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.
8. En el ejercicio de sus funciones el oficial de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable la existencia de cualquier deber de confidencialidad o secreto.	8. En el ejercicio de sus funciones el oficial de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el **Responsable o el Encargado** la existencia de cualquier deber de confidencialidad o secreto.

9. Cuando el oficial de protección de datos ~~aprecie~~ la existencia de una ~~vulneración relevante~~ en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable.	9. Cuando el oficial de protección de datos **tenga conocimiento de la** existencia de una **violación de seguridad** en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del **Responsable o Encargado.** **10. El oficial de protección de datos personales estará obligado por el secreto profesional y el deber de confidencialidad en lo que respecta al desempeño de sus funciones establecidas en esta Ley.**
ARTÍCULO 49- Intervención del oficial de protección de datos en caso de reclamación ante la Agencia de Protección de Datos 1. Cuando el responsable hubiera designado un oficial de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquel ante la Agencia de Protección de Datos, dirigirse al oficial de protección de datos de la entidad contra la que se reclame. En este caso, el oficial de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de ~~dos meses~~ a contar desde la recepción de la reclamación. 2. Cuando el afectado presente una reclamación ante la Agencia de Protección de Datos esta podrá remitir la reclamación al oficial de protección de datos a fin de que este responda en el plazo de ~~un mes~~. Si transcurrido dicho plazo el oficial de protección de datos no hubiera comunicado a la Agencia de Protección de Datos la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento con arreglo a lo establecido en esta Ley y en sus normas de desarrollo.	ARTÍCULO 49.- Intervención del oficial de protección de datos en caso de reclamación ante la Agencia de Protección de Datos 1. Cuando el **R**esponsable **o Encargado** hubiera designado un oficial de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquel ante la Agencia de Protección de Datos, dirigirse al oficial de protección de datos de la entidad contra la que se reclame. En este caso, el oficial de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de **cinco días hábiles** a contar desde la recepción de la reclamación. 2. Cuando el afectado presente una reclamación ante la Agencia de Protección de Datos esta podrá remitir la reclamación al oficial de protección de datos a fin de que este responda en el plazo de **cinco días hábiles.** Si transcurrido dicho plazo el oficial de protección de datos no hubiera comunicado a la Agencia de Protección de Datos la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento con arreglo a lo establecido en esta Ley y en sus normas de desarrollo.
ARTÍCULO 50- Mecanismos de autorregulación 1. El responsable podrá adherirse, de manera voluntaria, a esquemas de autorregulación vinculante, que tengan por objeto, entre otros, contribuir a la correcta	ARTÍCULO 50.- Mecanismos de autorregulación 1. El **R**esponsable **y el Encargado** podrá**n** adherirse, de manera voluntaria, a esquemas de autorregulación vinculante, que tengan por objeto, entre otros, contribuir a la correcta

aplicación de esta Ley y establecer procedimientos de resolución de conflictos entre el responsable y titular, teniendo en cuenta las características específicas de los tratamientos de datos personales realizados, así como el efectivo ejercicio y respeto de los derechos del titular. 2. Para los efectos del numeral anterior, se podrán desarrollar, entre otros, códigos deontológicos y sistemas de certificación y sus respectivos sellos de confianza que coadyuven a contribuir a los objetivos señalados en el presente numeral. 3. La Agencia de Protección de Datos establecerá las reglas que correspondan para la validación, confirmación o reconocimiento de los mecanismos de autorregulación ~~aludidos~~.	aplicación de esta Ley y establecer procedimientos de resolución de conflictos entre el **R**esponsable y **T**itular, teniendo en cuenta las características específicas de los tratamientos de datos personales realizados, así como el efectivo ejercicio y respeto de los derechos del **T**itular. 2. Para los efectos del numeral anterior, se podrán desarrollar, entre otros, códigos deontológicos y sistemas de certificación y sus respectivos sellos de confianza que coadyuven a contribuir a los objetivos señalados en el presente numeral. 3. La Agencia de Protección de Datos establecerá las reglas que correspondan para la validación, confirmación o reconocimiento de los mecanismos de autorregulación **elaborados por las asociaciones y otras organizaciones, nacionales o internacionales, de alcance general o sectoriales**.
ARTÍCULO 51- Evaluación de impacto a la protección de datos personales 1.- Cuando el responsable pretenda llevar a cabo un tipo de tratamiento de datos personales que, por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, realizará, de manera previa a la implementación del mismo, una evaluación del impacto a la protección de los datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares. 2. El responsable del tratamiento recabará el asesoramiento del oficial de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos. 3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de: a. Evaluación sistemática y exhaustiva de aspectos personales de personas	ARTÍCULO 51.- Evaluación de impacto a la protección de datos personales 1. Cuando el **R**esponsable pretenda llevar a cabo un tipo de tratamiento de datos personales que, por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los **T**itulares, realizará, de manera previa a la implementación del mismo, una evaluación del impacto a la protección de los datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares. 2. El **R**esponsable del tratamiento recabará el asesoramiento del oficial de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos. 3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de: a. Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento

físicas 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 físicas 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. 4. La Agencia de Protección de Datos ~~podrá~~ promulgar una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos, asimismo podrá establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. 5. La evaluación de impacto deberá incluir como mínimo: a. Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento. b. Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad. c. Una evaluación de los riesgos para los derechos y libertades de los titulares a que se refiere el apartado 1. d. Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con la presente Ley, teniendo en cuenta los derechos e intereses legítimos de los titulares y de otras personas afectadas.	automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; **b.** Tratamiento a gran escala de datos sensibles **o relativos a condenas e infracciones penales previstos en esta Ley.** c. Observación sistemática a gran escala de una zona de acceso público. 4. La Agencia de Protección de Datos **deberá** promulgar una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos, asimismo podrá establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. 5. La evaluación de impacto deberá incluir como mínimo: a. Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el **R**esponsable del tratamiento. b. Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad. c. Una evaluación de los riesgos para los derechos y libertades de los **T**itulares a que se refiere el apartado 1. d. Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con la presente Ley, teniendo en cuenta los derechos e intereses legítimos de los **T**itulares y de otras personas afectadas. **6.** El **R**esponsable consultará a la Agencia de Protección de Datos antes de proceder al

6. ~~Cuando proceda, el responsable podrá recabar la opinión de los titulares o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.~~ 7. El responsable consultará a la Agencia de Protección de Datos antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos pusiera de manifiesto que existe un alto riesgo si el responsable no toma medidas para para mitigarlo. Cuando la Agencia de Protección de Datos considere que el tratamiento previsto podría infringir la normativa vigente en materia de protección de datos, o cuando el responsable no haya identificado o mitigado suficientemente el riesgo, podrá, en un plazo de dos meses desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado. Dicho plazo podrá prorrogarse dos meses, en función de la complejidad del tratamiento previsto. La ~~autoridad de control~~ informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la ~~autoridad de control~~ haya obtenido la información solicitada a los fines de la consulta.	tratamiento cuando una evaluación de impacto relativa a la protección de los datos pusiera de manifiesto que existe un alto riesgo si el **R**esponsable no toma medidas para para mitigarlo. Cuando la Agencia de Protección de Datos considere que el tratamiento previsto podría infringir la normativa vigente en materia de protección de datos, o cuando el **R**esponsable no haya identificado o mitigado suficientemente el riesgo, podrá, en un plazo de dos meses desde la solicitud de la consulta, asesorar por escrito al **R**esponsable, y en su caso al **E**ncargado. Dicho plazo podrá prorrogarse dos meses, en función de la complejidad del tratamiento previsto. La **Agencia de Protección de Datos** informará al **R**esponsable y, en su caso, al **E**ncargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la **Agencia de Protección de Datos** haya obtenido la información solicitada a los fines de la consulta.
CAPÍTULO VII DISPOSICIONES APLICABLES A TRATAMIENTOS CONCRETOS	CAPÍTULO VII DISPOSICIONES APLICABLES A TRATAMIENTOS CONCRETOS
ARTÍCULO 52- Tratamientos con fines de videovigilancia 1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones. 2. Solo podrán captarse imágenes de la vía pública en la medida en que resulte	ARTÍCULO 52.- Tratamientos con fines de videovigilancia 1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones. 2. Solo podrán captarse imágenes de la vía pública en la medida en que resulte

imprescindible para la finalidad mencionada en el apartado anterior. No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio o bien privado. 3. Los datos serán suprimidos en el plazo máximo de dos meses desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación. 4. El deber de información previsto en el artículo 19 de esta Ley se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en el artículo 27 de esta Ley. El responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el artículo 19 antes citado. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información. 5. Al amparo del artículo 4.2.a) de la presente Ley, se considera excluido de su ámbito de aplicación el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio. Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes. 6. Se excluye de esta disposición el tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por parte de cuerpos de policía y	imprescindible para la finalidad mencionada en el apartado anterior. No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio o bien privado. 3. Los datos serán suprimidos en el plazo máximo de dos meses desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación. 4. El deber de información previsto en el artículo 19 de esta Ley se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del **R**esponsable y la posibilidad de ejercitar los derechos previstos en el artículo 27 de esta Ley. El **R**esponsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el artículo 19 antes citado. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información. 5. Al amparo del artículo 4.2.a) de la presente Ley, se considera excluido de su ámbito de aplicación el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio. Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes. 6. Se excluye de esta disposición el tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por parte de cuerpos de policía y por los órganos competentes para la vigilancia y control en los

por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. 7. El tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo siguiente. 8. Se prohíbe~~, sin excepción,~~ el uso de sistemas de identificación biométrica en tiempo real en espacios públicos ~~para cualquier finalidad, especialmente fines policiales o de investigación criminal.~~	centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. 7. El tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo siguiente. 8. Se prohíbe el uso de sistemas de identificación biométrica en tiempo real en espacios públicos **a través de cámaras o sistemas de videovigilancia que tengan por finalidad la identificación indiscriminada o masiva de las personas.**
ARTÍCULO 53- Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo 1.- Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores ~~o los empleados~~ público~~s~~, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos acerca de esta medida. En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores ~~o los empleados públicos~~ se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 52.4 de esta Ley. 2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores ~~o los empleados~~ público~~s~~, tales como vestuarios, servicios sanitarios, comedores y análogos.	ARTÍCULO 53.- Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo 1. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores **del sector** público **o privado**, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos acerca de esta medida. En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores **del sector público o privado,** se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 52.4 de esta Ley. 2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores **del sector** público **o privado,** tales como vestuarios, servicios sanitarios, **salas de lactancia**, comedores y análogos.

3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores.	3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores.
ARTÍCULO 54- Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral 1. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores ~~o los empleados~~ público~~s~~ previstas, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. 2. Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores ~~o los empleados~~ público~~s~~ y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.	ARTÍCULO 54.- Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral 1. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores **del sector** público **o privado** previstas, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. 2. Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores **del sector** público **o privado** y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.
ARTÍCULO 55- ~~Sistemas y proveedores de información crediticia~~ ~~Los datos personales relativos al comportamiento crediticio contenidos en el Centro de Información Crediticia así como el funcionamiento y reglas relacionadas con los sistemas o proveedores de información crediticia se regirán por las normas que regulan el Sistema Financiero Nacional y las que al respecto dicte la Superintendencia General de Entidades Financieras (SUGEF), de modo que el acceso a dichos datos permita a las entidades financieras y de crédito valorar el nivel de riesgo de crédito de sus clientes, sin comprometer las garantías, principios y derechos concedidos en esta Ley en una medida mayor a la~~	ARTÍCULO 55.- **Datos relativos al comportamiento crediticio del sector financiero y no financiero** **1. Los datos personales relativos al comportamiento crediticio tratados por el Centro de Información Crediticia (CIC) se regirán por las normas dictadas por la Superintendencia General de Entidades Financieras, de modo que el acceso a dichos datos permita a las entidades financieras y de crédito valorar el nivel de riesgo de crédito de sus clientes, respetando las garantías, principios y derechos concedidos en esta Ley. Esto sin perjuicio del tratamiento que sobre datos crediticios puedan hacer otros Responsables del sector**

~~estrictamente necesaria para cumplir la finalidad indicada.~~	**no financiero, en los términos indicados en el presente artículo.** **2. Queda expresamente autorizado el tratamiento de datos personales destinado a informar sobre la solvencia patrimonial o crediticia, incluyendo aquellos datos relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial y/o crediticio que permitan evaluar los riesgos de contratación, la conducta comercial y/o la capacidad de pago del Titular. Lo anterior, en los casos en que dichos datos personales sean obtenidos de fuentes de acceso público, y/o procedentes de informaciones facilitadas por el acreedor con base en su interés legítimo prevalente, o en las circunstancias previstas en la presente Ley.** **3. Cuando se realice una cesión de datos personales para el fin indicado en el párrafo anterior, el acreedor, en calidad de Responsable de los datos, deberá mantener un registro del Titular de los datos cedidos, que podrá ser requerido por la Agencia de Protección de Datos en el marco de una investigación o procedimiento sancionatorio.** **4. Los datos personales relativos al comportamiento crediticio que sean significativos para evaluar la solvencia económica o financiera podrán tratarse hasta por cuatro años, desde el vencimiento del plazo original de la operación de crédito. El plazo se reduce a dos años cuando el deudor cancele o extinga la obligación, plazo a contar a partir de la fecha en que lo hace, debiendo constar esta información en el informe crediticio.** **5. Cuando se cancele una obligación incumplida registrada en una base de datos de solvencia, o exista una orden judicial o administrativa que así lo ordene, el acreedor de la obligación deberá en un plazo máximo de cinco días hábiles de acontecido el hecho, comunicarlo al Responsable de la base de datos de solvencia. Una vez recibida la comunicación por el Responsable de la base de datos de solvencia, éste dispondrá de un plazo máximo de tres días hábiles para proceder a la actualización del dato,**

	asentando su nueva situación en el informe crediticio. **6. Los Responsables de las bases de datos sobre solvencia o insolvencia patrimonial deberán en todo momento velar por realizar valoraciones objetivas de la información, sin que esta pueda prestarse para ningún tipo de discriminación. Dichas condiciones serán supervisadas por la Agencia de Protección de Datos.**
ARTÍCULO 56- Tratamiento de datos en la investigación en salud 1. El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios: a. El titular o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica, en los términos previstos en la Ley 9234 Ley Reguladora de Investigación Biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora. ~~b. Las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública.~~ c. Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial. En tales casos, los responsables deberán publicar la información establecida en el artículo 19 de la presente Ley, en un lugar fácilmente accesible de la página web corporativa de la institución donde se	ARTÍCULO 56.- Tratamiento de datos en la investigación en salud 1. El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios: a. El **T**itular o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica, en los términos previstos en la Ley 9234 Ley Reguladora de Investigación Biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora. b. Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial. En tales casos, los **R**esponsables deberán publicar la información establecida en el artículo 19 de la presente Ley, en un lugar fácilmente accesible de la página web corporativa de la institución donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato.

realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato.	c. Se considera lícito el uso de datos personales anonimizados con fines de investigación en salud y, en particular, biomédica. El uso de datos personales anonimizados con fines de investigación en salud pública y biomédica requerirá: a) Una separación técnica y funcional entre el equipo investigador y quienes realicen la anonimización y conserven la información que posibilite la reidentificación. b) Que los datos anonimizados únicamente sean accesibles al equipo de investigación cuando:
d. Se considera lícito el uso de datos personales anonimizados con fines de investigación en salud y, en particular, biomédica. El uso de datos personales anonimizados con fines de investigación en salud pública y biomédica requerirá: a) Una separación técnica y funcional entre el equipo investigador y quienes realicen la anonimización y conserven la información que posibilite la reidentificación. b) Que los datos anonimizados únicamente sean accesibles al equipo de investigación cuando:	
i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.	i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.
ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados. Sólo podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.	ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados. Sólo podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.
~~e. Cuando se traten datos personales con fines de investigación en salud, y en particular la biomédica, podrán excepcionarse los derechos de los titulares previstos en los artículos 29, 30, 32 y 35 de esta Ley cuando:~~	d. Cuando se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a:
~~i) Los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados.~~	i) Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 51 de esta Ley. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización de los datos. ii) Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica. iii) Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.

~~ii) El ejercicio de tales derechos se refiera a los resultados de la investigación.~~ ~~iii) La investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley.~~ f. Cuando se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a: i) Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 51 de esta Ley. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización de los datos. ii) Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica. iii) Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados. iv) Designar un representante legal establecido en la República de Costa Rica, si el promotor de un ensayo clínico no está establecido en el territorio nacional. g. El uso de datos personales anonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité ~~de~~ étic~~a~~ de la investigación previsto en la ~~legislación~~. En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del oficial de protección de datos o, en su defecto, de un experto con los conocimientos en protección de datos personales.	iv) **Para que responda por el cumplimiento de las obligaciones derivadas de esta Ley, designar** un representante legal establecido en la República de Costa Rica, si el promotor de un ensayo clínico no está establecido en el territorio nacional. e. El uso de datos personales anonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité étic**o** de la investigación previsto en la **Ley 9234 Ley Reguladora de Investigación Biomédica**. En defecto de la existencia del mencionado Comité, la entidad **R**esponsable de la investigación requerirá informe previo del oficial de protección de datos o, en su defecto, de un experto con los conocimientos en protección de datos personales.
ARTÍCULO 57- Utilización de medios tecnológicos y datos personales en las actividades electorales	ARTÍCULO 57.- Utilización de medios tecnológicos y datos personales en las actividades electorales

1. El tratamiento de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales deberá respetar lo indicado en el artículo 11 de la presente Ley. 2. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial. 3. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral. 4. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición.	1. El tratamiento de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales deberá respetar lo indicado en el artículo 11 de la presente Ley. 2. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial. 3. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral. 4. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición.
ARTÍCULO 58- Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos 1. Cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias de su número de cédula de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse. 2. Cuando se trate de la notificación por medio de edictos, se identificará al afectado exclusivamente mediante el número completo de su cédula de identidad, número de identidad de extranjero, pasaporte o documento equivalente. 3. Cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos. En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.	ARTÍCULO 58.- Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos 1. Cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias de su número de cédula de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse. 2. Cuando se trate de la notificación por medio de edictos, se identificará al afectado exclusivamente mediante el número completo de su cédula de identidad, número de identidad de extranjero, pasaporte o documento equivalente. 3. Cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos. En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

ARTÍCULO 59- Derecho de rectificación en Internet 1.- Toda persona tiene derecho a la libertad de expresión en Internet. 2.- Los responsables de redes sociales y servicios equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio del derecho de rectificación ante los usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz.	ARTÍCULO 59- Derecho de rectificación en Internet 1.- Toda persona tiene derecho a la libertad de expresión en Internet. 2.- Los responsables de redes sociales y servicios equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio del derecho de rectificación ante los usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz.
ARTÍCULO 60- Tratamiento de datos de contacto de empresarios individuales y profesionales liberales 1. Salvo prueba en contrario, se presumirá amparado en lo dispuesto en el artículo 15.1.i) el tratamiento de los datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica siempre que se cumplan los siguientes requisitos: a. Que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional. b. Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios. 2. La misma presunción operará para el tratamiento de los datos relativos a los empresarios individuales y a los profesionales liberales, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas físicas. 3. Los responsables o encargados del tratamiento a los que se refiere el artículo 79 de esta Ley podrán también tratar los datos mencionados en los dos apartados anteriores cuando ello se derive de una obligación legal o sea necesario para el ejercicio de sus competencias.	ARTÍCULO 60.- Tratamiento de datos de contacto de empresarios individuales y profesionales liberales 1. Salvo prueba en contrario, se presumirá amparado en lo dispuesto en el artículo 15.1.i) el tratamiento de los datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica siempre que se cumplan los siguientes requisitos: a. Que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional. b. Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios. 2. La misma presunción operará para el tratamiento de los datos relativos a los empresarios individuales y a los profesionales liberales, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas físicas. 3. Los **R**esponsables o **E**ncargados del tratamiento a los que se refiere el artículo 79 de esta Ley podrán también tratar los datos mencionados en los dos apartados anteriores cuando ello se derive de una obligación legal o sea necesario para el ejercicio de sus competencias.

CAPÍTULO VIII AGENCIA DE PROTECCIÓN DE DATOS	CAPÍTULO VIII AGENCIA DE PROTECCIÓN DE DATOS
ARTÍCULO 61- Disposiciones generales 1. La Agencia de Protección de Datos Personales~~, será~~ un órgano ~~adscrito al~~ Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Micitt). Contará con grado de desconcentración máxima, con idoneidad especial y técnica, dotada de independencia operativa, técnica, administrativa, presupuestaria y funcional, y la potestad legalmente otorgada de dictar reglamentaciones específicas a la presente Ley, en la materia de su especialidad. Para garantizar la calidad e idoneidad de su personal, contará con los profesionales y técnicos que requiera en las materias de su competencia, incluidas personas científicas de datos y expertas en informática, ciberseguridad, entre otros, los cuales estarán sujetos a lo dispuesto por la ~~Ley 2, Código de Trabajo, de 27 de agosto de 1943~~. Su organización se definirá reglamentariamente, pero ajustará sus actuaciones a las disposiciones contenidas en esta ley. La adquisición de bienes y servicios que realice la Agencia de Protección de Datos deberá ajustarse a la Ley ~~7494~~, Ley de Contratación ~~Administrativa~~, de 2 de mayo de ~~1995~~ y su reglamento. 2. Contará con personalidad jurídica instrumental, por lo que tiene permitido celebrar todo tipo de contratos y convenios con entidades públicas o privadas, tanto a nivel nacional como internacional. Su competencia también abarca facultades plenas para conocer y resolver, ya sea por medio de denuncias o de oficio, así como sancionar, en caso de decidirlo discrecionalmente, toda conducta material o formal que configure una violación de los derechos de las personas a la protección de sus datos personales, en los términos establecidos en esta Ley y sus normas de desarrollo. 3. Sus decisiones darán por agotada la vía administrativa, sin que pudieran impugnarse las resoluciones ni ser avocadas sus competencias.	ARTÍCULO 61.- Disposiciones generales 1. La Agencia de Protección de Datos Personales **es la autoridad nacional de control encargada de la regulación y protección de los datos personales de los habitantes de la República.** **2. Será** un órgano **desconcentrado del** Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Micitt). Contará con grado de desconcentración máxima, con idoneidad especial y técnica, dotada de independencia operativa, técnica, administrativa, presupuestaria y funcional, y la potestad legalmente otorgada de dictar reglamentaciones específicas a la presente Ley, en la materia de su especialidad. Para garantizar la calidad e idoneidad de su personal, contará con los profesionales y técnicos que requiera en las materias de su competencia, incluidas personas científicas de datos y expertas en informática, ciberseguridad, entre otros, los cuales estarán sujetos a lo dispuesto por la **Ley Marco de Empleo Público, No. 10.159.** Su organización se definirá reglamentariamente, pero ajustará sus actuaciones a las disposiciones contenidas en esta **L**ey. La adquisición de bienes y servicios que realice la Agencia de Protección de Datos deberá ajustarse a la Ley **9986**, Ley **General** de Contratación **Pública**, del 2**7** de mayo de **2021** y su reglamento. 2. Contará con personalidad jurídica instrumental, por lo que tiene permitido celebrar todo tipo de contratos y convenios con entidades públicas o privadas, tanto a nivel nacional como internacional. Su competencia también abarca facultades plenas para conocer y resolver, ya sea por medio de denuncias o de oficio, así como sancionar, en caso de decidirlo discrecionalmente, toda conducta material o formal que configure una violación de los derechos de las personas a la protección de sus datos personales, en los términos establecidos en esta Ley y sus normas de desarrollo.

	3. Sus decisiones darán por agotada la vía administrativa, sin que pudieran impugnarse las resoluciones **ante el Micitt** ni ser avocadas sus competencias **por este.**
ARTÍCULO 62- Régimen económico presupuestario 1. El presupuesto de la Agencia de Protección de Datos estará constituido por: a. Una transferencia procedente del presupuesto nacional de la República, que corresponda al menos a cinco mil trescientos nueve coma cero cinco (5 309,05) salarios base, en concordancia con la normativa dispuesta en la Ley N.° 9635, Fortalecimiento de las Finanzas Públicas, de 3 de diciembre de 2018. La Dirección elaborará el presupuesto de la Agencia de Protección de Datos y lo remitirá al jerarca del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, para su incorporación dentro del presupuesto de esta cartera ministerial, de conformidad con lo dispuesto en la Ley N.° 9524, Fortalecimiento del Control Presupuestario de los Órganos Desconcentrados del Gobierno Central, de 7 de marzo de 2018. b. Las donaciones y las subvenciones provenientes de otros Estados, entidades públicas u organismos internacionales, que no comprometen la independencia y la transparencia de la Agencia de Protección de Datos. No se aceptarán donaciones de empresas que se dediquen a la comercialización de datos personales. c. Los ingresos por el cobro de sanciones producto del régimen sancionador previsto en esta Ley. 2. El funcionamiento ordinario de la Agencia de Protección de Datos, así como su presupuesto, estarán sujetos a la fiscalización de la Contraloría General de la República y de la auditoría interna del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, según las competencias establecidas en la normativa vigente.	ARTÍCULO 62.- Régimen económico presupuestario 1. El presupuesto de la Agencia de Protección de Datos estará constituido por: **a.** Una transferencia procedente del presupuesto nacional de la República, que corresponda al menos a cinco mil trescientos nueve coma cero cinco (5 309,05) salarios base, en concordancia con la normativa dispuesta en la Ley N.° 9635, Fortalecimiento de las Finanzas Públicas, de 3 de diciembre de 2018. La Dirección elaborará el presupuesto de la Agencia de Protección de Datos y lo remitirá al jerarca del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, para su incorporación dentro del presupuesto de esta cartera ministerial, de conformidad con lo dispuesto en la Ley N.° 9524, Fortalecimiento del Control Presupuestario de los Órganos Desconcentrados del Gobierno Central, de 7 de marzo de 2018. **La denominación salario base utilizada en esta Ley debe entenderse como la contenida en el artículo 2 de la Ley No. 7337 de 5 de mayo de 1993.** **b.** Las donaciones y las subvenciones provenientes de otros Estados, entidades públicas u organismos internacionales, que no comprometen la independencia y la transparencia de la Agencia de Protección de Datos, **en los términos que establezca el reglamento a esta Ley.** No se aceptarán donaciones de empresas que se dediquen a la comercialización de datos personales**, sean nacionales o internacionales.** c. Los ingresos por el cobro de sanciones producto del régimen sancionador previsto en esta Ley.

3. El o la jerarca del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones no tendrá injerencia en la asignación y ejecución del presupuesto de la Agencia de Protección de Datos Personales. 4. Se autoriza a las instituciones del Estado y entidades públicas estatales, así como a organismos nacionales e internacionales para que efectúen donaciones o aportes a la Agencia de Protección de Datos Personales y le asignen temporalmente el personal calificado para cumplir sus fines y ejecutar proyectos específicos.	2. El funcionamiento ordinario de la Agencia de Protección de Datos, así como su presupuesto, estarán sujetos a la fiscalización de la Contraloría General de la República y de la auditoría interna del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, según las competencias establecidas en la normativa vigente. 3. El o la jerarca del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones no tendrá injerencia en la asignación y ejecución del presupuesto de la Agencia de Protección de Datos Personales. 4. Se autoriza a las instituciones del Estado y entidades públicas estatales, así como a organismos nacionales e internacionales para que efectúen donaciones o aportes a la Agencia de Protección de Datos Personales y le asignen temporalmente el personal calificado para cumplir sus fines y ejecutar proyectos específicos.
ARTÍCULO 63- Funciones La Agencia de Protección de Datos tendrá las siguientes funciones: a. Supervisar la aplicación de esta ley y sus normas de desarrollo. b. Promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos de acuerdo con el tratamiento de los datos. Las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención. c. ~~Asesorar~~ a la Asamblea Legislativa, al Poder Ejecutivo y otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y las libertades de las personas físicas con respecto al tratamiento. d. Promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben. e. Previa solicitud, facilitar información a cualquier titular, en relación con el	ARTÍCULO 63.- Funciones La Agencia de Protección de Datos tendrá las siguientes funciones: a. Supervisar la aplicación de esta **L**ey y sus normas de desarrollo. b. Promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos de acuerdo con el tratamiento de los datos. Las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención. c. **Emitir criterio** a la Asamblea Legislativa, al Poder Ejecutivo y otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y las libertades de las personas físicas con respecto al tratamiento. d. Promover la sensibilización de los **Resp**onsables y **E**ncargados del

ejercicio de sus derechos y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados.	tratamiento acerca de las obligaciones que les incumben.
~~f. Resolver las reclamaciones presentadas por un titular o un organismo, organización o asociación. Investigar el motivo de la reclamación~~ e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable,~~ en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control.~~	e. Previa solicitud, facilitar información a cualquier **T**itular, en relación con el ejercicio de sus derechos y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados. f. **Investigar, resolver y sancionar, de oficio o a ante denuncia, cualquier infracción atribuida a una persona física o jurídica, del sector público o privado,** e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable.
g. Cooperar, en particular compartiendo información, con otras autoridades de control y prestar asistencia mutua, con el fin de garantizar la coherencia a la hora de aplicar y ejecutar las normativas en materia de protección de datos.	g. Cooperar, en particular compartiendo información, con otras autoridades de control y prestar asistencia mutua, con el fin de garantizar la coherencia a la hora de aplicar y ejecutar las normativas en materia de protección de datos.
h. Llevar a cabo investigaciones sobre la aplicación de la normativa nacional en materia de protección de datos, en particular cuando se basa en la información recibida de otra autoridad de control u otra autoridad.	h. Llevar a cabo investigaciones sobre la aplicación de la normativa nacional en materia de protección de datos, en particular cuando se basa en la información recibida de otra autoridad de control u otra autoridad.
i. Efectuar un seguimiento de cambios que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales.	i. Efectuar un seguimiento de cambios que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales.
j. Fomentar el uso de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos.	j. Fomentar el uso de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos.
k. Ser el organismo competente para la protección de las personas físicas en lo relativo al tratamiento de datos personales derivado de la aplicación de cualquier convenio internacional en el que sea parte la República de Costa Rica que atribuya a una autoridad nacional de control esa competencia.	k. Ser el organismo competente para la protección de las personas físicas en lo relativo al tratamiento de datos personales derivado de la aplicación de cualquier convenio internacional en el que sea parte la República de Costa

	Rica que atribuya a una autoridad nacional de control esa competencia. **l. Emitir dictámenes no vinculantes a solicitud de interesados, con el objeto de brindar criterios generales sobre el cumplimiento de las obligaciones y ejercicio de derechos contemplados en esta Ley y los reglamentos que la desarrollen.** **m. Gestionar y administrar sus recursos y presupuesto, para lo que podrá aprobar los contratos de obras y servicios, de acuerdo con el ordenamiento jurídico vigente.**
ARTÍCULO 64- Potestades 1. Para llevar a cabo las funciones de investigación, la Agencia de Protección de Datos podrá: a. Ordenar al responsable y al encargado del tratamiento, sea organismo público o privado, que faciliten cualquier información requerida para el desempeño de sus funciones. b. Llevar a cabo investigaciones en forma de auditorías de protección de datos. c. Notificar al responsable o al encargado del tratamiento las presuntas infracciones en materia de protección de datos, y, transcurridos los procedimientos respectivos, aplicar las sanciones previstas en esta Ley. d. Obtener del responsable y el encargado del tratamiento, el acceso a todos los datos personales y toda la información necesaria para el ejercicio de sus funciones. e. Efectuar inspecciones, físicas o virtuales, a todos los locales del responsable y el encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de lo cual levantará un acta que cumpla las formalidades previstas en el artículo 270 de la Ley General de la Administración Pública.	ARTÍCULO 64.- Potestades 1. Para llevar a cabo las funciones de investigación, la Agencia de Protección de Datos podrá: a. Ordenar al **R**esponsable y al **E**ncargado del tratamiento, sea organismo público o privado, que faciliten cualquier información requerida para el desempeño de sus funciones. b. Llevar a cabo investigaciones en forma de auditorías de protección de datos. c. Notificar al **R**esponsable o al **E**ncargado del tratamiento las presuntas infracciones en materia de protección de datos, y, transcurridos los procedimientos respectivos, aplicar las sanciones previstas en esta Ley. d. Obtener del **R**esponsable y el **E**ncargado del tratamiento, el acceso a todos los datos personales y toda la información necesaria para el ejercicio de sus funciones. e. Efectuar inspecciones, físicas o virtuales, a todos los locales del **R**esponsable y el **E**ncargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de lo cual levantará un acta que cumpla las formalidades previstas en el artículo 270 de la Ley General de la Administración Pública.

f. Dictar las disposiciones que fijen los criterios a que responderá la actuación de la Agencia en la aplicación de la presente ley, que se denominarán circulares. Para su elaboración se deberán contar con los informes técnicos y jurídicos necesarios, y conceder audiencia a los interesados. Las circulares serán obligatorias una vez publicadas en el Diario Oficial La Gaceta.	f. Dictar las disposiciones que fijen los criterios a que responderá la actuación de la Agencia en la aplicación de la presente **L**ey, que se denominarán circulares. Para su elaboración se deberán contar con los informes técnicos y jurídicos necesarios, y conceder audiencia a los interesados. Las circulares serán obligatorias una vez publicadas en el Diario Oficial La Gaceta.
g. Elaborar y publicar guías y manuales dirigidos a los responsables, encargados y ciudadanía en general, sobre asuntos relacionados con la protección de datos personales, para orientar a los actores hacia el cumplimiento de la legislación.	g. Elaborar y publicar guías y manuales dirigidos a los **R**esponsables, **E**ncargados y ciudadanía en general, sobre asuntos relacionados con la protección de datos personales, para orientar a los actores hacia el cumplimiento de la legislación.
h. Acordar la realización de planes de auditoría preventiva, referidos a los tratamientos de un sector concreto de actividad. Tendrán por objeto el análisis del cumplimiento de las disposiciones de la presente ley, a partir de la realización de actividades de investigación sobre entidades pertenecientes al sector inspeccionado o sobre los responsables objeto de la auditoría.	h. Acordar la realización de planes de auditoría preventiva, referidos a los tratamientos de un sector concreto de actividad. Tendrán por objeto el análisis del cumplimiento de las disposiciones de la presente **L**ey, a partir de la realización de actividades de investigación sobre entidades pertenecientes al sector inspeccionado o sobre los **R**esponsables objeto de la auditoría.
	i. Dictar y ejecutar medidas cautelares en sede administrativa para garantizar la protección de los datos personales de los habitantes.
Las potestades de inspección y recolección de información otorgadas a la Agencia de Protección de Datos en esta Ley, deberán ser ejercidas con sujeción a los principios de razonabilidad, proporcionalidad e interdicción de la arbitrariedad administrativa, en resguardo de los derechos involucrados, y previa comprobación de indicios suficientes que justifiquen la intervención, o la hagan necesaria para averiguar la verdad real de los hechos investigados.	Las potestades de inspección y recolección de información otorgadas a la Agencia de Protección de Datos en esta Ley, deberán ser ejercidas con sujeción a los principios de razonabilidad, proporcionalidad e interdicción de la arbitrariedad administrativa, en resguardo de los derechos involucrados, y previa comprobación de indicios suficientes que justifiquen la intervención, o la hagan necesaria para averiguar la verdad real de los hechos investigados**, salvo en el caso de auditorías preventivas, en cuyo caso podrá actuar sin comprobación previa de indicios.**
ARTÍCULO 65- Dirección de la Agencia de Protección de Datos	ARTÍCULO 65.- Dirección de la Agencia de Protección de Datos

1. La Dirección de la Agencia de Protección de Datos la dirige, ostenta su representación y dicta sus resoluciones, circulares y directrices. 2. La Dirección de la Agencia de Protección de Datos estará auxiliada por un Adjunto en el que podrá delegar sus funciones. Ambos ejercerán sus funciones con plena independencia y objetividad y no estarán sujetos a instrucción alguna en su desempeño. 3. La Dirección de la Agencia de Protección de Datos y su Adjunto serán nombrados por el Consejo de Gobierno, a propuesta del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, mediante concurso público de antecedentes entre personas de reconocida competencia profesional, en particular en materia de protección de datos. Dos meses antes de producirse la expiración del mandato o, en el resto de las causas de cese, cuando se haya producido éste, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones ordenará la publicación en el Diario Oficial La Gaceta así como en medios de comunicación colectiva, la convocatoria pública de candidatos. Previa evaluación del mérito, capacidad, competencia e idoneidad de las personas candidatas, el MICITT propondrá y el Consejo de Gobierno designará a la Dirección y el Adjunto de la Agencia de Protección de Datos. Una vez que el Consejo de Gobierno haya nombrado al director o directora tanto propietario como adjunto, enviará el nombramiento junto con el expediente del concurso a la Asamblea Legislativa, que dispondrá de un plazo de treinta días naturales para objetar el nombramiento por mayoría calificada. Si en ese lapso no se produjera objeción, se tendrán por ratificados. En caso contrario, el Consejo de Gobierno sustituirá a la persona cuyo nombramiento fue objetado y el nuevo nombramiento deberá seguir el mismo procedimiento previsto anteriormente. 5. El mandato de la Dirección y del Adjunto de la Agencia de Protección de Datos tiene una duración de cinco años y puede ser	1. La Dirección de la Agencia de Protección de Datos la dirige, ostenta su representación y dicta sus resoluciones, circulares y directrices. 2. La Dirección de la Agencia de Protección de Datos estará auxiliada por un Adjunto en el que podrá delegar sus funciones. Ambos ejercerán sus funciones con plena independencia y objetividad y no estarán sujetos a instrucción alguna en su desempeño. 3. La Dirección de la Agencia de Protección de Datos y su Adjunto serán nombrados por el Consejo de Gobierno, a propuesta del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, mediante concurso público de antecedentes entre personas de reconocida competencia profesional, en particular en materia de protección de datos. *Tienen impedimento para ser nombrados como Director y/o Adjunto los parientes, hasta tercer grado de consanguinidad o afinidad del presidente de la República, los vicepresidentes, los ministros y viceministros o con vínculo civil por afinidad hasta el mismo grado.* Dos meses antes de producirse la expiración del mandato o, en el resto de las causas de cese, cuando se haya producido éste, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones ordenará la publicación en el Diario Oficial La Gaceta así como en medios de comunicación colectiva, la convocatoria pública de candidatos. Previa evaluación del mérito, capacidad, competencia e idoneidad de las personas candidatas, el MICITT propondrá y el Consejo de Gobierno designará a la Dirección y el Adjunto de la Agencia de Protección de Datos. Una vez que el Consejo de Gobierno haya nombrado al director o directora tanto propietario como adjunto, enviará el nombramiento junto con el expediente del concurso a la Asamblea Legislativa, que dispondrá de un plazo de treinta días naturales para objetar el nombramiento por mayoría calificada. Si en ese lapso no se produjera objeción, se tendrán por ratificados. En caso contrario, el Consejo de Gobierno sustituirá a la persona cuyo nombramiento fue objetado y el nuevo nombramiento deberá seguir el mismo procedimiento previsto anteriormente.

renovado para un único período adicional de igual duración. La Dirección y el Adjunto solo cesarán de su cargo antes de la expiración de su mandato, a petición propia o por separación acordada por el Consejo de Gobierno, por: a. Incumplimiento grave de sus obligaciones. b. Incapacidad física o cognitiva sobrevenida para el ejercicio de su función. c. Incompatibilidad grave por hechos sobrevenidos que impidan o dificulten que pueda ejercer las funciones atribuidas en esta Ley de forma imparcial e independiente, y en cumplimiento del interés público. d. Condena firme por delito doloso. La remoción de la Dirección de la Agencia de Protección de Datos por las causales de los incisos a) y c) anteriores deberá tramitarse ante el Consejo de Gobierno, mediante el procedimiento ordinario establecido en la Ley N.º 6227, Ley General de la Administración Pública, de 2 de mayo de 1978 y sus reglamentos. Una vez tramitado el procedimiento, pero de previo a la adopción de la resolución final que decida sobre la separación, el Consejo de Gobierno enviará a la Procuraduría General de la República el expediente, para que ésta se manifieste, en un plazo razonable, sobre el carácter “grave” de la falta o la incompatibilidad y la procedencia de la separación. El criterio de la Procuraduría no será vinculante pero el Consejo deberá motivar su decisión de separarse de dicho criterio, si fuera el caso. 6. Los actos y disposiciones dictados por la Dirección de la Agencia de Protección de Datos ponen fin a la vía administrativa, siendo recurribles, directamente, ante la jurisdicción contencioso administrativa.	5. El mandato de la Dirección y del Adjunto de la Agencia de Protección de Datos tiene una duración de cinco años y puede ser renovado para un único período adicional de igual duración. La Dirección y el Adjunto solo cesarán de su cargo antes de la expiración de su mandato, a petición propia o por separación acordada por el Consejo de Gobierno, por: a. Incumplimiento grave de sus obligaciones. **b.** Incapacidad física o cognitiva sobrevenida para el ejercicio de su función **por un plazo superior a seis meses.** c. Incompatibilidad grave por hechos sobrevenidos que impidan o dificulten que pueda ejercer las funciones atribuidas en esta Ley de forma imparcial e independiente, y en cumplimiento del interés público. d. Condena firme por delito doloso**, incluso en grado de tentativa**. La remoción de la Dirección de la Agencia de Protección de Datos por las causales de los incisos a) y c) anteriores deberá tramitarse ante el Consejo de Gobierno, mediante el procedimiento ordinario establecido en la Ley N.º 6227, Ley General de la Administración Pública, de 2 de mayo de 1978 y sus reglamentos. Una vez tramitado el procedimiento, pero de previo a la adopción de la resolución final que decida sobre la separación, el Consejo de Gobierno enviará a la Procuraduría General de la República el expediente, para que ésta se manifieste, en un plazo razonable, sobre el carácter “grave” de la falta o la incompatibilidad y la procedencia de la separación. El criterio de la Procuraduría no será vinculante pero el Consejo deberá motivar su decisión de separarse de dicho criterio, si fuera el caso. 6. Los actos y disposiciones dictados por la Dirección de la Agencia de Protección de Datos ponen fin a la vía administrativa, siendo

	recurribles, directamente, ante la jurisdicción contencioso administrativa.
CAPÍTULO IX PROCEDIMIENTO EN CASO DE POSIBLE VULNERACIÓN A LA NORMATIVA DE PROTECCIÓN DE DATOS	CAPÍTULO IX PROCEDIMIENTO EN CASO DE POSIBLE VULNERACIÓN A LA NORMATIVA DE PROTECCIÓN DE DATOS
ARTÍCULO 66- Régimen de reclamaciones 1. Todo titular tendrá derecho a presentar su reclamación ante la Agencia de Protección de Datos, así como recurrir a la tutela judicial para hacer efectivos sus derechos conforme a la legislación aplicable en la materia.	ARTÍCULO 66.- Régimen de reclamaciones 1. Todo **T**itular tendrá derecho a presentar su reclamación ante la Agencia de Protección de Datos, así como recurrir a la tutela judicial para hacer efectivos sus derechos conforme a la legislación aplicable en la materia.
ARTÍCULO 67- Admisión a trámite de las reclamaciones 1. Cuando se presente ante la Agencia de Protección de Datos una reclamación, esta deberá evaluar su admisibilidad a trámite, de conformidad con las previsiones de este artículo. 2. La Agencia de Protección de Datos inadmitirá 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. 3. Igualmente, la Agencia de Protección de Datos podrá inadmitir la reclamación cuando el responsable o encargado del tratamiento, previa advertencia formulada por la Agencia, hubiera adoptado las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos y concurra alguna de las siguientes circunstancias: a. Que no se haya causado perjuicio al afectado en el caso de las infracciones leves previstas en el artículo 76 de esta Ley. b. Que el derecho del afectado quede plenamente garantizado mediante la aplicación de las medidas. 4. Antes de resolver sobre la admisión a trámite de la reclamación, la Agencia podrá remitir la misma al oficial de protección de datos	ARTÍCULO 67.- Admisión a trámite de las reclamaciones 1. Cuando se presente ante la Agencia de Protección de Datos una reclamación, esta deberá evaluar su admisibilidad a trámite, de conformidad con las previsiones de este artículo. 2. La Agencia de Protección de Datos inadmitirá 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. 3. Igualmente, la Agencia de Protección de Datos podrá inadmitir la reclamación cuando el **R**esponsable o **E**ncargado del tratamiento, previa advertencia formulada por la Agencia, hubiera adoptado las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos y concurra alguna de las siguientes circunstancias: a. Que no se haya causado perjuicio al afectado en el caso de las infracciones leves previstas en el artículo 76 de esta Ley. b. Que el derecho del afectado quede plenamente garantizado mediante la aplicación de las medidas. 4. Antes de resolver sobre la admisión a trámite de la reclamación, la Agencia podrá remitir la misma al oficial de protección de datos que

que hubiera, en su caso, designado el responsable del tratamiento. La Agencia podrá igualmente remitir la reclamación al responsable o encargado del tratamiento cuando no se hubiera designado un oficial de protección de datos, en cuyo caso el responsable o encargado deberá dar respuesta a la reclamación en el plazo de un mes. 5. La decisión sobre la admisión o inadmisión a trámite deberá notificarse al reclamante en el plazo de tres meses. Si transcurrido este plazo no se produjera dicha notificación, se entenderá que prosigue la tramitación de la reclamación a partir de la fecha en que se cumpliesen tres meses desde que la reclamación tuvo entrada en la Agencia de Protección de Datos.	hubiera, en su caso, designado el **R**esponsable del tratamiento. La Agencia podrá igualmente remitir la reclamación al **R**esponsable o **E**ncargado del tratamiento cuando no se hubiera designado un oficial de protección de datos, en cuyo caso el **R**esponsable o **E**ncargado deberá dar respuesta a la reclamación en el plazo de un mes. 5. La decisión sobre la admisión o inadmisión a trámite deberá notificarse al reclamante en el plazo de tres meses. Si transcurrido este plazo no se produjera dicha notificación, se entenderá que prosigue la tramitación de la reclamación a partir de la fecha en que se cumpliesen tres meses desde que la reclamación tuvo entrada en la Agencia de Protección de Datos.
ARTÍCULO 68- Actuaciones previas de investigación 1. Antes de la adopción del acuerdo de inicio de procedimiento, y una vez admitida a trámite la reclamación si la hubiese, la Agencia de Protección de Datos podrá llevar a cabo una investigación preliminar a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento. 2. La investigación preliminar no podrá tener una duración superior a doce meses a contar desde la fecha del acuerdo de admisión a trámite o de la fecha de la resolución por la que se decida su iniciación cuando la Agencia de Protección de Datos actúe de oficio.	ARTÍCULO 68.- Actuaciones previas de investigación 1. Antes de la adopción del acuerdo de inicio de procedimiento, y una vez admitida a trámite la reclamación si la hubiese, la Agencia de Protección de Datos podrá llevar a cabo una investigación preliminar a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento. 2. La investigación preliminar no podrá tener una duración superior a doce meses a contar desde la fecha del acuerdo de admisión a trámite o de la fecha de la resolución por la que se decida su iniciación cuando la Agencia de Protección de Datos actúe de oficio.
ARTÍCULO 69.-Acuerdo de inicio del procedimiento para el ejercicio de la potestad sancionadora 1. Concluidas, en su caso, las actuaciones preliminares a las que se refiere el artículo anterior, corresponderá a la Dirección de la Agencia de Protección de Datos, cuando así proceda, ordenar el inicio del procedimiento para el ejercicio de la potestad sancionadora, mediante un traslado de cargos en el 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 69.- Acuerdo de inicio del procedimiento para el ejercicio de la potestad sancionadora 1. Concluidas, en su caso, las actuaciones preliminares a las que se refiere el artículo anterior, corresponderá a la Dirección de la Agencia de Protección de Datos, cuando así proceda, ordenar el inicio del procedimiento para el ejercicio de la potestad sancionadora, mediante un traslado de cargos en el 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 70- Medidas provisionales y de garantía de los derechos	ARTÍCULO 70.- Medidas provisionales y de garantía de los derechos

1. Durante la realización de investigación preliminar o iniciado un procedimiento para el ejercicio de la potestad sancionadora, la Agencia podrá acordar motivadamente las medidas provisionales necesarias y proporcionadas para salvaguardar el derecho fundamental a la protección de datos. 2. En los casos en que la Agencia considere que la continuación del tratamiento de los datos personales, su ~~comunicación~~ o transferencia internacional comportara un menoscabo grave del derecho a la protección de datos personales, podrá ordenar a los responsables o encargados de los tratamientos el bloqueo de los datos y la cesación de su tratamiento y, en caso de incumplirse por estos dichos mandatos, proceder a su inmovilización. 3. Cuando se hubiese presentado ante la Agencia una reclamación que se refiriese, entre otras cuestiones, a la falta de atención en plazo de los derechos establecidos el artículo 27 de esta Ley, la Agencia podrá acordar en cualquier momento, incluso con anterioridad a la iniciación del procedimiento para el ejercicio de la potestad sancionadora, mediante resolución motivada y previa audiencia del responsable del tratamiento, la obligación de atender el derecho solicitado, prosiguiéndose el procedimiento en cuanto al resto de las cuestiones objeto de la reclamación.	1. Durante la realización de investigación preliminar o iniciado un procedimiento para el ejercicio de la potestad sancionadora, la Agencia podrá acordar motivadamente las medidas provisionales necesarias y proporcionadas para salvaguardar el derecho fundamental a la protección de datos. 2. En los casos en que la Agencia considere que la continuación del tratamiento de los datos personales, su **cesión** o transferencia internacional comportara un menoscabo grave del derecho a la protección de datos personales, podrá ordenar a los **R**esponsables o **E**ncargados de los tratamientos el bloqueo de los datos y la cesación de su tratamiento y, en caso de incumplirse por estos dichos mandatos, proceder a su inmovilización. 3. Cuando se hubiese presentado ante la Agencia una reclamación que se refiriese, entre otras cuestiones, a la falta de atención en plazo de los derechos establecidos el artículo 27 de esta Ley, la Agencia podrá acordar en cualquier momento, incluso con anterioridad a la iniciación del procedimiento para el ejercicio de la potestad sancionadora, mediante resolución motivada y previa audiencia del **R**esponsable del tratamiento, la obligación de atender el derecho solicitado, prosiguiéndose el procedimiento en cuanto al resto de las cuestiones objeto de la reclamación.
ARTÍCULO 71- Sustanciación de actuaciones En lo no expresamente previsto en esta Ley, el procedimiento administrativo se sustanciará de conformidad con las reglas para el procedimiento ordinario regulado el Libro Segundo de la Ley General de la Administración Pública.	ARTÍCULO 71.- Sustanciación de actuaciones En lo no expresamente previsto en esta Ley, el procedimiento administrativo se sustanciará de conformidad con las reglas para el procedimiento ordinario regulado el Libro Segundo de la Ley General de la Administración Pública.
CAPÍTULO X RÉGIMEN SANCIONADOR	CAPÍTULO X RÉGIMEN SANCIONADOR
ARTÍCULO 72- Sujetos responsables 1. Están sujetos al régimen sancionador establecido en la presente ley: a. Los responsables o corresponsables de los tratamientos. b. Los encargados de los tratamientos.	ARTÍCULO 72.- Sujetos responsables 1. Están sujetos al régimen sancionador establecido en la presente **L**ey: a. Los **R**esponsables o corresponsables de los tratamientos. **b.** Los **E**ncargados de los tratamientos**, en el cuanto su responsabilidad no se**

2. No será de aplicación al oficial de protección de datos el régimen sancionador establecido en este Capítulo.	**derive de instrucciones giradas por el Responsable, o del incumplimiento de este a las disposiciones de esta Ley o su reglamento.** 2. No será de aplicación al oficial de protección de datos el régimen sancionador establecido en este Capítulo.
ARTÍCULO 73- Infracciones 1. Constituyen infracciones los actos y conductas que resulten contrarias a la presente Ley. Si se ha incurrido en alguna de las infracciones tipificadas en esta Ley, se deberá imponer alguna de las siguientes sanciones, sin perjuicio de las sanciones penales correspondientes: a. Para las faltas leves, una multa hasta de entre diez ~~y veinte~~ salarios base. b. Para las faltas graves, una multa de ~~veinte~~ a cincuenta salarios base~~, y, en caso de personas jurídicas, el monto superior entre cincuenta salarios base y hasta un dos por ciento del volumen de ventas que hubiere reportado durante el periodo fiscal inmediato anterior a la comisión de la infracción.~~ c. Para las faltas gravísimas, una multa de cincuenta hasta ~~quinientos~~ salarios base, y, en caso de personas jurídicas, el monto superior entre ~~quinientos~~ salarios base y hasta un ~~cuatro~~ por ciento del volumen de ventas que hubiere reportado durante el periodo fiscal inmediato anterior a la comisión de la infracción.	ARTÍCULO 73.- Infracciones 1. Constituyen infracciones los actos y conductas que resulten contrarias a la presente Ley. Si se ha incurrido en alguna de las infracciones tipificadas en esta Ley, se deberá imponer alguna de las siguientes sanciones, sin perjuicio de las sanciones penales correspondientes: a. Para las faltas leves, una multa hasta de entre **cinco y** diez salarios base. b. Para las faltas graves, una multa de **diez** a cincuenta salarios base. c. Para las faltas gravísimas, una multa de cincuenta hasta **cien** salarios base, y, en caso de personas **físicas o** jurídicas **que cometieran la infracción en el ejercicio de una actividad lucrativa,** el monto superior entre **cien** salarios base y hasta un **dos** por ciento del volumen de ventas que hubiere reportado durante el periodo fiscal inmediato anterior a la comisión de la infracción.
ARTÍCULO 74- Infracciones consideradas muy graves 1. Se consideran muy graves y prescribirán a los tres años las siguientes infracciones: a. El tratamiento de datos personales vulnerando algunos o todos los principios establecidos en el artículo 13 de esta Ley. b. El tratamiento de datos personales sin que concurra alguna de las condiciones	ARTÍCULO 74.- Infracciones consideradas muy graves 1. Se consideran muy graves y prescribirán a los tres años las siguientes infracciones: a. El tratamiento de datos personales vulnerando algunos o todos los principios establecidos en el artículo 13 de esta Ley. b. El tratamiento de datos personales sin que concurra alguna de las condiciones de legitimación del tratamiento

de legitimación del tratamiento establecidas en el artículo 15 de esta Ley.	establecidas en el artículo 15 de esta Ley.
c. El incumplimiento de los requisitos exigidos para la validez del consentimiento.	c. El incumplimiento de los requisitos exigidos para la validez del consentimiento.
d. La utilización de los datos para una finalidad que no sea compatible con la finalidad para la cual fueron recogidos, sin contar con el consentimiento del afectado o con una base legal para ello.	d. La utilización de los datos para una finalidad que no sea compatible con la finalidad para la cual fueron recogidos, sin contar con el consentimiento del afectado o con una base legal para ello.
e. El tratamiento de datos personales sensibles sin que concurra alguna de las circunstancias previstas en el artículo 11 de esta Ley.	e. El tratamiento de datos personales sensibles sin que concurra alguna de las circunstancias previstas en el artículo 11 de esta Ley.
f. El tratamiento de datos personales relacionados con condenas e infracciones penales fuera de los supuestos permitidos por el artículo 12 de esta Ley.	f. El tratamiento de datos personales relacionados con condenas e infracciones penales fuera de los supuestos permitidos por el artículo 12 de esta Ley.
g. La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en el artículo 19 de esta Ley.	g. La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en el artículo 19 de esta Ley.
h. La vulneración del deber de confidencialidad establecido en el artículo 26 de esta Ley.	h. La vulneración del deber de confidencialidad establecido en el artículo 26 de esta Ley.
i. La exigencia del pago de un canon para facilitar al afectado la información a la que se refiere el artículo 19 de esta Ley, o por atender las solicitudes de ejercicio de derechos de los afectados previstos en el artículo 27 de esta Ley, fuera del supuestos establecido en el artículo 29 párrafo 4.	i. La exigencia del pago de un canon para facilitar al afectado la información a la que se refiere el artículo 19 de esta Ley, o por atender las solicitudes de ejercicio de derechos de los afectados previstos en el artículo 27 de esta Ley, fuera del supuestos establecido en el artículo 29 párrafo 4.
j. El impedimento o la obstaculización o la no atención reiterada del ejercicio de los derechos establecidos en el artículo 27 de la presente Ley.	j. El impedimento o la obstaculización o la no atención reiterada del ejercicio de los derechos establecidos en el artículo 27 de la presente Ley.
k. La transferencia internacional de datos personales a un destinatario que se encuentre en un tercer país o a una organización internacional, cuando no concurran las garantías, requisitos o	k. La transferencia internacional de datos personales a un destinatario que se encuentre en un tercer país o a una organización internacional, cuando no concurran las garantías, requisitos o excepciones establecidos en la presente Ley.

excepciones establecidos en ~~el artículo 45 de~~ la presente Ley. l. El incumplimiento de las resoluciones dictadas por la autoridad de protección de datos competente en ejercicio de los poderes que le confiere ~~el artículo 64 de~~ la presente Ley. m. El incumplimiento de la obligación de bloqueo de los datos establecida en el artículo 44 de esta Ley cuando la misma sea exigible. ~~n. No facilitar el acceso del personal de la autoridad de protección de datos competente a los datos personales, información, locales, equipos y medios de tratamiento que sean requeridos por la autoridad de protección de datos para el ejercicio de sus poderes de investigación.~~ o. La resistencia u obstrucción del ejercicio de la función inspectora de la Agencia de Protección de Datos. p. La reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados. q. La ~~transferencia~~ interinstitucional de datos personales en incumplimiento de lo establecido en el artículo 8 de la presente Ley. r. La utilización de sistemas de identificación biométrica en tiempo real en espacios públicos.	l. El incumplimiento de las resoluciones dictadas por la autoridad de protección de datos competente en ejercicio de los poderes que le confiere la presente Ley. m. El incumplimiento de la obligación de bloqueo de los datos establecida en el artículo 44 de esta Ley cuando la misma sea exigible. n. La resistencia u obstrucción del ejercicio de la función inspectora de la Agencia de Protección de Datos. o. La reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados. p. La **cesión** interinstitucional de datos personales en incumplimiento de lo establecido en el artículo 8 de la presente Ley. q. La utilización de sistemas de identificación biométrica en tiempo real en espacios públicos.
ARTÍCULO 75- Infracciones consideradas graves 1. Se consideran graves y prescribirán a los dos años las siguientes infracciones: a. El tratamiento de datos personales de un menor de edad sin recabar su consentimiento, cuando tenga capacidad para ello, o el del titular de su patria potestad o tutela. b. El impedimento o la obstaculización o la no atención reiterada de los derechos	ARTÍCULO 75.- Infracciones consideradas graves 1. Se consideran graves y prescribirán a los dos años las siguientes infracciones: a. El tratamiento de datos personales de un menor de edad sin recabar su consentimiento, cuando tenga capacidad para ello, o el del titular de su patria potestad o tutela. b. El impedimento o la obstaculización o la no atención reiterada de los derechos

de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando este, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación.	de acceso, rectificación, **cancelación o** supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando este, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación.
c. La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento.	c. La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento.
d. La contratación por el responsable del tratamiento de un encargado de tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas.	d. La contratación por el **R**esponsable del tratamiento de un **E**ncargado de tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas.
e. Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 41 de esta Ley.	e. Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 41 de esta Ley.
f. La contratación por un encargado del tratamiento de otros encargados sin contar con la autorización previa del responsable, o sin haberle informado sobre los cambios producidos en la subcontratación cuando fueran legalmente exigibles.	f. La contratación por un **E**ncargado del tratamiento de otros **E**ncargados sin contar con la autorización previa del **R**esponsable, o sin haberle informado sobre los cambios producidos en la subcontratación cuando fueran legalmente exigibles.
g. La infracción por un encargado del tratamiento de lo dispuesto en la presente Ley, al establecer relaciones en su propio nombre con los afectados aun cuando exista un contrato de encargo, conforme a lo dispuesto en el artículo 41 de esta Ley.	g. La infracción por un **E**ncargado del tratamiento de lo dispuesto en la presente Ley, al establecer relaciones en su propio nombre con los afectados aun cuando exista un contrato de encargo, conforme a lo dispuesto en el artículo 41 de esta Ley.
h. No disponer del registro de actividades de tratamiento establecido en el artículo 43 de la presente Ley.	h. No disponer del registro de actividades de tratamiento establecido en el artículo 43 de la presente Ley.
i. No poner a disposición de la autoridad de protección de datos que lo haya solicitado, el registro de actividades de tratamiento, conforme al apartado 4 del artículo 43 de la presente Ley.	i. No poner a disposición de la autoridad de protección de datos que lo haya solicitado, el registro de actividades de tratamiento, conforme al apartado 4 del artículo 43 de la presente Ley.

j. El tratamiento de datos personales sin llevar a cabo una previa valoración de los elementos mencionados en el artículo 37 de esta Ley.	j. El tratamiento de datos personales sin llevar a cabo una previa valoración de los elementos mencionados en el artículo 37 de esta Ley.
k. El incumplimiento del deber del encargado del tratamiento de notificar al responsable del tratamiento las violaciones de seguridad de las que tuviera conocimiento.	k. El incumplimiento del deber del **E**ncargado del tratamiento de notificar al **R**esponsable del tratamiento las violaciones de seguridad de las que tuviera conocimiento.
l. El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos de conformidad con lo previsto en el artículo 25 de la presente Ley.	l. El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos de conformidad con lo previsto en el artículo 25 de la presente Ley.
m. El tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible.	m. El tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible.
n. El incumplimiento de la obligación de designar un oficial de protección de datos cuando sea exigible su nombramiento.	n. El incumplimiento de la obligación de designar un oficial de protección de datos cuando sea exigible su nombramiento.
o. No posibilitar la efectiva participación del oficial de protección de datos en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones.	o. No posibilitar la efectiva participación del oficial de protección de datos en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones.

ARTÍCULO 76- Infracciones consideradas leves	ARTÍCULO 76.- Infracciones consideradas leves
Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal, en particular, las siguientes:	Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal, en particular, las siguientes:
a. El incumplimiento del principio de transparencia de la información o el derecho de información del afectado por no facilitar toda la información exigida por el artículo 19 de la presente Ley.	a. El incumplimiento del principio de transparencia de la información o el derecho de información del afectado por no facilitar toda la información exigida por el artículo 19 de la presente Ley.
b. No atender las solicitudes de ejercicio de los derechos establecidos en el artículo 27 de esta Ley, salvo que resultase de aplicación lo dispuesto en el artículo 74.1.j) de esta Ley.	b. No atender las solicitudes de ejercicio de los derechos establecidos en el artículo 27 de esta Ley, salvo que resultase de aplicación lo dispuesto en el artículo 74.1.j) de esta Ley.
c. El incumplimiento de la obligación de informar al afectado, cuando así lo haya solicitado, de los destinatarios a los que se hayan ~~tranferido~~ los datos personales rectificados, suprimidos o respecto de los que se ha limitado el tratamiento.	c. El incumplimiento de la obligación de informar al afectado, cuando así lo haya solicitado, de los destinatarios a los que se hayan **cedido o transferido** los datos personales rectificados, suprimidos o respecto de los que se ha limitado el tratamiento.
d. El incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando ello fuera exigible conforme al artículo 5 de esta Ley.	d. El incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando ello fuera exigible conforme al artículo 5 de esta Ley.
e. La falta de formalización por los corresponsables del tratamiento del acuerdo que determine las obligaciones, funciones y responsabilidades respectivas con respecto al tratamiento de datos personales y sus relaciones con los afectados al que se refiere el artículo 38 de esta Ley o la inexactitud en la determinación de las mismas.	e. La falta de formalización por los corresponsables del tratamiento del acuerdo que determine las obligaciones, funciones y responsabilidades respectivas con respecto al tratamiento de datos personales y sus relaciones con los afectados al que se refiere el artículo 38 de esta Ley o la inexactitud en la determinación de las mismas.
f. No poner a disposición de los afectados los aspectos esenciales del acuerdo formalizado entre los corresponsables del tratamiento, conforme exige el artículo 38 párrafo 2 de esta Ley.	f. No poner a disposición de los afectados los aspectos esenciales del acuerdo formalizado entre los corresponsables del tratamiento, conforme exige el artículo 38 párrafo 2 de esta Ley.
g. El incumplimiento por el encargado de las estipulaciones impuestas en el contrato o acto jurídico que regula el	g. El incumplimiento por el **E**ncargado de las estipulaciones impuestas en el contrato o acto jurídico que regula el

tratamiento o las instrucciones del responsable del tratamiento, salvo en los supuestos en que fuese necesario para evitar la infracción de la legislación en materia de protección de datos y se hubiese advertido de ello al responsable o al encargado del tratamiento.	tratamiento o las instrucciones del **R**esponsable del tratamiento, salvo en los supuestos en que fuese necesario para evitar la infracción de la legislación en materia de protección de datos y se hubiese advertido de ello al **R**esponsable o al **E**ncargado del tratamiento.
h. Disponer de un Registro de actividades de tratamiento que no incorpore toda la información exigida por el artículo 43 de esta Ley.	h. Disponer de un Registro de actividades de tratamiento que no incorpore toda la información exigida por el artículo 43 de esta Ley.
i. La notificación incompleta, tardía o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales.	i. La notificación incompleta, tardía o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales.
j. El incumplimiento de la obligación de documentar cualquier violación de seguridad.	j. El incumplimiento de la obligación de documentar cualquier violación de seguridad.
k. El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, salvo que resulte de aplicación lo previsto en el artículo 75.1 l) de esta Ley.	k. El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, salvo que resulte de aplicación lo previsto en el artículo 75.1 l) de esta Ley.
l. No publicar los datos de contacto del oficial de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando su nombramiento sea exigible de acuerdo con esta Ley.	l. No publicar los datos de contacto del oficial de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando su nombramiento sea exigible de acuerdo con esta Ley.

ARTÍCULO 77- Interrupción de la prescripción de la infracción Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de ~~doce~~ meses por causas no imputables al presunto infractor.	ARTÍCULO 77.- Interrupción de la prescripción de la infracción Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de **seis** meses por causas no imputables al presunto infractor.
ARTÍCULO 78- Sanciones y medidas correctivas 1.- Las sanciones se impondrán, en función de las circunstancias de cada caso individual, se tendrá debidamente en cuenta: a. La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de titulares afectados y el nivel de los daños y perjuicios que hayan sufrido. b. La intencionalidad o negligencia en la infracción. c. El carácter continuado de la infracción. d. La vinculación de la actividad del infractor con la realización de tratamientos de datos personales. e. Los beneficios obtenidos como consecuencia de la comisión de la infracción. f. La afectación a los derechos de los menores. g. Disponer, cuando no fuere obligatorio, de un oficial de protección de datos. h. Cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los titulares. i. El grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado.	ARTÍCULO 78.- Sanciones y medidas correctivas 1. Las sanciones se impondrán, en función de las circunstancias de cada caso individual, se tendrá debidamente en cuenta: a. La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de **T**itulares afectados y el nivel de los daños y perjuicios que hayan sufrido. b. La intencionalidad o negligencia en la infracción. c. El carácter continuado de la infracción. d. La vinculación de la actividad del infractor con la realización de tratamientos de datos personales. e. Los beneficios obtenidos como consecuencia de la comisión de la infracción. f. La afectación a los derechos de los menores. g. Disponer, cuando no fuere obligatorio, de un oficial de protección de datos. h. Cualquier medida tomada por el **R**esponsable o **E**ncargado del tratamiento para paliar los daños y perjuicios sufridos por los **T**itulares. i. El grado de responsabilidad del **R**esponsable o del **E**ncargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado.

j. Toda infracción anterior cometida por el responsable o el encargado del tratamiento. k. El grado de cooperación con la Agencia de Protección de Datos con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción. l. Las categorías de los datos de carácter personal afectados por la infracción. m. La forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida. n. 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. 3. Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones de la presente ley, la cuantía total de la sanción no será superior a la cuantía prevista para las infracciones más graves. 4. Será objeto de publicación en el Diario Oficial La Gaceta la información que identifique al infractor, la infracción cometida y el importe de la sanción impuesta cuando la sanción resulte de una la constatación de una falta grave o gravísima y el infractor sea una persona jurídica o entidad pública.	j. Toda infracción anterior cometida por el **R**esponsable o el **E**ncargado del tratamiento. k. El grado de cooperación con la Agencia de Protección de Datos con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción. l. Las categorías de los datos de carácter personal afectados por la infracción. m. La forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el **R**esponsable o el **E**ncargado notificó la infracción y, en tal caso, en qué medida. n. 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. 3. Si un **R**esponsable o un **E**ncargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones de la presente **L**ey, la cuantía total de la sanción no será superior a la cuantía prevista para las infracciones más graves. 4. Será objeto de publicación en el Diario Oficial La Gaceta la información que identifique al infractor, la infracción cometida y el importe de la sanción impuesta cuando la sanción resulte de una la constatación de una falta grave o gravísima y el infractor sea una persona jurídica o entidad pública.
ARTÍCULO 79- Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento 1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados: a. El Presidente de la República o sus vicepresidentes. b. La Asamblea Legislativa	ARTÍCULO 79.- Régimen aplicable a determinadas categorías de **R**esponsables o **E**ncargados del tratamiento 1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean **R**esponsables o **E**ncargados: a. El Presidente de la República o sus vicepresidentes. b. La Asamblea Legislativa

c. El Poder Judicial y los órganos jurisdiccionales.	c. El Poder Judicial y los órganos jurisdiccionales.
d. El Tribunal Supremo de Elecciones.	d. El Tribunal Supremo de Elecciones.
e. La Administración Pública centralizada y ~~desentralizada~~, excluyendo empresas públicas.	e. La Administración Pública centralizada y **descentralizada**, excluyendo empresas públicas.
f. La Defensoría de los Habitantes.	f. La Defensoría de los Habitantes.
g. Las Municipalidades.	g. Las Municipalidades.
h. Las Universidades Públicas.	h. Las Universidades Públicas.
2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refiere la presente ley, la Agencia de Protección de Datos Personales dictará resolución sancionando a las mismas con apercibimiento. La resolución ordenará asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.	2. Cuando los **R**esponsables o **E**ncargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refiere la presente **L**ey, la Agencia de Protección de Datos Personales dictará resolución sancionando a las mismas con apercibimiento. La resolución ordenará asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.
La resolución se notificará al jerarca de la entidad responsable o encargada del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de titulares, en su caso.	La resolución se notificará al jerarca de la entidad **R**esponsable o encargada del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de **T**itulares, en su caso.
~~3. Sin perjuicio de lo establecido en el apartado anterior, la Agencia de Protección de Datos propondrá también la iniciación de actuaciones disciplinarias contra los funcionarios implicados cuando existan indicios suficientes para ello. 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.~~	**3. Los funcionarios públicos que incurran en algunas de las infracciones establecidas en los artículos 74, 75 y 76 y se haya demostrado la culpa o dolo en su accionar u omisión, serán sancionados con la suspensión de su cargo por hasta noventa días, sin goce de salario, sin perjuicio de otras sanciones previstas en el régimen disciplinario aplicable al funcionario. 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.**
4. Se deberán comunicar a la Agencia Protección de Datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.	4. Se deberán comunicar a la Agencia Protección de Datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.
5. Se comunicarán a la Defensoría de los Habitantes las resoluciones dictadas al amparo de este artículo.	

	5. Se comunicarán a la Defensoría de los Habitantes las resoluciones dictadas al amparo de este artículo.
ARTÍCULO 80- Prescripción de las sanciones 1. Las sanciones impuestas en aplicación de esta Ley prescriben a los tres años. 2. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla. 3. La prescripción se interrumpirá por la notificación al investigado, del procedimiento de investigación, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.	ARTÍCULO 80.- Prescripción de las sanciones 1. Las sanciones impuestas en aplicación de esta Ley prescriben a los tres años. 2. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla. 3. La prescripción se interrumpirá por la notificación al investigado, del procedimiento de investigación, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.
CAPÍTULO XI DERECHO DE INDEMNIZACIÓN	CAPÍTULO XI DERECHO DE INDEMNIZACIÓN
ARTÍCULO 81- Reparación del daño 1. El titular que sufra daños y perjuicios derivados de una violación de su derecho a la protección de datos personales gozará del derecho de reclamar el resarcimiento de los daños y perjuicios ocasionados en infracción de las disposiciones de la presente ley. Si dicho daño fue ocasionado por un responsable y un encargado, ambos responderán solidariamente de los daños efectivamente ocasionados. 2. El ejercicio de acciones tendientes a la reparación de los daños sufridos será ejercido en la vía judicial y operará un plazo de prescripción de ~~un~~ año a partir de la existencia del mismo.	ARTÍCULO 81.- Reparación del daño 1. El **T**itular que sufra daños y perjuicios derivados de una violación de su derecho a la protección de datos personales gozará del derecho de reclamar el resarcimiento de los daños y perjuicios ocasionados en infracción de las disposiciones de la presente **L**ey. Si dicho daño fue ocasionado por un **R**esponsable y un **E**ncargado, ambos responderán solidariamente de los daños efectivamente ocasionados. 2. El ejercicio de acciones tendientes a la reparación de los daños sufridos será ejercido en la vía judicial y operará un plazo de prescripción de **tres** año**s** a partir de la existencia del mismo.
ARTÍCULO 82- Deróguese la Ley 8968 Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, del 07 de julio de 2011.	ARTÍCULO 82.- Deróguese la Ley 8968 Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, del 07 de julio de 2011.
ARTÍCULO 83- Las plazas de personal, el presupuesto, bienes, equipos y todos los demás activos asignados a la Agencia de Protección de Datos de los Habitantes (PRODHAB) se	ARTÍCULO 83.- Las plazas de personal, el presupuesto, bienes, equipos y todos los demás activos asignados a la Agencia de Protección de Datos de los Habitantes (PRODHAB) se

trasladarán a la Agencia de Protección de Datos Personales creada en esta ley, a fin de que continúen destinados al cumplimiento de los fines de esta última.	trasladarán a la Agencia de Protección de Datos Personales creada en esta **L**ey, a fin de que continúen destinados al cumplimiento de los fines de esta última.
DISPOSICIONES TRANSITORIAS	DISPOSICIONES TRANSITORIAS
TRANSITORIO I- El Poder Ejecutivo, en un plazo de seis meses contados a partir de la entrada en vigencia de esta ley, deberá concretar el traslado de los recursos, bienes y personal de la ~~Agencia de Protección de los Habitantes~~ a la Agencia de Protección de Datos Personales, e iniciar los procedimientos para el nombramiento de los puestos de dirección de la misma, en los términos previstos por esta Ley.	TRANSITORIO I.- El Poder Ejecutivo, en un plazo de seis meses contados a partir de la entrada en vigencia de esta **L**ey, deberá concretar el traslado de los recursos, bienes y personal de la **PRODHAB** a la Agencia de Protección de Datos Personales, e iniciar los procedimientos para el nombramiento de los puestos de dirección de la misma, en los términos previstos por esta Ley.
TRANSITORIO II- El siguiente Presupuesto Ordinario de la República que formule el Poder Ejecutivo después de la entrada en vigencia de esta Ley, deberá reflejar el traslado de las partidas presupuestarias del programa presupuestario de la Agencia de Protección de Datos de los Habitantes hacia el título presupuestario que se creará, correspondiente a la Agencia de Protección de Datos.	TRANSITORIO II.- **La PRODHAB continuará desarrollando sus funciones hasta que estas puedan ser asumidas de forma coordinada por la Agencia de Protección de Datos Personales creada en esta Ley, una vez que al menos su dirección haya sido designada y cuente con capacidad operativa para funcionar, lo que determinará la dirección mediante resolución que deberá ser publicada en el Diario La Gaceta y comunicada al público en general. Dicha transición deberá completarse en un periodo máximo de un año a partir de la entrada en vigor de esta Ley. Todos los procedimientos administrativos que estuvieran en trámite ante PRODHAB serán trasladados a la Agencia de Protección de Datos Personales a partir de que esta entre en funcionamiento, y serán continuados en el estado que estuvieren y hasta su efectiva finalización.**
TRANSITORIO III- Las personas físicas y jurídicas, públicas y privadas que ostenten condición de responsables o encargadas de datos personales gozarán de un periodo de doce meses para adecuar su funcionamiento a las disposiciones de esta Ley.	**TRANSITORIO III.** El siguiente Presupuesto Ordinario de la República que formule el Poder Ejecutivo después de la entrada en vigencia de esta Ley, deberá reflejar el traslado de las partidas presupuestarias del programa presupuestario de la **PRODHAB** hacia el título presupuestario que se creará, correspondiente a la Agencia de Protección de Datos.
TRANSITORIO VI- La Agencia de Protección de Datos emitirá la reglamentación requerida de esta Ley en el plazo de seis meses después de su entrada en funcionamiento.	TRANSITORIO I**V**. Las personas físicas y jurídicas, públicas y privadas que ostenten condición de **R**esponsables o **E**ncargadas de datos personales gozarán de un periodo de doce meses para adecuar su funcionamiento **y tratamiento de datos personales** a las disposiciones de esta Ley.
TRANSITORIO VII- La Superintendencia General de Entidades Financieras dictará las	TRANSITORIO V. La Agencia de Protección de Datos emitirá la reglamentación requerida de

regulaciones requeridas de acuerdo al artículo 55 de esta Ley, en el plazo de seis meses a partir de la entrada en vigor de esta Ley.	esta Ley en el plazo de seis meses después de su entrada en funcionamiento.
	TRANSITORIO VI. La Superintendencia General de Entidades Financieras dictará las regulaciones requeridas de acuerdo al artículo 55 de esta Ley, en el plazo de seis meses a partir de la entrada en vigor de esta Ley.
Rige a partir de su publicación.	Rige a partir de su publicación.

Elaborado por: ggr
/*lsch//16-11-2022
Arch// 23097 ITS//d/s/sil