IAIP

Instituto de Acceso a la Información Pública

LEY DE PROTECCIÓN DE DATOS PERSONALES

República de Honduras

AGRADECIMIENTO

DORIS IMELDA MADRID ZERON

El INSTITUTO DE ACCESO A LA INFORMACION PÚBLICA (IAIP), con al apoyo de la **Agencia Española de Cooperación Internacional para el Desarrollo AECID,** elaboro en el año 2013 el documento base para el Anteproyecto de Ley de Protección de Datos, en el marco del Proyecto **"Procesos de Participación Ciudadana en la Toma de Decisiones y Reformas Legales"** bajo consultoría realizada por el abogado **LESTER RAMIREZ.**

Con ese documento como base, el IAIP gestiono el financiamiento de la **Unión Europea** y a través del **Programa EUROsociAL I,** para que revisara y armonizara el Anteproyecto elaborado con la normativa internacional, a fin de que Honduras cuente con una legislación actualizada, moderna y apegada a los estándares nacional e internacionales en Protección de Datos Personales.

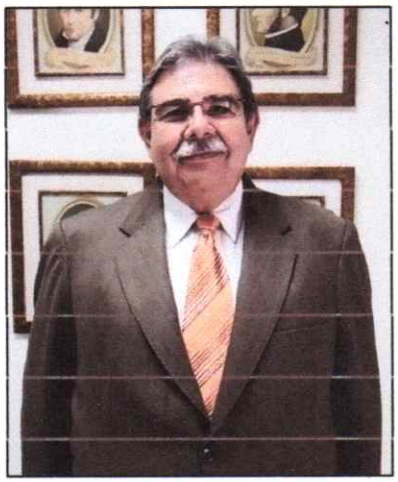
Con la aprobación del apoyo para realizar dicho proceso **Programa EUROsociAL I,** a travez de la **Fundación Centro de Educación a Distancia para el Desarrollo Económico y Tecnológico (CEDDET)**, identifico los expertos internacionales de diferentes países, coordinados por el abogado y ex magistrado de la sala constitucional del Reino de España y especialista en tecnologías de la comunicación JAVIER PUYOL, acompañado por Oscar Williams Altamirano de la superintendencia de telecomunicaciones de Ecuador, Fernando De la Cruz Prego Fundación CEDDET y Jose Ignacio Pariente De Prada de la Agencia Vasca de Protección de Datos del Reino de España; Samantha Alcalde Urbina del Instituto Federal de Acceso a la Información y Protección de Datos de Mexico y Felipe Eduardo Rotondó de la Agencia de Gobierno electrónico y Sociedad de la Información y del Conocimiento de Uruguay, .

Nuestro agradecimiento a las Organizaciones de Cooperación y a las personas que nos acompañaron en este proceso por garantizar la protección de los datos personales.

También nuestro especial agradecimiento a los servidores públicos del **INSTITUTO DE ACCESO A LA INFROMACIÓN PÚBLICA** que de una u otra forma contribuyeron a la elaboración del Anteproyecto de Ley y a la recolección de firmas.

DORIS IMELDA MADRID ZERON
COMISIONADA PRESIDENTA

PRESENTACIÓN



GUSTAVO ALDOLFO MANZANARES VAQUERO
Comisionado Secretario

Los derechos inherentes a la personalidad del ser humano, es decir aquellos que conforman nuestra propia individualidad y que pueden señalarse como el derecho al nombre, a la intimidad, a la propia imagen, al honor, e incluso los derechos del autor respecto a su obra literaria, artística o científica, han cobrado una enorme importancia en una forma simultánea al avance de la tecnología. Cada adelanto tecnológico en materia de comunicaciones entraña, muchas veces, nuevas posibilidades para lesionar los derechos de la personalidad, sobre todo, al facilitarse el tráfico de datos personales, lo que incide negativamente en el derecho a la intimidad, a la privacidad, al honor, a la autodeterminación informativa, a la identidad personal y, por supuesto, al derecho a ser diferentes.

La protección o tutela de los derechos al honor, intimidad personal o familiar y a la propia imagen, han sido reconocidos por la legislación hondureña desde la suscripción y ratificación de los instrumentos internacionales tales como la Declaración Universal de Derechos Humanos, la Convención Americana sobre Derechos Humanos y El Pacto Internacional de Derechos Civiles y Políticos. Sin embargo el reconocimiento del derecho a la protección de datos, como un derecho autónomo, se inició hasta el año 2003 con la aprobación del Decreto 243-2003, publicado en el Diario Oficial La Gaceta, de fecha 17 de febrero del 2005, en el que se aprueba, en primera instancia, la reforma al artículo 182 de la Constitución de la República, reconociendo la garantía de Hábeas Data, el cual, desafortunadamente, no fue ratificado. En el año 2004 con la Ley sobre Justicia Constitucional y en el 2006 con la Ley de Transparencia y Acceso a la Información Pública, se incluyen normas que reconocen la garantía de Hábeas Data, las que quedaron en suspenso hasta la aprobación de la correspondiente reforma Constitucional. Dicha reforma constitucional se produjo, finalmente, en el año 2013, quedando vigentes a partir del referido año todas las disposiciones legales relacionadas con el Hábeas Data.

A pesar de que la Ley de Transparencia y Acceso a la Información Pública reconoce en su artículo 25 que los Datos Personales serán protegidos siempre y de

que ya contamos con una garantía constitucional que nos permite ejercer una protección más efectiva sobre nuestros Datos, no es menos cierto que es necesario contar con una norma legal que reconozca en forma expresa los Derechos de los titulares de los datos personales como lo son, el de acceso, rectificación, cancelación y oposición, así como al recurso ante una autoridad independiente y especializada dotada de facultades sancionatorias.

Es por ello que como Pleno de Comisionados del **INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA,** presentamos el Anteproyecto de **LEY DE PROTECCIÓN DE DATOS PERSONALES**, a través del cual buscamos entregarle a cada hondureña y hondureño, la posibilidad de acceder a su información personal en posesión de cualesquiera terceros, ejerciendo un poder de control sobre las instituciones, públicas o privadas, que disponen de sus datos personales.

Asimismo, el Pleno de Comisionados del **INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA,** expresa que todos los grandes cambios y las grandes empresas comienzan con la voluntad de una sola persona por lo que en el presente caso, efectúa un especial reconocimiento a la **Comisionada Presidenta, Doris Imelda Madrid Zerón,** quien impulsó desde un inicio esta iniciativa para devolverle a cada persona, el control sobre sus propios datos, esfuerzo que se concreta con la entrega al Soberano Congreso Nacional de una propuesta de Ley moderna, actualizada y armonizada con la normativa internacional.

Finalmente, manifestamos que, en resumen, el presente Anteproyecto de **LEY DE PROTECCIÓN DE DATOS PERSONALES** tiene como único propósito que cada hondureña y hondureño tenga el derecho a decidir cuándo, cómo y quién va a tratar su información personal.

GUSTAVO ALDOLFO MANZANARES VAQUERO
Comisionado Secretario

ÍNDICE

NOTA INTRODUCTORIA

Este anteproyecto es el resultado de la revisión de los estándares internacionales en materia de protección de datos personales, específicamente los trabajos que viene realizando la Organización de las Naciones Unidas, a través de la *Resolución 45/95 Principios Rectores para la Reglamentación de las Bases Computarizados de Datos Personales*; el derecho comunitario europeo, mediante la *Directiva 95/46/CE* relativa a la protección de las personas naturales en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; y, la labor del foro regional para el intercambio de experiencias que realiza la Red Iberoamericana de Protección de Datos, reflejada en la *Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad y de los Datos de Carácter Personal*.

Complementado la doctrina jurídica y la revisión de los estándares internacionales, toma en cuenta el análisis comparativo de cinco legislaciones referenciales que han de contribuir a sentar las bases para una ley de protección de datos personales en Honduras:

1. Ley General de Protección de Datos Personales de Colombia.
2. Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales de Costa Rica.
3. Ley Orgánica de Protección de Datos de España.
4. Ley Federal de Protección de Datos Personales en Posesión de los Particulares de México.
5. Ley de Protección de Datos Personales y Acción de Habeas Data de Uruguay.
6. Proyecto de Reglamento Comunitario de Protección de Datos de carácter personal de la Unión Europea.

Este Anteproyecto de Ley de Protección de Datos Personales de Honduras es un primer esfuerzo de proponer una legislación que mejor se pueda adaptar al contexto institucional, jurídico, social y económico de Honduras. A continuación se presenta una breve explicación de su estructura y contenido.

I. El Título I "Disposiciones Generales", establece el objeto de la Ley, el cual consiste en la protección de los datos personales con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. También detalla el ámbito de aplicación de la Ley, haciendo la salvedad que no será aplicable a las bases de datos de

personas naturales destinadas a actividades personales o domésticas; las que tienen por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito. Finalmente, el Título I, define una serie de términos jurídicos y técnicos en materia de protección de datos.

II. El Título II "Principios y Derechos Básicos para la Protección de Datos Personales", presenta la base de la interpretación y aplicación de la normativa de protección de datos.

Ha de ser la brújula que guía el actuar de los titulares y responsables, garantiza la efectiva aplicación del derecho a los titulares y orientan las decisiones del órgano de control como las instancias judiciales. La recopilación de los principios parte de la Resolución 45/95 de la ONU, los establecidos en las legislaciones española, mexicana, uruguaya y costarricense, contextualizado a terminología legal hondureña.

III. El Título III "Derechos de Protección de Datos", dividió en dos capítulos, en el primer capítulo se establecen las disposiciones generales e incluyendo en el mismo el tratamiento de datos de carácter personal de menores de edad. En el segundo capítulo se desarrollan los derechos ARCO, definiendo los conceptos de acceso, rectificación, cancelación y oposición.

IV. El Título IV "Procedimientos para hacer efectivos los Derechos de Acceso, Rectificación, Cancelación y Oposición", describe los procedimientos para ejercer los derechos de acceso, rectificación, cancelación y oposición ante el responsable del tratamiento. Para la recolección de datos, la persona titular o su representante, debe manifestar su consentimiento por escrito; ya sea en un documento físico o electrónico, o en cualquier otra forma legalmente prevista, el cual podrá ser revocado de la misma forma, sin efecto retroactivo. Se incluye el formato y la información que debe contener la solicitud que presenta el titular de los datos personales, los plazos que ha de resolver el responsable del tratamiento y atiende posibles casos especiales que se pueden dar en la práctica o situaciones imprevistas.

V. El Título V "Los Tratamientos y Obligaciones de los responsables" enumera la responsabilidad y los principales deberes que tiene el responsable del tratamiento y el encargado del tratamiento. Es importante

aclarar que ambos sujetos son considerados obligados pero no solidarios. El responsable del tratamiento por ser el que obtiene el consentimiento del titular, es a quien recae el grueso de las obligaciones y sanciones por incumplimiento. Por otro lado, el responsable del tratamiento debe asegurar que los datos que brinde al encargado son correctos y cerciorarse del manejo adecuado de estos por parte de éste.

VI. El Título VI "Seguridad de datos", establece los lineamientos para el responsable del tratamiento y el Instituto de Acceso a la Información Pública (IAIP) en materia de seguridad. El responsable de la base de datos tiene la obligación de adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de la información, evitando su alteración, destrucción o acceso no autorizado. Consecuentemente, quienes intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional o funcional, aún después de finalizada su relación con la base de datos. El IAIP, como órgano regulador establecerá los requisitos y las condiciones que deban reunir las bases de datos, y de las personas que intervengan en la recolección, almacenamiento y uso de los datos.

VII. El Título VII "Categoría Especiales de Datos", regula el tratamiento de los datos sensibles qué utilizados de manera discrecional o abusiva pueden infringir la privacidad e imagen de la persona, causando daños patrimoniales, y/o discriminación. Asimismo, se regulan los datos que manejan los operadores de telecomunicaciones, y aquellos que se utilizan para fines publicitarios y la actividad financiera, crediticia y comercial; en este caso, a pesar que la CNBS tiene su propia normativa, se recalca que los derechos de acceso, rectificación, cancelación y oposición se aplican también a normas especiales. Estableciendo también en esta categoría las bases de datos de las Fuerzas y Cuerpos de Seguridad, y desarrollando lo relativo a la video vigilancia.

VIII. El Título VIII "Cesión de Datos y Prestación de Servicios" aclara que el responsable del tratamiento de la base de datos, pública o privada, solo podrá comunicar los datos contenidos en ellas cuando el titular haya dado su consentimiento expreso e inequívoco, y se haga sin vulnerar los principios y derechos reconocidos en esta Ley y su Reglamento. Asimismo, presenta una serie de supuestos considerados como excepciones al consentimiento requerido para ceder datos personales.

CONTENIDO

CONSIDERANDO: Que la intimidad como derecho fundamental es reconocido en los instrumentos internacionales relativos a los Derechos Humanos ratificados por Honduras, entre estos el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana de Derechos Humanos, al disponer que toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad, que nadie puede ser objeto de injerencias arbitrarias o ilegales en su vida privada, la de su familia, ni de ataques a su honra o reputación, y que toda persona tiene derecho a la protección de la ley contra esas injerencias o ataques.

CONSIDERANDO: Que la Constitución de la República establece que la persona humana es el fin supremo de la sociedad y del Estado. Todos tienen la obligación de respetarla y protegerla.

CONSIDERANDO: Que la Constitución de la República garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen.

CONSIDERANDO: Que ante los avances sociales, económicos y tecnológicos globalizadores es imperante que el Estado de Honduras establezca unos niveles de protección adecuados de datos personales registrados en bases de datos para garantizar el derecho al honor, a la intimidad personal, familiar y a la propia imagen.

CONSIDERANDO: Que el Instituto de Acceso a la Información Pública, es el órgano responsable de la protección de datos personales y de establecer los lineamientos y políticas generales para el manejo, mantenimiento, seguridad y protección de los datos personales, que estén en posesión de las dependencias y entidades.

LEY DE PROTECCIÓN DE DATOS PERSONALES

TÍTULO I
DISPOSICIONES GENERALES
CAPÍTULO ÚNICO

Artículo 1.- Objeto y Fin. La presente Ley es de orden público y de observancia general en toda la República y tiene por objeto la protección de los datos personales con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la protección de datos personales.

Artículo 2.- Ámbito de Aplicación. Esta Ley será de aplicación a los datos personales registrados en bases de datos automatizadas o manuales, de organizaciones del sector público como del sector privado, y a toda modalidad de uso posterior de estos datos. El IAIP aplicará la presente Ley cuando:

a) El tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio de la República de Honduras.

b) El responsable del tratamiento no esté establecido en el territorio de la República de Honduras, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público.

c) El responsable del tratamiento no esté establecido en el territorio de la República de Honduras y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el citado territorio de la República de Honduras, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por dicho territorio.

En el caso de los literales b) y c) antes mencionados, el responsable del tratamiento deberá designar un representante establecido en el territorio de la República de Honduras, sin perjuicio de las acciones que pudieran promoverse contra el propio responsable del tratamiento.

El régimen de protección de datos personales que se establece en la presente Ley, no será de aplicación a:

a) Las bases de datos mantenidas por personas naturales en el ejercicio de actividades exclusivamente personales o domésticas.
b) Las bases de datos que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito.
c) Las bases de datos creadas y reguladas por leyes especiales.

Artículo 3.- Definiciones. Para efectos de esta ley se entiende por:

1. **Aviso de privacidad:** Documento físico, electrónico o en cualquier otro formato generado por el responsable del tratamiento que es puesto a disposición del titular, previo al tratamiento de sus datos personales.
2. **Base de datos:** Conjunto organizado de datos personales que sea objeto de tratamiento o procesamiento, automatizado o manual, cualquiera que sea la modalidad de su elaboración, organización o acceso.

3. **Dato Anonimizado:** Es aquel dato no asociado a persona identificada o identificable, por haberse destruido el nexo con toda la información que identifica al sujeto.
4. **Cesión de datos:** Toda revelación de datos realizada a personas distintas del interesado.
5. **Computación en la nube (Cloud Computing):** Conjunto de servicios basados en la web en los que los usuarios disponen de una gran variedad de capacidades funcionales por las que pagan solo en la medida que las usan, que se basa en la compartición de recursos en la red en lugar de utilizar servidores locales o propietarios de cada organización.
6. **Consentimiento:** Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular consienta el tratamiento de datos personales que le concierne.
7. **Cookies:** Archivo de texto que los navegadores almacenan en los ordenadores de los usuarios y que, posteriormente, pueden ser actualizados y recuperados por la entidad responsable de su instalación con diversas finalidades.
8. **Datos personales:** Cualquier información numérica, acústica, alfabética, biométrica, gráfica, fotográfica, de imagen, o de cualquier otro tipo concerniente a una persona natural identificada o identificable.
9. **Datos sensibles:** Aquellos que se refieran a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada, tales como: Los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud, físicos o psíquicos y preferencias sexuales, así como cualquier otra información considerada como tal por ley; y, cualquier otro dato respecto de la libertad individual protegido por la Constitución de la República o en Convenios Internacionales suscritos por Honduras.
10. **Datos electrónicos:** Información almacenada en forma de bites que solo puede ser de acceso a través de un dispositivo electrónico.
11. **Delegado de protección de datos:** Aquella persona independiente que con una función claramente preventiva y proactiva, supervisa, coordina y transmite la política de protección de datos al responsable del tratamiento, al afectado y a la autoridad de control.
12. **Derecho al olvido:** Derecho que tiene el titular de un dato personal a borrar, bloquear o suprimir información personal que se considera obsoleta por el transcurso del tiempo o que de alguna manera afecta el libre desarrollo de alguno de sus derechos fundamentales.
13. **Derechos ARCO:** Los derechos de acceso, rectificación, cancelación u oposición de datos personales.
14. **Derecho fundamental a la protección de datos:** Es el derecho que toda persona tiene a controlar sus datos personales que se encuentran registrados

en bases de datos de entidades públicas o privadas, personas naturales o jurídicas.

15. **Encargado del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en conjunto con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.
16. **Evaluación de Impacto en la Protección de Datos Personales (EIPD):** Es un análisis de los riesgos que un producto o servicio puede entrañar para la protección de datos de los afectados y, como consecuencia de ese análisis, la gestión de dichos riesgos mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos.
17. **Exportador de datos personales:** La persona natural o jurídica, pública o privada u órgano administrativo situado en la República de Honduras que realice, conforme a lo dispuesto en la presente ley, una transferencia de datos de carácter personal a un país tercero.
18. **Fuentes accesibles al público:** Base de datos cuyo acceso o consulta puede ser efectuado legítimamente por cualquier persona, sin más exigencias que, en su caso, el pago de una contraprestación. No se considerara tal cuando la información sea o tenga una procedencia ilícita. Estas fuentes incluyen el internet y las publicaciones en medios públicos y privados de comunicación.
19. **Grupo de empresas:** Un grupo que comprenda una empresa que ejerce el control y las empresas controladas;
20. **IAIP:** Instituto de Acceso a la Información Pública y Protección de Datos Personales al que hace referencia la Ley de Transparencia y Acceso a la Información Pública.
21. **Importador de datos personales:** La persona natural o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos desde un tercer país, ya sea responsable o encargado del tratamiento o tercero.
22. **Internet de las cosas:** Red de dispositivos interconectados a través de internet que se comunican entre ellos y que pueden realizar acciones en función del entorno y las informaciones que reciben.
23. **Lugar de establecimiento**: Es el «establecimiento principal». En lo que se refiere a los fines, condiciones y medios del tratamiento de datos personales en el responsable del tratamiento:

    I) Es el lugar de su establecimiento en el ámbito territorial de Honduras en el que se adopten las decisiones principales;

    II) En otro caso, es el lugar en donde se ejecutan las principales actividades del tratamiento en el contexto de las actividades de un establecimiento del responsable del tratamiento en Honduras.

    Por lo que respecta al encargado del tratamiento, se entiende el lugar de su administración central en Honduras.

24. **Normas corporativas vinculantes:** Las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de Honduras para las transferencias o un conjunto de transferencias de datos personales a un responsable o encargado del tratamiento en uno o más países terceros, dentro de un grupo de empresas;
25. **Responsable del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en conjunto con otros, decida sobre la base de datos y/o el tratamiento de los datos.
26. **Titular:** Persona natural cuyos datos personales sean objeto de recolección y tratamiento.
27. **Transferencia internacional de datos:** Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Estado, bien constituya una comunicación o cesión de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del tratamiento establecido en territorio de la República de Honduras.
28. **Tratamiento de datos personales:** Cualquier operación o conjunto de operaciones, efectuadas mediante procedimientos automatizados o manuales y aplicadas a datos personales, tales como la recolección, el registro, el almacenamiento, la modificación, la extracción, la consulta, la utilización, la comunicación, la transferencia, difusión o cualquier otra forma que facilite el acceso a estos, el cotejo o la interconexión, así como su bloqueo, supresión o destrucción.
29. **Tratamientos masivos de datos (Big Data):** Tratamientos de grandes cantidades de datos que tienen por finalidad analizar los mismos, para establecer correlaciones entre ellos con las más diversas finalidades.
30. **Versión pública:** Un documento en el que se testa o elimina la información clasificada como reservada o confidencial para permitir su acceso a la parte pública de dicho documento.
31. **Violación de datos personales:** Toda violación de la seguridad que ocasione la destrucción accidental o ilícita, la pérdida, alteración, comunicación no autorizada o el acceso a datos personales transmitidos, conservados o tratados de otra forma.

TÍTULO II

PRINCIPIOS Y DERECHOS BÁSICOS PARA LA PROTECCIÓN DE DATOS PERSONALES

CAPÍTULO I
PRINCIPIOS RECTORES

Artículo 4.-Principios para la protección de datos personales. La actuación de los responsables de los tratamientos, tanto públicos como privados, y, en general,

de todos quienes actúan en relación a datos personales de terceros, deberá ajustarse a los siguientes principios generales, los cuales se han de aplicar, de manera armónica e integral:

a. **Principio de lealtad y legalidad:** Los datos personales no se recolectaran ni elaborarán con procedimientos desleales o ilícitos, ni se utilizarán con fines contrarios a los propósitos establecidos por esta Ley y demás normativa aplicable.
b. **Principio de exactitud:** Los datos personales que se recolecten deberán ser exactos, adecuados, necesarios y no excesivos en relación con la finalidad para la cual se hubieran obtenido.

   El responsable del tratamiento tendrá la obligación de verificar la exactitud y pertinencia de los datos registrados y tomará las medidas necesarias en cuanto tenga conocimiento o constate el error, con respecto a los fines para los que fueron recolectados o para los que fueron tratados posteriormente, sean cancelados o rectificados.
c. **Principio de finalidad de propósito:** El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades determinadas, explícitas y legítimas del titular de los mismos. De igual forma el responsable o el encargado del tratamiento, deberá limitarse al cumplimiento de las finalidades previstas en la presente Ley.

   Si el responsable del tratamiento pretende tratar los datos para un fin distinto que no resulte compatible a los fines para los cuales fueron recolectados, requerirá obtener nuevamente el consentimiento del titular.

   No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.
d. **Principio de acceso a información:** Los datos personales deberán ser almacenados de modo que permitan al titular de los mismos su acceso o conocimiento. En el tratamiento debe garantizarse el derecho del titular a obtener del responsable del tratamiento, en cualquier momento de acuerdo con lo previsto en esta Ley, información acerca de la existencia de datos que le conciernan.
e. **Principio de consentimiento:** El tratamiento sólo puede ejercerse con el consentimiento, libre, previo, expreso e informado del titular. La acreditación de que dicho consentimiento ha sido prestado por el titular de los datos, corresponderá al responsable del tratamiento. Los datos personales no podrán ser obtenidos o comunicados sin previa autorización, o en ausencia de mandato legal, resolución administrativa o judicial, que sustituya el consentimiento.

   El consentimiento prestado podrá no ser considerado como tal, cuando exista un desequilibrio evidente entre la posición del interesado y el responsable del tratamiento.

f. **Principio de no discriminación:** No deberán registrarse datos sensibles que puedan originar discriminación, en particular información que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, así como los relativos a la salud y a la vida sexual. Los datos biométricos no podrán ser utilizados como elementos de discriminación o arbitrariedad.
g. ***Principio de seguridad:*** *La información sujeta a tratamiento por el* responsable o encargado del tratamiento, se deberá manejar con las medidas de seguridad, técnicas y organizativas, que sean necesarias para otorgar seguridad a las bases de datos evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
h. **Principio de responsabilidad:** El responsable o encargado del tratamiento deberá cumplir con los principios y obligaciones de la presente Ley y dotarse de aquellos mecanismos necesarios para evidenciar dicho cumplimiento, tanto ante los interesados como ante el IAIP en el ejercicio de sus competencias y facultades.
i. **Principio de proporcionalidad:** El responsable del tratamiento solo deberá recolectar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.
j. **Principio de confidencialidad**: Es el deber que tiene el responsable o el encargado del tratamiento de no mostrar, compartir, revelar o transmitir la base de datos a personas naturales o jurídicas que carezcan de la previa autorización por parte del titular.

Artículo 5.- Excepciones a los principios y derechos para la protección de datos personales. Los principios, los derechos y las garantías aquí establecidas podrán ser limitados de manera justa, razonable de acuerdo con el principio de proporcionalidad, cuando se persigan los siguientes fines:

a. La seguridad del Estado.
b. La eficaz actividad ordinaria de la Administración Pública, así como la adecuada prestación de servicios públicos.
c. La prevención, persecución, investigación, detención y represión de las infracciones penales, o de las infracciones de la deontología en las profesiones.
d. Las partes de un precontrato o contrato privado, social o administrativo y que sean necesarios para su nacimiento, desarrollo y cumplimiento.
e. La preparación y desarrollo de los procesos electorales.
f. Los procedimientos judiciales de toda índole.

CAPÍTULO II
DERECHOS DEL TITULAR DE LOS DATOS

Artículo 6.- Derechos frente a la recolección de datos. El titular tiene el derecho a ser informado, a través del aviso de privacidad, en el momento en el que se le soliciten sus datos de carácter personal a conocer de manera expresa, previa, inequívoca y de forma que le sea comprensible, los fines para los cuales se recolecta dicha información.

Artículo 7.- Contenido del aviso de privacidad. El aviso de privacidad deberá contener, al menos, la siguiente información:

a. La identidad y domicilio del responsable del tratamiento de los datos;
b. Las finalidades del tratamiento de datos;
c. La posibilidad de que los datos recolectados sean cedidos o comunicados a un tercero y la identidad y domicilio de dicho cesionario;
d. Las consecuencias de proporcionar los datos y de la negativa a hacerlo o su inexactitud;
e. La manera para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley.

Artículo 8.- Mecanismos de comunicación. El aviso de privacidad debe ponerse a disposición del titular de los datos a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología, de la siguiente manera:

a. Cuando los datos personales hayan sido obtenidos personalmente del titular, el aviso de privacidad deberá ser facilitado en el momento en que se recolecte el dato de forma clara y fehaciente, a través de los formatos establecidos, salvo que se hubiera facilitado el aviso con anterioridad. Cuando se obtengan por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, el responsable del tratamiento deberá proporcionar al titular de manera inmediata, la información a que se refiere el artículo anterior.
b. Cuando los datos personales no hayan sido recolectados del titular, el responsable del tratamiento, deberá dar a conocer al titular el aviso de privacidad, dentro de los treinta (30) días calendario, siguientes al momento del registro de los datos; el titular podrá oponerse al tratamiento en el plazo de diez (10) días calendario siempre que así se lo comunique al responsable del tratamiento.

Cuando resulte imposible dar a conocer el aviso de privacidad al titular o exija esfuerzos desproporcionados, en consideración al número de titulares, la antigüedad de los datos o cualquier circunstancia análoga, previa autorización del IAIP, el responsable podrá instrumentar medidas compensatorias en términos del

Reglamento de esta Ley.

Artículo 9.- Excepción al consentimiento previo del titular. No será necesario el consentimiento previo e informado cuando:

a. Los datos provengan de fuentes públicas de información, tales como internet o publicaciones en medios públicos y privados de comunicación;
b. Se recolecten para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;
c. El Registro Nacional de las Personas recolecte, trate, verifique y disponga de los datos a los que se hace referencia en el artículo 109 de Ley de Registro Nacional de las Personas.
d. La Ley Electoral y de las Organizaciones Políticas se refiera a la recolección, tratamiento y cesión de datos, concernientes a la organización y desarrollo de los procesos electorales.
e. Deriven de una relación contractual, del titular de los datos, y sean necesarios para su nacimiento, desarrollo y ejecución;
f. Se realice por personas naturales para su uso exclusivo, personal o doméstico;
g. El tratamiento responda o sea consecuencia de un interés legítimo del responsable del tratamiento.

TÌTULO III
DERECHOS DE PROTECCION DE DATOS

CAPÌTULO I
DISPOSICIONES GENERALES

Artículo 10.-Consideraciones generales. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad. En este caso, el afectado tendrá derecho a obtener información del responsable de la base de datos sobre los criterios de valoración y el tratamiento que sirvió para adoptar la decisión en que consistió el acto.

La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del

afectado.

Artículo 11.- El tratamiento de datos de carácter personal de menores de edad. Podrá procederse al tratamiento de los datos de los mayores de dieciséis (16) años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de dieciséis (16) años se requerirá el consentimiento de los padres o tutores.

En ningún caso podrán recabarse del menor, datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.

Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.

Corresponderá al responsable de la base de datos, articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.

CAPITULO II
DERECHOS ARCO

Artículo 12.-Derecho de acceso. El titular tiene derecho a solicitar y ser informado sobre sus datos personales que estén en posesión del responsable o encargado del tratamiento, el origen de dichos datos, el tratamiento del cual sean objeto, las cesiones realizadas o que se pretendan realizar, así como a tener acceso al aviso de privacidad al que está sujeto el tratamiento, en los términos previstos en la ley. El ejercicio de este derecho siempre será gratuito.

El responsable del tratamiento, debe responder al ejercicio del derecho de acceso, incluso en los casos en los que no haya tratado datos de carácter personal del interesado en su base de datos.

Artículo 13.-Derecho de rectificación. El titular tendrá derecho a solicitar la rectificación de sus datos personales cuando sean inexactos, incompletos, inadecuados o excesivos, siempre que sea posible y no exija esfuerzos desproporcionados.

El responsable del tratamiento tiene la obligación de poner en conocimiento a quienes haya cedido o comunicado los datos de la rectificación realizada para que también proceda a hacer la respectiva rectificación.

Artículo 14.- Derecho de cancelación. La cancelación de datos personales procede a solicitud del titular cuando se presente alguno de los siguientes supuestos:

a. Se dé un tratamiento a los datos personales en contravención a lo dispuesto por la presente Ley;
b. Los datos personales hayan dejado de ser necesarios para el cumplimiento de la finalidad o finalidades de la base de datos previstas en el aviso de privacidad.

Sin perjuicio de lo que disponga la normativa aplicable al caso concreto, el responsable procederá a la cancelación de datos, previo bloqueo de los mismos.

Cuando los datos personales hubiesen sido comunicados a la fecha de cancelación deberán comunicárseles el ejercicio del derecho, quienes deberán realizar también la rectificación correspondiente.

El "derecho al olvido" y las condiciones de ejercicio del borrado, bloqueo o supresión de datos correspondientes a cualquier titular o afectado que se consideren obsoletos por el transcurso del tiempo, o que de alguna manera afecten al libre desarrollo de alguno de sus derechos fundamentales, será desarrollado reglamentariamente.

Del mismo modo, las instituciones públicas tendrán la obligación de elaborar versiones públicas las resoluciones a los efectos de divulgación pública en bases de datos, colecciones legislativas y jurisprudenciales o gacetas.

Artículo15.-Cancelación, conservación y bloqueo de los datos. Los datos personales una vez que dejen de ser necesarios para la finalidad o finalidades para los que se recolectaron, deberán ser cancelados.

La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades que pudieran reclamarse.

La conservación de tales datos lo será a elección del responsable del tratamiento, por el plazo derivado de las relaciones contractuales entre la persona o entidad responsable del tratamiento y el titular de dichos datos, o la extinción de las responsabilidades nacidas del tratamiento.

Cumplido el citado plazo deberá procederse a la supresión o borrado de los datos.

Artículo 16.-Derecho de oposición. El titular de los datos tendrá derecho a oponerse al tratamiento de sus datos personales en el supuesto en que los datos se hubiesen recolectado sin su consentimiento, cuando existan motivos fundados para ello y la Ley no disponga lo contrario. La procedencia del derecho de oposición, dará lugar a la cancelación de los datos, previo bloqueo de los mismos.

Artículo 17.-Derecho referente a la comunicación de datos. El responsable del tratamiento solo podrá ceder o comunicar los datos contenidos en la base de datos, cuando el titular haya dado su consentimiento expreso e inequívoco, y se haga sin vulnerar los principios y derechos reconocidos en esta Ley y su Reglamento.

Artículo 18.-Derecho al ejercicio de acciones derivado de la vulneración de esta normativa. El titular de los datos que considere que ha sufrido un daño o lesión en sus bienes o derechos como consecuencia del incumplimiento a lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, podrá ejercer las acciones que estime pertinentes derivadas de los daños y perjuicios sufridos, o en el ejercicio de cualquier otra pretensión que sea procedente en derecho.

TÍTULO IV

PROCEDIMIENTOS PARA HACER EFECTIVOS LOS DERECHOSDE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN

CAPÍTULO ÚNICO

Artículo 19.- Ejercicio de los derechos de acceso, rectificación, cancelación y oposición. El titular, o en su caso su representante, podrá ejercer los derechos de acceso, rectificación, cancelación u oposición en los términos previstos en la presente Ley. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de cualquier otro derecho. La procedencia de estos derechos, en su caso, se hará efectiva una vez que el titular o su representante acrediten su identidad o representación, respectivamente. El responsable del tratamiento tiene, en todo caso, obligación de dar respuesta al derecho ejercitado.

Artículo 20.- Designación de representante. Todo responsable o encargado del tratamiento deberá designar con carácter inmediato un representante que se responsabilice de dar una respuesta a la mayor brevedad posible a la solicitud del titular de los datos o su representante, a consecuencia del ejercicio de los derechos a que se refiere la presente Ley. Dicho nombramiento podrá ser verificado, en su caso, por el IAIP.

Artículo 21.- Contenido de la solicitud. La solicitud de acceso, rectificación, cancelación u oposición se podrá presentar de manera escrita o por medio electrónico, conteniendo como mínimo, los siguientes requisitos:

a. Lugar y fecha en que se presenta la solicitud.
b. El responsable o encargado del tratamiento a quien se dirija;
c. El nombre del titular de los datos;
d. Los documentos que acrediten la identidad o, en su caso, la representación del titular;
e. La descripción clara y precisa de los datos personales respecto de los que se pretende ejercer alguno de los derechos antes mencionados;
f. El medio elegido para comunicarle la respuesta a su solicitud, yasea por escrito, por medio electrónico o en la forma prescrita por el responsable o el encargo del tratamiento; y
g. Cualquier otro elemento o documento que facilite la localización de los datos personales.

Artículo 22.- Entrega de información sobre datos personales. La información, debe ser proporcionada por el responsable o encargado del tratamiento, dentro de los diez (10) días hábiles después de haber sido solicitada, entregándose en forma clara y sencilla.

Cuando no fuere posible atender la solicitud de acceso, rectificación, cancelación u oposición a datos personales dentro de dicho plazo, se informará al titular o a su representante bajo cualquier título, expresando los motivos del retraso y señalando la fecha en que se atenderá la solicitud, la cual en ningún caso podrá superar los diez (10) días hábiles siguientes al vencimiento del primer plazo.

Artículo 23.- Límite temporal al ejercicio del derecho de acceso. La solicitud de acceso a datos personales almacenados en una base de datos solamente se podrá realizar en intervalos de seis (6) meses calendario, salvo que el titular haga constar en su solicitud la existencia de un interés legítimo, y una causa debidamente justificada.

Artículo 24.- Procedimiento de rectificación, cancelación u oposición.- El titular de los datos que considere que sus datos personales almacenados en una base de datos deben ser objeto de rectificación, cancelación u oposición, presentará una solicitud ante el responsable o encargado del tratamiento, la cual será tramitada bajo las siguientes reglas:

a. La solicitud ha de cumplir con las formalidades establecidas en el artículo 19de la presente Ley. En el caso de solicitud de rectificación de datos personales, el titular de los mismos deberá indicar, las modificaciones a realizar y aportar la documentación en que justifique su petición.
b. Si la solicitud resulta incompleta, el responsable o encargado del tratamiento requerirá al interesado dentro de los tres (3) días siguientes para que proceda a la subsanación de la misma. Transcurridos dos (2) meses calendario desde la fecha del requerimiento, sin que el interesado presente la información solicitada, se entenderá que ha desistido de dicha solicitud.
c. Una vez subsanada la solicitud, el responsable o encargado del tratamiento incluirá en la base de datos una leyenda que diga "solicitud en trámite" y el motivo de la misma, en un plazo no superior a tres (3) días hábiles. Dicha leyenda deberá mantenerse hasta que la solicitud sea resuelta.
d. El plazo para atender la solicitud será de diez (10) días hábiles contados a partir del día siguiente de recibida la solicitud, o una vez que haya dado cumplimiento al requerimiento establecido en el apartado b) del presente artículo. Cuando no fuere posible atender la solicitud dentro de dicho término, se informará al interesado de los motivos del retraso, y la fecha en que se atenderá previsiblemente su solicitud, la cual en ningún caso podrá superar los diez (10) días hábiles siguientes al vencimiento del primer plazo.
e. El responsable o encargado del tratamiento comunicará al titular de los datos la determinación adoptada en un plazo máximo de diez (10) días hábiles, contados a partir de la fecha en que se recibió la solicitud de rectificación, cancelación u oposición, a los efectos de que, si resulta procedente, se haga efectiva la misma en el plazo descrito en el inciso anterior.

Cuando los datos personales hubiesen sido comunicados a terceros, con anterioridad a la fecha de rectificación o cancelación, el responsable o encargado del tratamiento deberá poner en conocimiento de dicho tercero en el plazo de los diez (10) días siguientes, el ejercicio de derechos por parte del titular de los datos, para que proceda también a dar cumplimiento a dicho derecho en igual término.

Artículo 25.- Denegación justificada al acceso, rectificación, cancelación u oposición. El responsable o encargado del tratamiento podrá denegar el acceso a los datos personales, o a realizar la rectificación, cancelación, o conceder la oposición al tratamiento de los mismos, en los siguientes supuestos:

a. Cuando el solicitante no sea el titular de los datos personales, o el representante no esté debidamente acreditado para ello;
b. Cuando en su base de datos, no se encuentren los datos personales del solicitante;
c. Cuando se lesionen los derechos de un tercero;
d. Cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos, y;
e. Cuando el ejercicio de los derechos de rectificación, cancelación u oposición haya sido ya satisfecho.

En todos los casos anteriores, el responsable o encargado del tratamiento deberá informar el motivo de su decisión y comunicarla al titular de los datos, o en su caso, a su representante, en un plazo máximo de diez (10) días hábiles siguientes a la recepción de la solicitud, por el medio designado por el titular, acompañando, en su caso, los documentos o pruebas que resulten pertinentes.

La negativa a que se refiere este artículo podrá ser parcial, en cuyo caso el responsable o encargado del tratamiento dará respuesta al ejercicio de los derechos de acceso, rectificación, cancelación u oposición efectuados por el titular.

Artículo 26.- Excepciones a los derechos de acceso, rectificación, cancelación u oposición. El responsable o encargado del tratamiento que contenga los datos podrá denegar el acceso, la rectificación o cancelación en función de los riesgos que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

Los responsables de la base de datos de la Secretaría de Estado en el Despacho de Finanzas podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas enfocadas a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del IAIP, el que deberá asegurarse de la procedencia o improcedencia de la denegación.

TÍTULO V

LOS TRATAMIENTOS Y LAS OBLIGACIONES DE LOS RESPONSABLES

CAPITULO I
CUESTIONES GENERALES

Artículo 27.- Responsabilidad del responsable del tratamiento. El responsable del tratamiento debe garantizar, en todo caso, la protección de los datos del titular de los mismos en cada tratamiento que realice.

Consecuentemente con ello, se establece la responsabilidad general del responsable por cualquier tratamiento de datos personales realizado por él mismo o en su nombre. En particular, el responsable del tratamiento debe garantizar y está obligado a demostrar que cada operación de tratamiento cumple lo dispuesto en la presente Ley.

Asimismo, el responsable del tratamiento debe garantizar que los datos personales no sean accesibles a un número indeterminado de personas.

Artículo 28.-La adopción de medidas preventivas y las evaluaciones de impacto. El IAIP, a los efectos de prevenir las violaciones de los datos de carácter personal podrá exigir al responsable y al encargado de tratamiento la adopción de medidas preventivas que eviten la comisión de infracciones de privacidad.

En este sentido, se podrá exigir la realización de una consulta previa por parte del responsable ante dicha autoridad de control en relación con operaciones de tratamiento que probablemente impliquen riesgos específicos para los derechos y libertades de los titulares de los datos, en razón de la naturaleza, alcance, y/o fines del tratamiento.

Dicha consulta previa no será necesaria cuando:

a. El responsable del tratamiento sea una autoridad u organismo público.
b. El tratamiento se efectúe en cumplimiento de una obligación legal.

Las medidas preventivas a implantar así como el procedimiento a seguir en la *realización de estas consultas de carácter previo será objeto del correspondiente* desarrollo reglamentario.

Cuando el IAIP considere que el tratamiento previsto no es conforme a lo dispuesto en la Ley, en particular cuando los riesgos no estén suficientemente identificados o atenuados prohibirá el tratamiento pudiendo, en su caso, efectuar propuestas para

remediar dicha falta de conformidad.

Artículo 29.- Delegado de Protección de Datos. El responsable del tratamiento deberá designar un delegado de protección de datos en los siguientes supuestos:

a) Cuando el tratamiento sea llevado a cabo por una autoridad u organismo público.
b) Cuando el tratamiento sea llevado a cabo por una empresa que emplee a doscientas cincuenta personas o más.
c) Cuando las actividades principales del responsable o del encargado del tratamiento consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran un seguimiento periódico y sistemático de los interesados.

Reglamentariamente se regularán su perfil profesional, funciones, sus relaciones con la autoridad de control, y cuantas otras cuestiones afecten o puedan afectar al desarrollo de su actividad.

CAPÍTULO II
DEBERES DEL RESPONSABLE Y ENCARGADO DEL TRATAMIENTO

Artículo 30.- Deberes del responsable del tratamiento. El responsable del tratamiento deberá cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente Ley y en su Reglamento:

a. Garantizar al titular de los datos, el pleno y efectivo ejercicio del derecho fundamental a la protección de sus datos personales;
b. Informar debidamente al titular de los datos acerca de la finalidad de la recolección y los derechos que le asisten, sobre la base del consentimiento otorgado;
c. Cumplir con las obligaciones contenidas en el aviso de privacidad.
d. Tramitar y dar respuesta a las solicitudes de acceso, rectificación, cancelación y oposición en los términos previstos en la presente Ley;
e. Adoptar las medidas de seguridad técnicas y organizativas necesarias para conservar la información e impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
f. Dar instrucciones claras y precisas al encargado del tratamiento para que éste pueda llevar a cabo el tratamiento adecuado;
g. Adoptar las medidas necesarias para que la información suministrada se mantenga actualizada;
h. Exigir al encargado del tratamiento en todo momento, el respeto a las

condiciones de seguridad y privacidad de la información del titular;

i. Implementar un manual de políticas y procedimientos de seguridad para garantizar el adecuado cumplimiento de la presente Ley;
j. Registrar en la base de datos la leyenda "Solicitud en Trámite" en la forma en que se regula en la presente Ley;
k. Abstenerse de comunicar o ceder información que se encuentre bloqueada por el IAIP;
l. Informar al IAIP, cuando se presenten eventos que deriven en violaciones a las políticas y procedimientos de seguridad y existan riesgos en la administración de la información de los titulares de los datos,
m. Cumplir las instrucciones y requerimientos que imparta el IAIP, y
n. Cumplimentar los derechos de acceso, rectificación, cancelación y oposición (ARCO) ejercitados ante el encargado del tratamiento, cuando contractualmente el responsable haya asumido dicha obligación.

Artículo 31.- Deberes del encargado del tratamiento. El encargado del tratamiento deberá cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente Ley y su Reglamento:

a. Garantizar al titular de los datos, en todo tiempo, el pleno y efectivo ejercicio del derecho fundamental de protección de datos personales;
b. Adoptar las medidas de seguridad técnicas y organizativas necesarias para conservar la información e impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
c. Tramitar y dar respuesta a las solicitudes de acceso, rectificación, cancelación y oposición en los términos previstos en la presente Ley;
d. Actualizar la información proporcionada por el responsable del tratamiento dentro de los cinco (5) días hábiles contados a partir de la respectiva notificación;
e. Implementar un manual de políticas y procedimientos de seguridad para garantizar el adecuado cumplimiento de la presente Ley;
f. Registrar en la base de datos la leyenda "solicitud en trámite" en la forma en que se regula en la presente Ley;
g. Abstenerse de comunicar o ceder información que se encuentre bloqueada por el IAIP;
h. Informar al IAIP, cuando se presenten eventos que deriven en violaciones a las políticas y procedimientos de seguridad y existan riesgos en la administración de la información de los Titulares de los datos, y
i. Cumplir las instrucciones y requerimientos que imparta el IAIP.

Artículo 32.-Obligación de informar a la Gerencia de Protección de Datos (PRODATOS) del IAIP. El responsable del tratamiento está obligado a informar

inmediatamente a la Gerencia de Protección de Datos (PRODATOS) del IAIP sobre cualquier brecha en la seguridad en sus bases de datos y en un plazo máximo de seis (6) horas desde que se produjo dicho evento o que se tuvo conocimiento del mismo.

TÍTULO VI
SEGURIDAD DE DATOS

CAPÍTULO ÚNICO

Artículo 33.- Seguridad de los datos. El responsable del tratamiento deberá adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, destrucción, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a esta Ley.

Dichas medidas deberán incluir, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual, para garantizar la protección de la información almacenada.

Las bases de datos en las que se registren datos de carácter personal deberán reunir las condiciones que garanticen plenamente la seguridad y la integridad de los mismos.

Por vía de Reglamento se establecerán los requisitos y las condiciones que deban reunir las bases de datos, y en las personas que intervengan en la recolección, almacenamiento y uso de los datos, así como las medidas de seguridad exigibles a las bases de datos en función de la calidad de los datos que sean objeto de tratamiento.

Artículo 34.- Deber de confidencialidad. El responsable del tratamiento y quienes intervengan en cualquier fase del tratamiento de datos personales están obligados a guardar secreto, aun después de finalizada su relación con la base de datos.

Artículo 35.- Manual de políticas y procedimientos de seguridad. El responsable del tratamiento elaborará un manual de políticas y procedimientos en el cual establecerá los pasos que deberá seguir en la recolección, el almacenamiento, el manejo de los datos personales y las medidas de seguridad técnicas y organizativas, de conformidad con las disposiciones previstas en esta

Ley, su Reglamento, y demás normativa aplicable.

El manual de políticas y procedimientos de seguridad, así como sus posteriores modificaciones, serán aprobados por el IAIP; el cual podrá verificar, en cualquier momento, que la base de datos esté cumpliendo cabalmente con los términos de dicho manual.

TÍTULO VII
CATEGORIAS ESPECIALES DE DATOS
CAPÍTULO ÚNICO

Artículo 36.- Datos sensibles. Son aquellos que se refieren a la vida privada del titular de los datos y que se encuentran definidos en el artículo 3 apartado e) de la presente ley.

Artículo 37.- Tratamiento de datos sensibles. Los datos sensibles podrán ser objeto de tratamiento cuando:

a) El titular haya dado su consentimiento expreso a dicho tratamiento, salvo en los casos en que por ley no sea requerido el otorgamiento de dicha autorización.
b) El tratamiento sea necesario para salvaguardar el interés vital del titular de los datos y éste se encuentre jurídicamente incapacitado, debiendo mediar, en tal caso, la autorización de su representante.
c) El titular de los datos autorice que el tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de partidos políticos, sindicatos o asociaciones civiles.
d) El tratamiento de los datos se realice con finalidades estadísticas o científicas cuando se disocien de su titular. Lo anterior se entenderá sin perjuicio de lo establecido en la legislación sanitaria.
e) El tratamiento sea necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la prestación de servicios de salud, siempre que dicho tratamiento de datos se realice por un profesional de la salud.

Artículo 38.- Datos relativos a las telecomunicaciones y comunicaciones electrónicas. Los operadores autorizados para prestar a terceros servicios de telecomunicaciones deberán garantizar, en el ejercicio de su actividad, la protección de los datos conforme a la presente Ley y, en su defecto, a las contenidas en el régimen jurídico de las telecomunicaciones.

Asimismo, deberán adoptar las medidas técnicas y los procesos adecuados para

preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar que sus niveles de protección de los datos personales sean los exigidos por esta Ley. En caso que exista un riesgo particular de violación de la seguridad de la red pública, el operador que explote dicha red o preste servicios de telecomunicaciones y comunicaciones electrónicas informará a los abonados sobre dicho riesgo, y las medidas a adoptar.

Artículo 39.- Datos relativos a bases de datos con fines de publicidad, actividades comerciales o de mercadeo. En la recopilación de la información sobre las direcciones, el reparto de documentos, la publicidad, la venta y otras actividades de naturaleza análoga, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o realizar estudios de mercado, cuando los datos figuren en fuentes accesibles al público, o cuando el titular haya prestado su consentimiento.

Si los datos proceden de fuentes accesibles al público o se trata de evaluaciones comerciales llevadas a cabo por el responsable del tratamiento, éste tendrá la obligación de informar adecuadamente al titular de los datos conforme a las prescripciones establecidas en la presente Ley.

Con relación a lo establecido en el presente artículo, los derechos de acceso, rectificación, cancelación y oposición (ARCO) se ejercerán de acuerdo con lo previsto en la presente Ley.

Artículo 40.- Datos relativos a la prestación de servicios de información de la actividad financiera, crediticia y comercial.

1. Los prestadores de servicios de información financiera, crediticia y comercial en el tratamiento de datos de carácter personal estarán sometidos a lo establecido en esta Ley en lo referente a su actividad exclusivamente.

2. Quienes se dediquen a la prestación de servicios de información financiera, crediticia y comercial sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto, o procedentes de información facilitada por el interesado o con su consentimiento.

3. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones pecuniarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos, con carácter previo a la inscripción en cualquier Base de Datos de solvencia patrimonial y crédito se procederá a notificar al presunto deudor o deudores de la posibilidad de llevar a cabo la inscripción de sus datos de carácter personal a consecuencia de su deuda, para que en el plazo de

treinta días (30) calendario antes de proceder a dicho registro, el deudor pueda cumplir con sus obligaciones. Transcurrido dicho plazo, sin que las mismas se hayan satisfecho, se podrá proceder sin más trámites a la indicada inscripción. Corresponde la acreditación de la notificación al responsable del tratamiento.

4. Deberá procederse a la cancelación de manera inmediata de los datos de carácter personal del deudor o deudores inscritos a consecuencia de la falta de cumplimiento de sus obligaciones, una vez que las mismas hayan sido cumplidas. En ningún caso la inscripción podrá permanecer más del plazo de cinco (5), años, a contar desde que se produjo la mencionada inscripción.

5. En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis (6) meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.

6. Se podrán registrar y ceder los datos de carácter personal que sean necesarios para determinar la solvencia económica de los interesados y que no se refieran, cuando le sean adversos, a más de tres (3) años, siempre que respondan con veracidad a la situación actual de aquéllos.

7.- Con relación a la prestación de servicios financieros, crediticios y comerciales, se aplicarán los derechos de acceso, rectificación, cancelación y oposición en los términos previstos en esta Ley.

8. Para la prestación de cualquier otro servicio de información financiera, crediticia y comercial se tendrán que aplicar las disposiciones contenidas en la presente Ley.

Artículo 41.- El tratamiento de otra clase de datos, o el uso para ello de dispositivos y servicios. El tratamiento de datos numéricos, acústicos, alfabéticos, biométricos, gráficos, fotográficos, de imágenes, cookies o de cualquier otro tipo de dispositivo o servicios concernientes o que afecten a una persona natural identificada o identificable, por sus especiales características, podrá ser objeto de desarrollo reglamentario para su regulación.

Del mismo modo, reglamentariamente podrá ser objeto de especial normativa, la regulación el uso de dispositivos o la prestación de servicios en Internet, especialmente los derivados de las nubes de almacenamiento (cloud computing), los tratamientos masivos de datos (big data), así como los derivados del uso de

dispositivos inteligentes y cualquier otra manifestación de internet aplicada a las cosas.

Los tratamientos de datos de carácter personal derivados de los servicios de telecomunicación u otros de carácter análogo, serán normados por la Ley que regule los mismos.

Artículo 42.- El tratamiento de la imagen en general, y con fines de video vigilancia. La presente Ley abarca el tratamiento de datos personales de imágenes de personas naturales identificadas o identificables, con carácter general y con fines de vigilancia a través de dispositivos móviles, cámaras, videocámaras, vehículos no tripulados (drones) y otros instrumentos análogos.

El tratamiento comprende la grabación, captación, transmisión, difusión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas.

Se considerará identificable una persona cuando su identidad pueda determinarse mediante los tratamientos, sin que ello requiera plazos o actividades desproporcionados.

Las referencias contenidas en esta Ley a videocámaras y cámaras se entenderán hechas también a cualquier medio técnico análogo y, en general, a cualquier sistema que permita los tratamientos previstos en la misma, incluidos los sistemas de circuitos cerrados de televisión.

No se encuentra dentro del ámbito de esta Ley, el tratamiento de los datos personales procedentes de las imágenes obtenidas mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad, ni en general aquellos tratamientos expresamente excluidos del ámbito de esta Ley, que se regirán por las disposiciones sobre la materia.

Tampoco se considera objeto de regulación en esta Ley el tratamiento de imágenes en el ámbito personal y doméstico, entendiéndose por tal el realizado por una persona física en el marco de una actividad exclusivamente privada o familiar salvo que dichas imágenes sean difundidas por cualquier medio.

Sin perjuicio de lo dispuesto en esta Ley, las demás cuestiones referentes a la video vigilancia serán objeto del correspondiente desarrollo reglamentario.

Artículo 43.- Base de datos de las Fuerzas y Cuerpos de Seguridad. Las bases de datos creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recolectado para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.

La recolección y tratamiento de datos de carácter personal para fines de prevención y represión del delito realizados por las Fuerzas y Cuerpos de Seguridad sin el consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para los supuestos de prevención o de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en base de datos específicas establecidas al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad. Las bases de datos previstas en este artículo serán reguladas por la Ley por la que fue creada y en lo no previsto en la misma, por lo dispuesto en la presente Ley. En este sentido, el ejercicio de los derechos de acceso, rectificación, cancelación y oposición quedará supeditado a lo que disponga la legislación sobre dichas bases de datos en función de la propia naturaleza de las mismas.

Dichos datos se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento. A estos efectos, se consideraran especialmente: a) la edad del afectado; b) el carácter de los datos almacenados; c) la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto; d) la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Dicha recolección y tratamiento, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

TÍTULO VIII

CESIÓN DE DATOS Y PRESTACION DE SERVICIOS

CAPÍTULO I

LA CESIÓN DE DATOS

Artículo 44.- Cesión de datos a terceros. Los datos personales 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,

con el previo consentimiento expreso del titular de los datos.

Artículo 45.- Nulidad del consentimiento del titular de los datos. Será nulo el consentimiento para la cesión de datos personales a un tercero, cuando el aviso de privacidad que se le facilita al titular de los datos por parte del responsable del tratamiento, no le permita conocer la finalidad o finalidades que tendrán sus datos personales al ser cedidos a un tercero.

Artículo 46.- Excepciones a la exigencia del consentimiento para ceder datos personales. El consentimiento exigido no será necesario cuando:

a. La cesión se encuentre autorizada por una Ley;
b. El tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo nacimiento, desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con la base de datos de terceros;
c. La cesión que deba efectuarse tenga por destinatario a los operadores de justicia, en el cumplimiento de sus atribuciones según Ley;
d. La cesión se produzca entre organismos de la Administración Pública en el ejercicio de sus funciones y atribuciones legales, y
e. La cesión de datos personales relativos a la salud sea necesaria para atender una emergencia, que requiera acceder a una base de datos, o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre salud pública.

En todo lo demás, el cedente de los datos personales tendrá que observar lo prescrito en la presente Ley.

Artículo47.-Supuestos especiales. En los supuestos en que se produzca una modificación del responsable del tratamiento como consecuencia de una operación de fusión, escisión, transformación y cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la normativa mercantil, no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable del deber de información para con el titular de los datos.

Artículo 48.- Cumplimiento legal por cuenta de terceros. El tercero a quien se le cedan los datos personales, incluso en los casos en que no sea necesario el consentimiento del titular de los mismos, se obliga, por el solo hecho de la cesión, a la observancia de las disposiciones de la presente Ley.

En los supuestos de cesiones de datos en cumplimiento de lo dispuesto en una Ley, el cesionario no tendrá la obligación de informar al titular de los datos acerca del tratamiento de los mismos, pero sí de cumplir la finalidad legal para la cual dichos datos fueron cedidos.

CAPITULO II
EL TRATAMIENTO DE DATOS POR TERCEROS

Artículo 49.- Tratamiento de datos por terceros. El acceso a los datos por parte de un encargado del tratamiento que resulte necesario para la prestación de un servicio al responsable, no se considerará comunicación de datos, siempre y cuando se cumpla lo establecido en la presente Ley.

El servicio prestado por el encargado del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido.

No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado.

Artículo 50.-Contrato de tratamiento de datos por terceros. El tratamiento de datos por cuenta de terceros deberá estar regulado en un contrato que constará necesariamente por escrito, ajustándose siempre a los requisitos establecidos en la presente Ley y estableciéndose expresamente en el mismo:

a) Que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento;
b) Que no los aplicará o utilizará con un fin distinto al que figure en dicho contrato; y,
c) Que no los cederá a otras personas, ni siquiera para su conservación.

En el contrato se estipularán, asimismo, las medidas de seguridad de carácter técnicas y organizativas, a que se refiere el Titulo VI de la presente Ley, referente a la "Seguridad de Datos", que el encargado del tratamiento estará obligado a implementar y cumplir.

Cuando el responsable del tratamiento contrate la prestación de un servicio que involucre un tratamiento de datos personales sometido a lo dispuesto en este Capítulo, deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en esta Ley.

Artículo 51.- Destino de los datos una vez cumplida las previsiones contractuales. El contrato de prestación de servicios deberá contener previsiones con relación al destino de los datos objeto de tratamiento una vez que se hayan cumplido las prestaciones contractuales a las que se deberán someter las partes. En su defecto, el encargado del tratamiento procederá a la devolución, destrucción o borrado seguro de los datos.

El encargado del tratamiento, asimismo, a la finalización del contrato, garantizará al responsable del tratamiento la plena portabilidad de sus datos de modo que se posibilite el cambio de prestador de servicios.

En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato al que se refiere el artículo siguiente, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo.

Artículo 52.- Posibilidad de subcontratación de los servicios. El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiere encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.

No obstante lo dispuesto en el párrafo anterior, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos:

a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar. Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a *la subcontratación.*

b) Que el tratamiento de datos de carácter personal por parte del o los subcontratistas se ajusten a las instrucciones del responsable del tratamiento.

c) Que el encargado del tratamiento y la(s) empresa(s) subcontratista(s) formalicen el contrato, en los términos previstos en el artículo anterior. En este

caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en los dos artículos anteriores.

Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados anteriormente.

La identidad de los subcontratistas y de las prestaciones contractuales a los que los mismos vienen obligados en cada momento del contrato, será conocida por el responsable del tratamiento y se ajustará en todo caso a lo pactado contractualmente.

Artículo 53.- Conservación de los datos por el encargado del tratamiento. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable o al encargado del tratamiento que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

No procederá la destrucción de los datos cuando exista una norma legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del tratamiento dicha conservación.

Sin perjuicio de lo anterior, el encargado del tratamiento tiene la obligación de conservar, debidamente bloqueados, los datos a la finalización de la prestación de los servicios comprometidos durante un tiempo equiparable a las responsabilidades derivadas del tratamiento o de las relaciones contractuales suscritas con el responsable del tratamiento.

TITULO IX
TRANSFERENCIA INTERNACIONAL DE DATOS

CAPITULO UNICO

Artículo 54.- Transferencia internacional de datos. Se permite la transferencia de datos personales, si bien la misma deberá realizarse con países u organismos internacionales que proporcionen niveles de tratamiento y protección adecuados.

El carácter adecuado del nivel de tratamiento y la protección que ofrece el país de destino se evaluará por el IAIP, atendiendo a todas las circunstancias que concurran en la transferencia de datos que se pretenda realizar. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del

tratamiento o de los tratamientos previstos, el país de origen y destino final, las normas de derecho general o sectorial vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, la certificación de Puerto Seguro, así como las normas profesionales y las medidas de seguridad aplicables en dichos países.

Sin perjuicio de lo dispuesto en el primer y segundo párrafo del presente artículo, el IAIP podrá autorizar una o varias transferencias de datos personales a un tercer país que no garantice un nivel adecuado de protección, cuando el responsable del tratamiento ofrezca garantías respecto a la protección de la vida, de los derechos y libertades fundamentales de las personas, y del ejercicio de los respectivos derechos. Dichas garantías podrán derivarse de cláusulas contractuales apropiadas u otras fórmulas análogas.

Vía Reglamento se regularán las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de Honduras para las transferencias o un conjunto de transferencias de datos personales a un responsable o encargado del tratamiento en uno o más países terceros, dentro de un grupo de empresas.

Artículo55.- Transferencia simultánea realizada a diversos países. El IAIP evaluará en los casos de varias transferencias simultáneas a diversos países, la procedencia de las mismas, y que en cada una de ellas se observen las prescripciones contempladas en el presente Titulo de esta Ley.

Artículo 56.- La transferencia internacional de datos a países que no reúnan garantías adecuadas. La prohibición de realizar tales transferencias, no será *aplicable cuando:*

a. El titular de los datos haya dado su autorización explícita a dicho tratamiento;
b. Se requiera el intercambio de datos de carácter sanitario para atender el tratamiento de salud del titular de los datos;
c. La transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrarse en interés del titular de los datos, entre el responsable del tratamiento y un tercero, o para la ejecución de medidas precontractuales tomadas a petición de aquel;
d. Cuando sea necesaria para proteger los intereses vitales del interesado o de otra persona, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento.
e. Cuando sea necesaria para la satisfacción de los intereses legítimos del responsable o del encargado del tratamiento, que no puedan ser calificados de frecuentes ni de masivos, y el responsable o el encargado hayan evaluado

todas las circunstancias que rodean la operación o la serie de operaciones de transferencia de datos y hayan ofrecido en su caso, sobre la base de dicha evaluación, garantías apropiadas con respecto a la protección de datos personales.

f. La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público relevante;
g. La realizada a instancia de la Administración Pública en el ejercicio de sus competencias;
h. La transferencia tenga lugar desde un registro que, en virtud de disposiciones legales o reglamentarias correspondientes se realicepor operadores de justicia o en el marco de la cooperación judicial internacional; y,
i. En el cumplimiento de acuerdos, tratados o convenios Internacionales delos cuales la República de Honduras forme parte.

TÍTULO X
DISPOSICIONES SECTORIALES

CAPÍTULO I
BASES DE DATOS DE TITULARIDAD PÚBLICA

Artículo57.- Adecuación a la normativa sobre transparencia. La creación, modificación o cancelación de bases de datos de titularidad pública siempre estará en concordancia con las disposiciones establecidas en la Ley de Transparencia y Acceso a la Información Pública. El IAIP tendrá la obligación de velar por ello, pudiendo adoptar adicionalmente aquellas medidas que considere oportunas a los efectos de favorecer dicha transparencia informativa.

Reglamentariamente se podrá determinar los procesos de reutilización de la información incorporada a base de datos de naturaleza pública.

Artículo 58.- La creación, modificación o cancelación de bases de datos de titularidad pública. La creación, modificación o cancelación de bases de datos pertenecientes a organismos del sector público deberá registrarse en el IAIP.

Reglamentariamente se determinarán los requisitos que han de reunir las bases de datos del sector público para su registro, que solo será obligatorio para aquellas bases sujetas a la presente Ley.

Cualquier modificación que se produzca en la estructura de dichas bases de datos deberá ser comunicada asimismo al IAIP para proceder a la modificación del

registro. Del mismo modo, la cancelación de las bases de datos, se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción, devolución o borrado seguro.

Artículo 59.- Registro de bases de datos de organismos del sector público. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que deba contener el registro de bases de datos del sector público, entre los cuales figurarán:

a. El organismo público responsable de la base de datos;
b. La finalidad de la base de datos;
c. Las personas naturales sobre las que se pretenda tratar datos personales o que resulten legal o reglamentariamente obligados a suministrarlos;
d. Los procedimientos de recolección de los datos personales y tratamiento de estos;
e. La determinación de los campos donde se van a tratar datos de carácter personal y la descripción de los tipos de datos personales incluidos en ella;
f. La garantía de que se han adoptado medidas de seguridad técnicas y organizativas y de confidencialidad;
g. El destino de los datos y de las personas naturales o jurídicas a las que pueden ser cedidos los datos personales;
h. El tiempo estimado de conservación de los datos personales;
i. La forma y las condiciones que el titular de los datos pueda ejercitar los derechos previstos en esta Ley y la determinación de la instancia administrativa competente para el ejercicio y resolución de dichos derechos;
j. En su caso, las transferencias internacionales de datos que se prevean efectuar a países terceros u organismos internacionales.
k. Cuantas otras informaciones se consideren necesarios o convenientes que consten.

CAPÍTULO II
BASE DE DATOS DE TITULARIDAD PRIVADA

Artículo 60.- Creación de bases de datos privadas. Podrán crearse bases de datos de titularidad privada que contengan datos personales cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular de las mismas, y siempre que se respeten las garantías y los requisitos que esta Ley establece para la creación de dichas bases de datos, y la protección de los datos personales.

Artículo 61.- Registro de bases de datos de titularidad privada. Toda persona

natural o jurídica que proceda a la creación, modificación o cancelación de una base de datos personales, y que no sean para un uso exclusivamente personal o doméstico, deberá registrar la misma previamente ante el IAIP.

Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que deba contener el Registro de bases de datos de carácter privado, entre los cuales figurarán:

a. La persona o entidad responsable del tratamiento de la base de datos;
b. La finalidad de la base de datos;
c. Las personas naturales sobre las que se pretenda tratar datos personales;
d. Los procedimientos de tratamiento de los datos personales;
e. La determinación de los campos donde se van a tratar datos de carácter personal y la descripción de los tipos de datos personales incluidos en ella;
f. La garantía de que se han adoptado medidas de seguridad técnicas y organizativas y de confidencialidad;
g. El destino de los datos y de las personas naturales o jurídicas a las que pueden ser cedidos los datos personales;
h. Tiempo estimado de conservación de los datos personales;
i. Forma y condiciones en que el titular de los datos pueda ejercitar los derechos previstos en esta ley;
j. En su caso, las transferencias internacionales de datos que se prevean efectuar a países terceros u organismos internacionales.
k. Cuantas otras informaciones se consideren necesarios o convenientes que consten.

TÍTULO XI

DE LOS MECANISMOS DE VIGILANCIA Y SANCIÓN

CAPÍTULO I

DEL INSTITUTO DE ACCESO A LA INFORMACION PÚBLICA Y PROTECCIÓN DE DATOSPERSONALES

Artículo 82.- Autoridad de Protección de Datos. Para los objetivos y propósitos de la presente Ley, el Instituto de Acceso a la Información Pública y de Protección de Datos Personales (IAIP) es el responsable de promover y garantizar el derecho fundamental de protección de datos personales, y ejercer la vigilancia para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente Ley y su Reglamento.

Le corresponde al IAIP asumir todas las competencias que se le atribuyen por esta Ley, así como adoptar las resoluciones, elaborar los reglamentos y las demás disposiciones pertinentes para asegurar la correcta aplicación de la presente Ley y su Reglamento. Para tal fin, el IAIP, creará la Gerencia de Protección de Datos Personales (PRODATOS) y determinará en todo momento su estatuto orgánico y funcionamiento. Los servidores públicos al servicio del IAIP y de la Gerencia de Protección de Datos Personales (PRODATOS) estarán, asimismo, sometidos a un estatuto profesional especial, donde se determinará su régimen de incompatibilidades.

Dichos servidores públicos no podrán dedicarse a la actividad desarrollada por el IAIP y por la Gerencia de Protección de Datos Personales (PRODATOS), hasta transcurridos tres años desde su cese de actividad efectivo en dichas Instituciones.

Artículo 64.-Dirección. La Gerencia de Protección de Datos Personales (PRODATOS) estará bajo la dirección, orientación, administración y supervisión de un(a) Gerente el cual será nombrado por el Pleno de los Comisionados del IAIP.

Para ser nombrado Gerente de PRODATOS, se deberá cumplir con los requisitos que se establezcan reglamentariamente.

Artículo 65.- Funciones. El IAIP deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente Ley. A tales efectos tendrá las siguientes funciones:

a. Promover y divulgar los derechos de las personas en relación con el tratamiento de datos personales;
b. Implementar planes de promoción para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos.
c. Colaborar con los titulares de las bases de datos para el desarrollo de proyectos en materia de protección de datos y proporcionar apoyo técnico a los responsables que lo soliciten, para el cumplimiento de las obligaciones establecidas en la presente Ley;
d. Velar por el cumplimiento de la legislación en materia de protección de datos personales, tanto por parte de personas naturales o jurídicas privadas, como por organismos públicos.
e. Recomendar los ajustes, correctivos y/o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional.
f. Solicitar a los responsables y encargados del tratamiento la información que sea necesaria para el ejercicio efectivo de sus funciones.

g. Desarrollar, fomentar y difundir análisis, estudios e investigaciones en materia de protección de datos, de toda índole que garanticen el cocimiento del régimen jurídico de la protección de datos y el cumplimiento del mismo, de acuerdo con las previsiones contenidas en esta Ley.
h. Realizar y mantener actualizado un registro de bases de datos inscritas de acuerdo a lo previsto en la presente Ley.
i. Realizar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de protección de datos.
j. Conocer y resolver los procedimientos de protección y de verificación de derechos señalados en esta Ley;
k. Conocer y resolver los recursos de revisión interpuestos por los titulares en el marco de esta ley.
l. Realizar las inspecciones y verificaciones que sean necesarias para la correcta aplicación de los derechos de protección de datos.
m. Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva.
n. Ejercitar las funciones sancionadoras previstas en la presente Ley.
o. Administrar el Registro Nacional de Protección de Datos, y emitir las órdenes y los actos necesarios para su administración y funcionamiento.
p. Emitir autorizaciones de conformidad sobre las transferencias internacionales de datos.
q. Cooperar con otras autoridades de supervisión y organismos nacionales e internacionales, a efecto de coadyuvar en materia de protección de datos.

Artículo 66. El Registro Nacional de Protección de Datos. El IAIP podrá constituir, en su caso, un Registro General de Protección de Datos, a los efectos de posibilitar la inscripción, la modificación, la cancelación, las reclamaciones, los recursos contra las resoluciones correspondientes, y demás extremos y actuaciones que se consideren pertinentes de acuerdo con el contenido de la presente Ley.

En el Registro Nacional de Protección de Datos serán objeto de inscripción:

a. Las bases de datos gestionadas por organismos del sector público;
b. Las bases de datos de titularidad privada;
c. El nombre del responsable del tratamiento que tiene a su cargo la base de datos;
d. La denominación de la base de datos y el tipo de datos personales objeto de tratamiento.

e. Los datos relativos a las bases de datos que sean necesarios para el ejercicio de los derechos previstos en esta Ley, así como la unidad administrativa ante la cual podrán ejercitarse dichos derechos.
f. Las personas naturales, jurídicas u órganos administrativos a los que los datos personales pueden ser cedidos;
g. El tiempo aproximado de conservación de los datos; y
h. Las garantías de que se hayan adoptado y las medidas de seguridad, técnicas, organizativas y de confidencialidad adecuadas.

Por vía reglamentaria se regulará el procedimiento de inscripción de bases de datos, tanto del sector público como del privado.

Artículo 67.- Consejo Consultivo de Protección de Datos.- El IAIP estará asesorado por un Consejo Consultivo que apoyará en materia de desarrollo normativo, regulatorio, tecnológico y cuantos otros resulten pertinentes en torno a la promoción y a las garantías derivadas de la protección de datos personales.

El Consejo Consultivo estará integrado por representantes de los sectores públicos y privados, en la forma siguiente:

a. Un experto en la materia, nombrado por el Poder Legislativo;
b. Un experto en la materia, nombrado por el Poder Ejecutivo;
c. Un experto en la materia, nombrado por el Poder Judicial;
d. Un experto en la materia, propuesto por el Consejo Superior de Universidades;
e. Un experto en la materia, de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente;
f. Un experto en la materia, representante del sector de bases de datos de titularidad privada, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente,
g. Un experto en la materia, representante de una organización de derechos humanos de la sociedad civil, seleccionada del modo que se prevea reglamentariamente, y
h. Dos expertos en la materia, representantes nominados por el IAIP.

El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan.

Artículo 68.- Promoción y difusión del derecho fundamental de protección de datos. El IAIP elaborará e implementará la estrategia de comunicación, así como cuantas acciones y actuaciones se consideren pertinentes dirigidas a fomentar el conocimiento por los ciudadanos, las empresas y la sociedad en general el

régimen jurídico derivado de la protección de los datos de carácter personal.

Asimismo, promoverá entre las personas naturales y jurídicas que recolecten, almacenen o traten datos personales, la adopción de las mejores prácticas y protocolos de actuación acordes con la protección de dicha información. Ello abarca también la promoción de códigos tipo empresariales que impliquen la asunción de los principios contenidos en la presente Ley u otros tipos de desarrollo normativos.

El IAIP prestará una especial atención a los grupos de empresas nacionales o multinacionales a los efectos de favorecer el cumplimiento del régimen jurídico derivado de los principios establecidos en esta Ley.

CAPÍTULO II
RECURSO DE REVISIÓN

Artículo 69.- Recurso de revisión. El titular de los datos al que se le deniegue, total o parcialmente el ejercicio de los derechos de acceso, rectificación, cancelación u oposición, podrá interponer el recurso de revisión ante el Instituto de Acceso a la Información Pública y Protección de Datos Personales (IAIP).

Articulo 70.-Procedencia del recurso de revisión. El titular de los datos o su representante podrán interponer el recurso de revisión cuando:

1. Se denieguen total o parcialmente los derechos de acceso, rectificación, cancelación u oposición (ARCO) de sus datos personales;
2. Exista una omisión total o parcial de la respuesta debida al titular de los datos;
3. Se considere por el titular de los datos que la respuesta es desfavorable a la solicitud de ejercicio de derechos formulada.

Artículo 71.- Solicitud del recurso de revisión. El recurso de revisión podrá interponerse por escrito, por medios electrónicos o mediante el uso de los formatos que al efecto proporcione el IAIP y deberá contener la siguiente información:

a. El nombre del recurrente titular de los datos o, en su caso, el de su representante;
b. El nombre del responsable del tratamiento ante el cual se presentó la solicitud de acceso, rectificación, cancelación u oposición de datos personales;
c. Los datos de comunicación, especialmente los de carácter electrónico, a los efectos de la realización y recepción de notificaciones;
d. La fecha en que se le notificó la respuesta, salvo que el procedimiento se

inicie con la falta de respuesta. En este caso, se deberá indicar la fecha de presentación de la solicitud de ejercicio de los derechos de acceso, rectificación, cancelación u oposición;

e. Las razones que justifican su recurso de revisión;
f. La copia de la respectiva solicitud de ejercicio de los derechos de acceso, rectificación, cancelación u oposición con el respectivo atestado de presentación ante el responsable del tratamiento, y;
g. Los demás elementos que se considere procedente poner en conocimiento del IAIP a los efectos de la sustanciación del recurso.

La forma y términos en que deba acreditarse la identidad del titular o cualquier otro extremo que a criterio del IAIP sea necesario tomar en consideración a los efectos de la tramitación del recurso de revisión se regularan de forma reglamentaria.

Artículo 72.- Plazo para interponer el recurso de revisión. El recurso de revisión podrá interponerse dentro del término de diez (10) días hábiles siguientes a la notificación por parte del responsable del tratamiento, o al vencimiento del plazo para obtener respuesta del mismo.

Artículo 73.- Subsanación. En el caso de que el escrito que contenga el recurso de revisión se considere que se encuentra incompleto, el IAIP requerirá al recurrente dentro de los tres (3) días siguientes a la presentación del recurso a los efectos de que proceda a subsanarlo dentro de un plazo de diez (10) días, con el apercibimiento de que, en caso contrario, se tendrá por no presentado dicho recurso.

Artículo 74.- Traslado al responsable del tratamiento. Una vez admitido el recurso de revisión, el IAIP dará traslado del mismo al responsable del tratamiento, para que, en el plazo de diez (10) días, efectúe y aporte las alegaciones y pruebas que estime oportunas. Además se adjuntará una declaración jurada sobre lo expresado y entregado.

Artículo 75.- Medidas provisionales. Cuando de oficio o a instancia de parte, el IAIP tenga conocimiento de presuntas infracciones a los principios y derechos protegidos en la presente Ley, podrá efectuar sin previo aviso inspecciones, auditorías, o cualquier otra medida de control que se considere pertinente sobre los datos contenidos en las bases de datos del responsable y/o encargado del tratamiento.

También si las circunstancias lo ameritan, podrá ordenar el bloqueo temporal de los datos o cualesquiera otras medidas que no podrán aplicarse por un período que exceda de treinta (30) días calendario, las cuales podrán ser prorrogadas por

inicie con la falta de respuesta. En este caso, se deberá indicar la fecha de presentación de la solicitud de ejercicio de los derechos de acceso, rectificación, cancelación u oposición;

e. Las razones que justifican su recurso de revisión;
f. La copia de la respectiva solicitud de ejercicio de los derechos de acceso, rectificación, cancelación u oposición con el respectivo atestado de presentación ante el responsable del tratamiento, y;
g. Los demás elementos que se considere procedente poner en conocimiento del IAIP a los efectos de la sustanciación del recurso.

La forma y términos en que deba acreditarse la identidad del titular o cualquier otro extremo que a criterio del IAIP sea necesario tomar en consideración a los efectos de la tramitación del recurso de revisión se regularan de forma reglamentaria.

Artículo 72.- Plazo para interponer el recurso de revisión. El recurso de revisión podrá interponerse dentro del término de diez (10) días hábiles siguientes a la notificación por parte del responsable del tratamiento, o al vencimiento del plazo para obtener respuesta del mismo.

Artículo 73.- Subsanación. En el caso de que el escrito que contenga el recurso de revisión se considere que se encuentra incompleto, el IAIP requerirá al recurrente dentro de los tres (3) días siguientes a la presentación del recurso a los efectos de que proceda a subsanarlo dentro de un plazo de diez (10) días, con el apercibimiento de que, en caso contrario, se tendrá por no presentado dicho recurso.

Artículo 74.- Traslado al responsable del tratamiento. Una vez admitido el recurso de revisión, el IAIP dará traslado del mismo al responsable del tratamiento, para que, en el plazo de diez (10) días, efectúe y aporte las alegaciones y pruebas que estime oportunas. Además se adjuntará una declaración jurada sobre lo expresado y entregado.

Artículo 75.- Medidas provisionales. Cuando de oficio o a instancia de parte, el IAIP tenga conocimiento de presuntas infracciones a los principios y derechos protegidos en la presente Ley, podrá efectuar sin previo aviso inspecciones, auditorías, o cualquier otra medida de control que se considere pertinente sobre los datos contenidos en las bases de datos del responsable y/o encargado del tratamiento.

También si las circunstancias lo ameritan, podrá ordenar el bloqueo temporal de los datos o cualesquiera otras medidas que no podrán aplicarse por un período que exceda de treinta (30) días calendario, las cuales podrán ser prorrogadas por

causas debidamente justificadas y por el mismo período.
Dichas medidas deberán ser acordadas y/o prorrogadas mediante resolución motivada en la que constará específicamente el nombre y demás datos identificativos del responsable y/o encargado de tratamiento, los datos o bases de datos que deben ser afectados, y los servidores públicos encargados de llevarlas a cabo, los cuales tendrán la condición de autoridad pública.

El procedimiento de adopción y cualquier otra vicisitud relativa a estas medidas se establecerá reglamentariamente.

Artículo 76.- Conciliación. El IAIP podrá en cualquier momento de la sustanciación del recurso propiciar una conciliación entre el titular de los datos y el responsable del tratamiento, excepto cuando la presunta falta sea considerada muy grave. La transacción privada sobre un hecho que pueda ser calificado como infracción a la presente Ley no será oponible ante el IAIP.

De llegarse a un acuerdo de conciliación entre ambos, éste se hará constar por escrito y tendrá efectos vinculantes para las partes, teniéndose el respectivo recurso de revisión por concluido. El IAIP verificará el cumplimiento efectivo del acuerdo respectivo.

El procedimiento y demás efectos derivados de la conciliación se determinarán en el Reglamento de esta Ley.

Artículo 77.- Plazo para emitir resolución. El plazo máximo para dictar la correspondiente resolución en el recurso de revisión será de treinta (30) días, contados a partir de la fecha de recepción de la respuesta por parte del responsable del tratamiento. Cuando haya causa justificada, el IAIP podrá ampliar por una vez y hasta por un período adicional de veinte (20) días este plazo.

La ausencia de resolución deberá interpretarse como desestimación tácita de la reclamación efectuada.

Artículo 78.- Resolución favorable al titular. En el caso de que la resolución de protección de derechos sobre datos personales, resulte favorable al titular de los datos, el IAIP requerirá al responsable del tratamiento para que, en el plazo de los diez (10) días siguientes a la notificación de dicha resolución, dé cumplimiento efectivo a la misma. El responsable, a su vez, deberá comunicar su realización por escrito al IAIP, dentro de los cinco (5) días siguientes a la fecha en que se hubiera efectuado su cumplimiento.

Si por el responsable del tratamiento no se da cumplimiento a lo ordenado, el IAIP actuará conforme a las disposiciones previstas en la presente Ley.

Contra las resoluciones que emita el IAIP, sólo procederá el recurso de amparo en los términos que establece la Ley Sobre Justicia Constitucional.

Artículo 79.- Publicación de resoluciones: *Todas las resoluciones del* ***IAIP*** *serán* susceptibles de difundirse públicamente en versiones públicas, debiendo previamente anonimizarlas, eliminando aquellas referencias del titular de los datos que lo identifiquen o lo hagan identificable.

CAPÍTULO III
DEL PROCEDIMIENTO DE IMPOSICIÓN DE SANCIONES

Artículo 80.- Imposición de sanciones. El IAIP de oficio o a instancia de parte, cuando proceda, abrirá el correspondiente procedimiento sancionador a un responsable o encargado del tratamiento, cuando se tenga conocimiento del presunto incumplimiento de alguno de los principios o disposiciones de esta Ley, a efecto de deducir las responsabilidades que sean procedentes en derecho.

Artículo 81.- Procedimiento de imposición de sanciones. El procedimiento de imposición de sanciones dará comienzo con la notificación que efectúe el IAIP al presunto infractor, sobre los hechos que motivaron el inicio del procedimiento, y le otorgará un plazo de diez (10) días para que efectúe las alegaciones y aporte las pruebas que a su derecho convenga.

El IAIP admitirá las evidencias y pruebas que estime pertinentes y procederá a su evaluación. Asimismo, podrá solicitar del presunto infractor los elementos de prueba que estime necesarios. Concluida la actividad probatoria, el IAIP notificará la correspondiente providencia al presunto infractor relativa al derecho que le asiste para que, de considerarlo necesario, presente sus alegatos finales dentro del plazo de los diez (10) días siguientes a dicha notificación.

En el supuesto de que el presunto infractor no efectúe alegaciones ni aporte prueba o evidencia alguna, el IAIP dictará resolución una vez analizadas las pruebas y demás elementos que estime pertinentes, en el plazo de treinta (30) días a la fecha en que inició el procedimiento sancionador. Cuando haya causa justificada, el IAIP podrá ampliar por una vez y hasta por un período adicional de veinte (20) días este plazo para resolver.

Reglamentariamente se determinará la forma, los términos y los plazos por los que

se sustanciará el procedimiento de imposición de sanciones, incluyendo presentación de pruebas y alegaciones, la celebración de audiencias y el cierre del proceso, y cuantas otras diligencias sean precisas al efecto.

CAPÍTULO IV
DE LAS INFRACCIONES Y SANCIONES

Artículo 82. Cuestiones generales. En ningún caso podrá imponerse una sanción más grave que la fijada en la Ley para la clase de infracción en la que se integre la que se pretenda sancionar.

Para la imposición de las sanciones habrá de observarse los procedimientos y criterios establecidos en el presente Capítulo

El IAIP actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.

Artículo 83.- Faltas leves. Serán consideradas faltas leves, para los efectos de esta Ley:

a. Recolectar datos personales sin que sedé cumplimiento al aviso de privacidad previsto en esta Ley, y
b. No dar adecuado cumplimiento por parte del responsable o encargado del tratamiento al ejercicio de los derechos de acceso, rectificación, cancelación u oposición del titular de los datos en los términos previstos en esta Ley;
c. No permitir al Instituto de Acceso a la Información Pública y Protección de Datos realizar las notificaciones previstas en esta Ley o en su reglamento.
d. No solicitar la inscripción de la base de datos de carácter personal en el Registro Nacional de Bases de Datos.
e. El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado.
f. La transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes establecidos en el artículo 25 de la presente Ley.

Artículo 84.- Faltas graves. Serán consideradas faltas graves, para los efectos de esta Ley:

a. Recolectar, almacenar, transferir o de cualquier otra forma emplear datos personales sin el consentimiento informado e inequívoco del titular de los datos, con arreglo a las disposiciones de esta ley;

b. No adoptar por parte del responsable del tratamiento las medidas de seguridad técnicas y organizativas necesarias para garantizar la seguridad, integridad e inalterabilidad de los datos objeto de tratamiento;
c. Declarar la inexistencia de datos personales, cuando existan total o parcialmente en las bases de datos del responsable del tratamiento;
d. No respetar adecuadamente el principio de calidad de los datos, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados el derecho del titular;
e. La reincidencia en la comisión de faltas leves;
f. Proceder a la creación de bases de datos de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos, sin la autorización de una disposición general, publicada en el Diario Oficial La Gaceta;
g. Tratar datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto en esta Ley y su reglamento;
h. Tratar datos de carácter personal o usarlos posteriormente con infracción de los principios y garantías establecidos en el Titulo II "Principios y Derechos Básicos para la Protección de Datos Personales" de la presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave;
i. La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 34de la presente Ley;
j. El impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición;
k. El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos no hayan sido recabados del propio interesado;
l. El incumplimiento de los restantes deberes de notificación o requerimiento al afectado impuestos por esta Ley y su reglamento;
m. Mantener las bases de datos, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamento se determinen;
n. No atender los requerimientos realizados por el IAIP o no proporcionarle los documentos e información solicitados por el Instituto;
o. La obstrucción al ejercicio de la función de los servidores públicos del IAIP, salvo que el hecho constituya una infracción muy grave;
p. La comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello en los términos previstos en esta Ley y su reglamento, salvo que la misma sea constitutiva de una infracción muy grave.

Artículo 85.- Faltas muy graves. Serán consideradas faltas muy graves, para los

efectos de esta ley:

a. La recolección de datos en forma engañosa o fraudulenta, o sin proporcionar el correspondiente aviso de privacidad;
b. Obtener, del titular o de terceros, datos personales de una persona por medio de engaño, violencia o amenaza;
c. Incumplir el deber de confidencialidad establecido en esta Ley;
d. Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin respetar el principio de consentimiento definido en el artículo 4, inciso e). de esta Ley;
e. Vulnerar deliberadamente la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable;
f. Llevar a cabo la comunicación o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley;
g. Revelar información registrada en una base de datos personales cuyo secreto esté obligado a guardar conforme a la Ley;
h. Obstruir los actos de verificación o requerimientos, de la autoridad o de los servidores del IAIP, con independencia de que se dé traslado de la infracción cometida al órgano persecutor de la acción pública
i. Proporcionar a un tercero, información falsa o distinta a la contenida en un archivo de datos;
j. Realizar un tratamiento de datos personales sin encontrarse la base de datos debidamente inscrita ante el IAIP;
k. Continuar con el uso ilegítimo o tratamiento de los datos personales cuando se haya solicitado el cese del mismo por el IAIP o los titulares de los datos;
l. Tratar o ceder de manera voluntaria e ilegítima los datos de carácter personal a los que hace referencia la presente Ley, con conocimiento de dichas circunstancias;
m. Transferir, a las bases de datos de terceros países, información de carácter personal de los hondureños o de los extranjeros radicados en el país, sin el consentimiento de sus titulares;
n. La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección adecuada sin autorización del IAIP salvo en los supuestos establecidos en esta Ley.

Artículo 86.- Sanciones. Si se ha incurrido en alguna de las faltas tipificadas en esta ley, el IAIP impondrá alguna de las siguientes sanciones:

a. Para faltas leves, apercibimiento, o una multa de diez (10) a veinte (20) *salarios mínimos*.

   El apercibimiento podrá ser procedente cuando se trate de un primer incumplimiento a lo dispuesto en esta Ley, y el mismo se considere que no ha sido deliberado;

b. Para las faltas graves, una multa de veintiún (21) hasta cuarenta (40) salarios mínimos;
c. Para las faltas muy graves, una multa de cuarenta y un (41) a sesenta (60) salarios mínimos.

Artículo87.- Criterios para imponer las sanciones. El IAIP fundará y motivará sus resoluciones, considerando:

a. La naturaleza del dato;
b. La notoria improcedencia de la negativa del responsable del tratamiento, para realizar los actos solicitados por el titular, en términos de esta Ley;
c. El carácter intencional o no, de la acción u omisión constitutiva de la infracción;
d. Las acciones llevadas a cabo por el responsable o encargado del tratamiento para aminorar o eliminar las consecuencias derivadas de la infracción cometida;
e. La capacidad económica del responsable del tratamiento; y,
f. La reincidencia.

Artículo 88 - Criterios para determinar la cuantía *La cuantía de las sanciones se* graduará, asimismo, atendiendo a los siguientes criterios:

a. El carácter continuado de la infracción.
b. El volumen de los tratamientos efectuados.
c. La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.
d. El volumen de negocio o actividad del infractor.
e. Los beneficios obtenidos como consecuencia de la comisión de la infracción.
f. El grado de intencionalidad.
g. La reincidencia por comisión de infracciones de la misma naturaleza.
h. La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.
i. La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recolecta y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos *no debida a una falta de diligencia exigible al infractor.*
j. Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

Artículo 89.- Aplicación de la cuantía de la sanción. El órgano sancionador (IAIP) establecerá la cuantía de la sanción aplicando la escala relativa a la clase de

infracciones que preceda inmediatamente en gravedad, a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:

a. Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios anteriormente enunciados.

b. Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.

c. Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.

d. Cuando el infractor haya reconocido espontáneamente su culpabilidad.

e. Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente.

Artículo 90.- Aplicación de la sanción de apercibimiento. Excepcionalmente el órgano sancionador (IAIP) podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos anteriormente, no acordar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:

a. Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.

b. Que el infractor no hubiese sido sancionado o apercibido con anterioridad. Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.

Artículo 91.- Infracciones de las Administraciones públicas. Cuando las infracciones a que se refiere el presente Capítulo fuesen cometidas en base de datos de titularidad pública o en relación con tratamientos cuyos responsables lo serían de la base de datos de dicha naturaleza, el órgano sancionador (IAIP) dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable dela base de datos, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

El órgano sancionador (IAIP) también podrá proponer la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las

establecidas en la legislación sobre régimen disciplinario de las Instituciones Públicas.

Se deberán comunicar al órgano sancionador (IAIP) las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

Artículo 92.- Prescripción de la Infracción. Las infracciones muy graves prescribirán a los tres (3) años, las graves a los dos (2) años y las leves en un (1) año.

El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.

Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis (6) meses por causas no imputables al presunto infractor.

Artículo 93.- Prescripción de la Ejecución de las Sanciones Impuestas.
La ejecución de las sanciones impuestas por faltas muy graves prescribirá a los tres (3) años, las impuestas por faltas graves a los dos (2) años y las impuestas por faltas leves en un (1) año.

El plazo de prescripción de la ejecución de las sanciones impuestas, comenzará a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impone la sanción.

La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Artículo 94.- Otras responsabilidades. Las sanciones que se señalan en este Capítulo se impondrán sin perjuicio de la responsabilidad civil o penal que resulte de la comisión de las infracciones previstas en esta Ley.

TÍTULO XII
CÁNONES

Artículo 95.- Canon por regulación y administración de bases de datos. El responsable del tratamiento que deba inscribirse ante el IAIP, de conformidad con los artículos56 y 59de esta Ley, estará sujeto a un canon de regulación y administración de bases de datos que deberá ser cancelado anualmente, con un monto equivalente al treinta por ciento (30%) del salario mínimo promedio a la fecha en cada momento vigente. Este monto será entregado a la Tesorería General de la República, el cual por conducto de la Secretaría de Estado en el Despacho de Finanzas deberá ser incorporado en forma mensual al Presupuesto Anual de Ingresos y Egresos del IAIP, específicamente para el funcionamiento y operación de la Gerencia de PRODATOS. El procedimiento para realizar el cobro del presente canon se determinará en el Reglamento que a los efectos deberá emitir el IAIP.

Artículo 96.- Canon por comercialización de consulta. El responsable del tratamiento de la base de datos deberá cancelar ante el IAIP un canon por cada venta de los datos personales, de personas individualizables registradas legítimamente y siempre que sea comercializado con fines de lucro, el cual ascenderá al cuarenta por ciento (40%) del valor de la venta individual de datos personales, monto que podrá ser actualizado por vía reglamentaria.

El IAIP se reserva la facultad de establecer nuevos cánones a consecuencia de la prestación de servicios a los responsables y/o encargados del tratamiento y a terceros, como consecuencia de la aplicación de la presente Ley. Reglamentariamente se determinarán los mismos así como el proceso para su exacción y cobro y cuantas otras cuestiones tengan que ser objeto de determinación y cuantificación.

En caso de contratos globales de bajo, medio y alto consumo de consultas, o modalidades contractuales de servicio en línea por número de aplicaciones u otros conceptos de carácter análogos, será el reglamento de la Ley el que fije el detalle del cobro del canon que no podrá ser superior al diez por ciento (10%) del precio contractual.

DISPOSICIONES TRANSITORIAS

PRIMERA.- La presente Ley entrará en vigencia a partir de su publicación en el *Diario Oficial La Gaceta*.

SEGUNDA.- A partir de la fecha de entrada en vigencia de esta Ley, se iniciará el proceso de conformación e integración de la **Gerencia de Protección de Datos (PRODATOS)**; para ello, se dispondrá de un plazo máximo de **seis (6) meses calendario.**

TERCERA.- El Instituto de Acceso a la Información Pública emitirá el Reglamento General de esta Ley dentro del año siguiente a su entrada en vigor.

Asimismo, el IAIP dictará aquellas normas de desarrollo de la presente Ley, que se consideren necesarias para la correcta aplicación de la misma.

CUARTA.- Las personas naturales o jurídicas, públicas o privadas, que en la actualidad son titulares o administradoras de las bases de datos objeto de esta Ley, deberán inscribir las mismas en el Registro correspondiente y adecuar sus procedimientos y reglas de actuación, así como el contenido de sus bases de datos a lo establecido en la presente Ley, en un plazo máximo de un año a partir de la entrada en vigencia de la ley.

QUINTA.- Una vez entrada en vigor la presente Ley, todas las bases de datos que contengan datos de carácter personal, con excepción de los supuestos excluidos en la misma, se regirán por las previsiones contenidas en la propia Ley, aunque su fecha de constitución sea anterior a su aplicación.

DISPOSICIONES ADICIONALES

PRIMERA.-El Decreto Legislativo No. 170-2006 y sus reformas que contiene la Ley de Transparencia y Acceso a la Información Pública tendrán carácter supletorio en la interpretación u aplicación de la presente Ley.

SEGUNDA. Se da nueva redacción al artículo 109 del Decreto No. 62/2004, por el que se aprueba la Ley del Registro Nacional de las Personas, el cual queda redactado de acuerdo con el siguiente contenido:

"Articulo 109: Datos contenidos en la ley Registro Nacional de las Personas:

1. Se reconoce capacidad y competencia al Registro Nacional de las Personas para la recolección, tratamiento, verificación y disposición de los datos a los que se hace referencia en el apartado 3ºde este precepto, el cual podrá ceder los mismos, sin necesidad del previo consentimiento del titular de los datos en los siguiente supuestos:

a). Cuando los mismos afecten a la seguridad del Estado, a la Administración de Justicia, o a una autoridad pública en el ejercicio de sus legítimas competencias.

b). En cualquier otro supuesto donde exista la habilitación legal al efecto.

2. Los datos contenidos en el Registro Nacional de las Personas son los correspondientes a:
   a) A los existentes en el Registro Civil y los correspondiente a la identificación de las personas naturales.
   b) Y cualesquiera otros que en Registro Nacional de las Personas considere convenientes o necesarios para el ejercicio de sus competencias legales.

TERCERA. El IAIP asumirá exclusivamente la total regulación en materia de protección de datos de carácter personal sobre las funciones propias de la Comisión Nacional de Bancos y Seguros, la cual mantendrá íntegramente el resto de sus competencias.