POLÍTICA INTERNA DE PROTECCIÓN DE DATOS PERSONALES DEL INSTITUTO DE ADMINISTRACIÓN Y AVALÚOS DE BIENES NACIONALES

CONTENIDO

I.- PRESENTACIÓN

El Instituto de Administración y Avalúos de Bienes Nacionales (INDAABIN) en términos del artículo 31, fracción XXIX, de la Ley Orgánica de la Administración Pública Federal, en relación con el Segundo Transitorio, del Decreto publicado el 18 de julio de 2016, en el Diario Oficial de la Federación, por el que se reforman, adicionan y derogan diversas disposiciones de la Ley Orgánica de la Administración Pública Federal, 2, apartado D, fracción VI, y 6°, fracción XXXV, del Reglamento Interior de la Secretaría de Hacienda y Crédito Público, es un órgano desconcentrado de la Secretaría de Hacienda y Crédito Público que le está jerárquicamente subordinado y tiene la organización y las atribuciones que le confiere su Reglamento, al que le corresponde el despacho de, entre otros asuntos, el de conducir la política inmobiliaria de la Administración Pública Federal salvo por lo que se refiere a las playas, zona federal marítimo terrestre, terrenos ganados al mar o cualquier depósito de aguas marítimas y demás zonas federales.

El INDAABIN al ser un órgano desconcentrado de la Secretaría de Hacienda y Crédito Público, forma parte de la administración pública federal, por lo que es considerado sujeto obligado en términos del artículo 1 párrafo quinto de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y en consecuencia, debe cumplir con las disposiciones establecidas en materia de protección de datos personales.

En ese sentido, el artículo 6, Base A, fracción II de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) establece que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes, en tanto que su diverso 16, segundo párrafo dispone que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, lo cual garantiza a los titulares el derecho a su privacidad, el buen uso de su información personal y su derecho a la autodeterminación informativa, el cual implica que toda persona decida de manera libre e informada, sobre el uso de la información que les pertenece.

Por otro lado, la LGPDPPSO, establece que es obligación de todo responsable proteger los datos personales que trate, garantizar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información, y responsabilidad,

los deberes de seguridad y confidencialidad, y las obligaciones derivadas de dicha Ley.

Para tales efectos, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), emitió los Lineamientos Generales de Protección de Datos Personales para el Sector Público (LGPDPSP), en el que desarrolló y concentró en un solo cuerpo normativo las obligaciones señaladas en la LGPDPPSO, con la finalidad facilitar y hacer más comprensible y simple el conocimiento y la exigibilidad del derecho a la protección de datos personales en el sector público federal, así como evitar la fragmentación o atomización en innumerables ordenamientos que pudiera repercutir en el cumplimiento efectivo de la dicha Ley por parte de los responsables del ámbito federal, o bien, hacer inaccesible el derecho para cualquier persona.

De esa manera, de conformidad a lo establecido en los artículos 16, último párrafo, 45, 54, 72, 107 y 118 de los LGPDPSP, la carga de la prueba para acreditar el cumplimiento de los principios, deberes y obligaciones relativas a la protección de datos personales en su tratamiento, en todo momento, recaerá en el responsable por lo que deberán adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la LGPDPPSO y los LGPDPSP.

Asimismo, el 26 de noviembre de 2021 el INAI emitió el Acuerdo mediante el cual se aprueban los Instrumentos Técnicos de Evaluación que refiere el Título Décimo de los LGPDPSP, en los cuales se estableció el tipo de evaluación, la metodología, los criterios, los formatos y los indicadores de cumplimiento que deberán observar los sujetos obligados en el tratamiento de datos personales.

En ese sentido, a efecto de salvaguardar el derecho humano a la protección de datos personales y en observancia al principio de responsabilidad que establece que el responsable del tratamiento de datos personales deberá implementar mecanismos para el cumplimiento de los principios, deberes y obligaciones establecidos en la LGPDPPSO y los LGPDPSP, se considera necesario emitir una Política Interna de Protección de datos personales de observancia obligatoria para el personal del Instituto que realice un tratamiento de datos personales, la cual instituya un programa de trabajo dirigido a la protección de los datos personales en posesión del INDAABIN.

II. OBJETO

Primero. – La presente Política Interna tendrá por objeto establecer un programa de trabajo que contemple las medidas necesarias para proteger los datos personales en posesión del INDAABIN.

Segundo. – La presente Política Interna tendrá como fin que el personal que labora en el Instituto realice un tratamiento de datos personales en estricto apego a los principios, deberes y obligaciones previstos en la LGPDPPSO y demás disposiciones aplicables, lo cual permitirá garantizar la adecuada protección de los datos personales y el ejercicio de los derechos de Acceso, Rectificación, Cancelación, Oposición y Portabilidad al tratamiento de datos personales por parte de sus titulares.

Tercero. – Garantizar el cumplimiento de los principios, deberes y obligaciones en materia de protección de datos personales para otorgar certeza jurídica a sus titulares sobre el control su información personal; que incluyen el derecho a saber quién posee sus datos personales, el tratamiento al que están siendo sometidos y el poder de oponerse a esa posesión y tratamiento.

III. ALCANCE

La presente Política es de observancia obligatoria para todo el personal de las unidades administrativas del INDAABIN, involucrado en el tratamiento de datos personales, así como, para los integrantes de su Comité de Transparencia (en lo sucesivo CT), con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización, en la que se encuentren los datos personales.

CAPÍTULO I. MARCO NORMATIVO

1. Que el artículo 6, Base A, fracción II de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) establece que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

2. Que el artículo 16, segundo párrafo de la CPEUM establece que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

3. Que el 26 de enero de 2017 se publicó en el Diario Oficial de la Federación el Decreto por el cual se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), misma que en su artículo 1, párrafo segundo y cuarto establece que todas sus disposiciones según corresponda en el ámbito de su competencia son de aplicación y observancia directa para los sujetos obligados pertenecientes al orden federal, asimismo que tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados.

4. Que el artículo 2, fracciones II, IV y VI de la LGPDPPSO tiene entre sus objetivos, establecer las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, mediante procedimientos sencillos y expeditos; garantizar la observancia de los principios de protección de datos personales, así como garantizar que toda persona pueda ejercer el derecho a la protección de los datos personales, entre otros.
5. Que el artículo 16 de la LGPDPPSO, establece la observancia por parte del responsable, de los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales, así como en su artículo 31 determina que el responsable deberá

establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

6. Que los artículos 29 y 30, fracciones I y VII, de la LGPDPPSO, el responsable deberá implementar mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en dicha Ley, entre los cuales se encuentran, destinar recursos autorizados para tal fin para la instrumentación de programas y políticas de protección de datos personales, así como diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la LGPDPPSO y las demás que resulten aplicables en la materia.

7. Que los artículos 43 a 47 de la LGPDPPSO establecen los derechos de acceso, rectificación, cancelación y oposición (ARCO) que tienen los titulares de los datos personales y la forma en la que podrán ejercerlos.

8. Que el artículo 83 de la LGPDPPSO establece que cada sujeto obligado contará con un Comité de Transparencia (CT), mismo que se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y demás normatividad aplicable, el cual será la autoridad máxima en materia de protección de datos personales.

9. Que el artículo 30, fracciones I y II y 84, fracción I de la LGPDPPSO, prevé que los responsables tendrán que coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en aquellas disposiciones que resulten aplicables en la materia; por su parte el CT, entre otras, tendrán facultades y atribuciones para coordinar, supervisar y realizar, en términos de las disposiciones aplicables, las acciones y procedimientos para garantizar el derecho a la protección de los datos personales en la organización del responsable.

10. Que el 26 de enero de 2018, se publicaron en el Diario Oficial de la Federación los Lineamientos Generales de Protección de Datos Personales para el Sector Público (LGPDPSP), mismos que establece en su artículo 46, párrafo primero, que el responsable deberá adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la LGPDPPSO y en los referidos Lineamientos, así como establecer aquellos mecanismos necesarios para evidenciar dicho cumplimiento ante los titulares y el INAI.

11. El 12 de febrero de 2018 se publicó en el Diario Oficial de la Federación, el Acuerdo del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, mediante el cual se aprueban los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, en cuyo artículo 14 dispone que para la portabilidad de datos personales el responsable deberá observar los requisitos, plazos, condiciones, términos y procedimientos establecidos en el Título tercero, Capítulo II de la LGPDPPSO.

12. Que conforme a lo dispuesto por el artículo 247 de los Lineamientos Generales, el Instituto aprobará los Instrumentos Técnicos de Evaluación que sean necesarios para medir el desempeño de los responsables respecto al cumplimiento de las obligaciones previstas en la Ley General y demás disposiciones aplicables en la materia; los cuales contemplarán, al menos, el tipo de evaluación, la metodología, los criterios, los formatos, por lo que el 26 de noviembre de 2021 se publicó en el Diario Oficial de la Federación el ACUERDO mediante el cual se aprueban los Instrumentos Técnicos que refiere el Título Décimo de los LGPDPSP en los cuales se estableció el tipo de evaluación, la metodología, los criterios, los formatos y los indicadores de cumplimiento que deberán cumplir los sujetos obligados en el tratamiento de datos personales.

    Por las razones expuestas y con fundamento en lo dispuesto por los artículos 6, Base A, fracción II y 16, segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos; 30, fracciones I y II, 84, fracciones I de la LGPDPPSO y 104 de los LGPDPSP, el CT emite la Presente Política Interna de Protección de Datos Personales del INDAABIN.

CAPÍTULO II. GLOSARIO DE TÉRMINOS COMUNES RELACIONADOS CON ESTE DERECHO.

Para los efectos de los presentes Lineamientos se entenderá por:

I. Aviso de privacidad: Documento a disposición del titular de los datos de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

II. Bases de datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento u organización.

III. Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. a. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.

IV. Ciclo de vida. - Se refiere a las fases del tratamiento de los datos personales, consistentes en la obtención, almacenamiento, uso, divulgación, bloqueo y cancelación.

V. Consentimiento: manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

VI. Comité de Transparencia: Órgano colegiado encargado de supervisar, vigilar y coordinar los procedimientos derivados de la LGTAIP y LFTAIP, según lo señalado en los artículos 44 y 65 respectivamente.

Asimismo, de conformidad con el artículo 83, de la LGPDPPSO es la autoridad máxima en materia de datos personales.

VII. Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad puede determinarse directa o indirectamente a través de cualquier información.

VIII. Datos personales sensibles: Aquellos que se refieran a la esfera más íntima del titular, cuya utilización indebida pueda dar origen a actos de discriminación o implique riesgos para aquél. De manera enunciativa, mas no limitativa se consideran sensibles los datos personales relacionados con origen racial o étnico; estado de salud presente o futuro, información genética, creencias religiosas, filosóficas o morales; opiniones políticas y orientación sexual.

IX. Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

X. Derecho de portabilidad: Prerrogativa del titular de los datos personales a obtener de la INDAABIN en su calidad de responsable, una copia de los datos personales objeto de tratamiento, en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.

XI. Días hábiles: Todos los del año, con excepción de los inhábiles, según el Acuerdo que para tal efecto emita el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

XII. Disociación: El procedimiento mediante el cual los datos personales no pueden asociarse al titular, ni permitir por su estructura, contenido o grado de desagregación, la identificación del mismo.

XIII. INAI: El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

XIV. INDAABIN: El Instituto de Administración y Avalúos de Bienes Nacionales

XV. Inventario de datos personales. - Identificación de las bases de datos de tratamiento de las unidades administrativas, por le cual se documenta la información básica de cada tratamiento realizado, con independencia de su forma de almacenamiento, en la cual se incluye el ciclo de vida del dato personal.

XVI.- LGPDPPSO: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

XVII. Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Público.

XVIII.- Portabilidad de datos personales. - Prerrogativa de los titulares de datos personales que les permite, bajo las condiciones establecidas en la normatividad aplicable, recibir los datos personales que han proporcionada a un responsable del tratamiento en un formato estructurado, de uso común y lectura mecánica, y transmitirlos a otro responsable del tratamiento sin impedimentos.

XIX.- Principios. - El derecho a la protección de datos personales se regula a través de ocho principios, los cuales se traducen en obligaciones, y son: licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

XX.- Remisión: Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano.

XXI.- Responsable: Sujeto Obligado de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados que decide sobre el tratamiento de datos personales, conforme lo dispuesto en su artículo 1.

XXII.- SISAI: Sistema Informático de Solicitudes de Acceso a la Información, de acceso, rectificación, cancelación, oposición y portabilidad de datos personales que se encuentra en la plataforma del Sistema Nacional de Transparencia.

XXIII.- Sistema de Datos Personales: Constituye el conjunto ordenado de datos personales que estén en posesión de una dependencia o entidad, con independencia de su forma de acceso, creación, almacenamiento u organización. Los sistemas de datos personales podrán distinguirse entre físicos y automatizados, definiéndose cada uno de ellos de la siguiente forma:

a) Físicos: Conjunto ordenado de datos que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos.

b) Automatizados: Conjunto ordenado de datos que para su tratamiento han sido o están sujetos a un tratamiento informático que requieren de una herramienta tecnológica específica para su acceso, recuperación o tratamiento.

XXIV.- Supresión: La baja archivística de los datos personales conforme la normativa de archivo aplicable que resulte en la eliminación, borrado o destrucción de datos personales bajo las medidas de seguridad previamente establecidas por el responsable.

XXV.- SNT: Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

XXVI.- Titular: La persona física a quién le pertenecen los datos personales.

XXVII.- Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

XXVIII.- Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales; relacionados con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

XXIX.- Unidad de Transparencia: Unidad administrativa que tiene por objetivo principal hacer las gestiones necesarias al interior del INDAABIN para lograr que funcionen adecuadamente la LGTAIP, la LGPDPPSO y la LFTAIP. Así como la instancia a que hace referencia el artículo 45 de la Ley General de Transparencia y acceso a la Información Pública.

DISPOSICIONES GENERALES

PRIMERO.- La presente Política de Protección de Datos Personales es de observancia general para todo el personal del INDAABIN involucrado en el tratamiento de datos personales.

SEGUNDO.- Corresponde al Comité de Transparencia, como máxima autoridad en materia de protección de datos personales, vigilar y verificar el cumplimiento de la presente Política de Protección de Datos Personales.

TERCERO.- El Comité de Transparencia establecerá los mecanismos para vigilar y verificar el cumplimiento de las políticas, principios y deberes en el tratamiento y protección de datos personales.

CUARTO.- El Comité de Transparencia establecerá criterios específicos que resulten necesarios para una mejor observancia de la presente Política de Protección de Datos Personales, así como de las disposiciones aplicables de protección de datos personales.

QUINTO. La Unidad de Transparencia asesorará a las unidades administrativas del Instituto en materia de protección de datos personales conforme a los principio, deberes y obligaciones establecidos en la LGPDPPSO y en los Lineamientos Generales, la presente Política y demás normativa aplicable.

SEXTO.- Para las actividades señaladas en la presente Política, será necesario contar con personas servidoras públicas que funjan como enlaces en materia de datos personales en cada una de las unidades administrativas, las cuales serán designadas por la persona Titular de las mismas.

SÉPTIMO. El Comité de Transparencia y la Unidad de Transparencia podrán sugerir a las unidades administrativas que realicen diversas actividades a fin de cumplir con los principios, deberes y obligaciones en materia de protección de datos personales.

OCTAVO.- El Comité de Transparencia y la Unidad de Transparencia cuando adviertan un hecho que pueda constituir una resunta falta administrativa en materia de datos personales en términos de la normatividad aplicable, lo harán de conocimiento del Órgano Interno de Control, para los efectos conducentes.

CAPÍTULO III. PRINCIPIOS EN EL TRATAMIENTO DE DATOS PERSONALES.

Los principios de protección de datos personales, son las herramientas para garantizar la efectiva protección de los datos personales de sus titulares cuando son tratados; herramientas de uso o obligatorio para interpretar y aplicar la LGPDPPSO y demás normatividad aplicable en la materia, asimismo, representan un límite al tratamiento de datos personales que se encuentren en posesión de sujetos obligados.

Los principios de protección de datos personales son los siguientes:

I.- Licitud;
II.- Finalidad;
III.- Lealtad;
IV.- Consentimiento;
V.- Calidad;
VI.- Proporcionalidad;
VII.- Información;
VIII.- Responsabilidad.

I.- Principio de Licitud.

El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la legislación mexicana e internacional le confiera.

Dicho de otra forma, el principio de licitud significa que el tratamiento de datos personales es una actividad que depende de las atribuciones o facultades que previamente le otorga la ley a los Sujetos Obligados, en consecuencia, no deben tratarse datos personales si no se tienen facultades previamente otorgadas por la normatividad aplicable.

Obligaciones vinculadas al principio de licitud.

Para cumplir el principio de licitud, el responsable tiene las siguientes obligaciones:

1) Tratar siempre los datos personales de conformidad con las atribuciones o facultades conferidas por la normatividad, actuando con apego a la legislación

mexicana, incluida la aplicable en materia de protección de datos personales y, en su caso, el derecho internacional.

2) El tratamiento se debe realizar tomando en consideración los derechos y libertades de los titulares y respetando la garantía de legalidad de los gobernados.

Mecanismos para dar cumplimiento.

Los responsables deberán Identificar el marco normativo (leyes, tratados o acuerdos internacionales, reglamentos, lineamientos, entre otros, con sus respectivos artículos) que faculta a la unidad administrativa a tratar los datos personales, para cada una de las finalidades, y aquellos que regulan dicho tratamiento.

II.- Principio de Finalidad.

Este principio atiende al propósito, motivo o razón por el cual se tratan datos personales, es decir, todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera, entendiéndose por estas lo siguiente:

- **Concretas:** Cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en el titular.

- **Explícitas:** Cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad.

- **Lícitas:** Cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable.

- **Legítimas:** Cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento del titular, salvo

que se actualice alguna de las causales de excepción previstas en el artículo 22 de la LGPDPPSO.

En ese sentido la finalidad o finalidades del tratamiento de datos personales deberán ser determinadas, es decir, deberán especificar para qué objeto se tratarán los datos personales de manera clara, sin lugar a confusión y con objetividad.

Ahora bien, en caso que los datos personales se traten para finalidades distintas a aquellas que motivaron su tratamiento original se deberán considerar 4 aspectos principales:

- La expectativa razonable de privacidad del titular basada en la relación que tiene con éste.
- La naturaleza de los datos personales.
- Las consecuencias del tratamiento posterior de los datos personales para el titular.
- Las medidas adoptadas para que el tratamiento posterior de los datos personales cumpla con las disposiciones previstas en la LGPDPPSO y los Lineamientos Generales.

En todo caso, el titular de los datos personales puede negar o revocar su consentimiento, así como oponerse para el tratamiento de sus datos personales para las finalidades distintas a aquellas que motivaron su tratamiento original, sin que ello tenga como consecuencia la conclusión del tratamiento para las finalidades originarias.

En ese sentido, es indispensable que en el aviso de privacidad se identifique y distinga las finalidades del tratamiento. Asimismo, se deberá indicar el mecanismo habilitado para que el titular, si así lo desea, pueda manifestar su negativa al tratamiento de sus datos personales para todas o algunas de las finalidades.

El responsable solo podrá realizar tratamiento para una finalidad distinta a las que fueron informadas previamente al titular en los siguientes supuestos:

- Se cuente con atribuciones legales y medie el consentimiento del titular, en términos de la LGPDPPSO.
- Una persona reportada como desaparecida.

Obligaciones vinculadas al principio de finalidad:

Derivado del cumplimiento al principio de finalidad el responsable tiene las siguientes obligaciones:

1. Tratar los datos personales únicamente para la finalidad o finalidades que hayan sido informadas al titular en el aviso de privacidad y, en su caso, consentidas por éste.

2. Informar en el aviso de privacidad todas las finalidades para las cuales se tratarán los datos personales, y redactarlas de forma tal que sean determinadas.

3. Identificar y distinguir en el aviso de privacidad entre las finalidades que dan origen al tratamiento de aquellas que son distintas a las que lo originaron, pero se consideran compatibles y/o análogas.

4. Ofrecer al titular de los datos personales un mecanismo para que pueda manifestar su negativa al tratamiento de sus datos personales para todas o algunas de las finalidades secundarias.

5. Cuando el aviso de privacidad se dé a conocer a través de un medio indirecto, como el correo postal, informar al titular que tiene cinco días hábiles para manifestar su negativa para el tratamiento de su información.

6. No condicionar el tratamiento para finalidades, con aquellas distintas a las que dieron origen al tratamiento.

7. Tratar los datos personales para finalidades distintas que no resulten compatibles o análogas con aquéllas para las que se hubiese recabado de origen los datos personales y que hayan sido previstas en el aviso de privacidad, al menos que lo permita una ley o reglamento, o se obtenga el consentimiento del titular de los datos.

Mecanismos para cumplir con el principio de finalidad.

1. Identificar las finalidades de cada tratamiento que se realice, y verificar que las mismas atiendan a fines específicos o determinados, y que sean acordes a las atribuciones o facultades del sujeto obligado y unidad administrativa de que se trate.

2. Verificar que en los avisos de privacidad se informan todas las finalidades para las cuales se tratan los datos personales, y que éstas se describen de manera clara.

3. Identificar qué finalidades requieren consentimiento y solicitarlo de acuerdo a lo establecido en la LGPDPPSO.

III. Principio de Lealtad.

El responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, para lo cual se deberá observar lo siguiente:

No se recaben datos personales con dolo, mala fe o negligencia.

No tratar los datos de tal manera que genere discriminación o un trato injusto contra los titulares.

No se vulnere la confianza del titular con relación a que sus datos personales serán tratados conforme a lo acordado.

Se informen todas las finalidades del tratamiento en el aviso de privacidad. Con este principio no se permite el tratamiento, tramposo, deshonesto y no ético de la información sobre los titulares, los derechos del titular dependen del Responsable, para que de esta manera el titular pueda confiar en la buena fe del Responsable.

Obligaciones vinculadas al principio de lealtad:

El responsable tiene las siguientes obligaciones en torno al principio de lealtad:

1) No hacer uso de medios engañosos o fraudulentos para la obtención de los datos personales.

2) Respetar en todo momento la expectativa razonable de privacidad del titular.

Mecanismos para cumplir el principio de lealtad.

1) Verificar que los datos personales no se obtengan con dolo, mala fe o negligencia.

2) Verificar los tratamientos que realiza el sujeto obligado, a fin de confirmar que los mismos no den lugar a discriminación o trato injusto o arbitrario en contra del titular.

3) Elaborar avisos de privacidad con todos los elementos informativos que establece la LGPDPPSO, y con información que corresponda a la realidad del tratamiento que se efectúa.

4) Incluir en los avisos de privacidad todas las finalidades de los tratamientos, las cuales deberán estar redactadas de forma clara y concreta, para que no haya lugar a confusión al respecto.

5) Llevar a cabo el tratamiento de los datos personales sólo para los fines informados en el aviso de privacidad.

IV. Principio de Consentimiento.

Cuando no se actualicen algunas de las causales de excepción previstas en el artículo 22 de la LGPDPPSO, el responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma:

- **Libre:** Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular.

- **Específica:** Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento.

- **Informada:** Que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales.

En la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la LGPDPPSO, se estará a lo dispuesto en las reglas de representación previstas en la legislación civil que resulte aplicable.

El consentimiento podrá manifestarse de las siguientes maneras:

- **Expreso.** Cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.
- **Tácito**. Cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario.

Tratándose de datos personales sensibles el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos previstos en el artículo 22 de la LGPDPPSO.

La solicitud del consentimiento deberá ir siempre ligada a las finalidades concretas del tratamiento que se informen en el aviso de privacidad, es decir, el consentimiento se deberá solicitar para tratar los datos personales para finalidades específicas.

De conformidad con el artículo 22 de la Ley General el consentimiento no se deberá recabar en los siguientes casos:

- Cuando una ley así lo disponga, debiendo ser acorde a las bases, principios y disposiciones establecidos en la normatividad en materia de datos personales.

- Cuando las transferencias se realicen entre responsables, se trate de datos personales que utilicen en el ejercicio de las facultades del sujeto obligado o sean compatibles o análogas con la finalidad que dio origen al tratamiento de los datos personales.

- Cuando exista una orden judicial, resolución o mandato fundado y motivado de una autoridad competente.

- Para el reconocimiento o defensa de derechos del titular ante autoridad competente.

- Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable.

- Cuando exista una situación de emergencia que pueda dañar a un individuo en su persona o sus bienes.

- Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico o la prestación de asistencia sanitaria.

- Cuando los datos personales figuren en fuentes de acceso público.

- Cuando los datos personales se sometan a un procedimiento previo de disociación.

- Cuando el titular de los datos sea una persona reportada como desaparecida.

Sin embargo, aunque en dichos supuestos no se requiera el consentimiento para el tratamiento, se deberán cumplir los otros principios, lo que incluye la obligación de poner a disposición del titular el aviso de privacidad.

El consentimiento expreso o por escrito se puede obtener a través del aviso de privacidad o de cualquier otro documento físico o electrónico que determine el responsable.

En caso que el responsable decidiera tratar los datos personales para finalidades distintas a las que informó originalmente en el aviso de privacidad, y para las cuales obtuvo el consentimiento inicial por parte de los titulares, será necesario solicitar el consentimiento de los titulares para las nuevas finalidades, siempre y cuando estas finalidades no actualicen los supuestos de excepción que señala el artículo 22 de la Ley General.

Obligaciones vinculadas al principio de consentimiento

El responsable tiene las siguientes obligaciones en torno al principio de consentimiento.

1. Obtener el consentimiento del titular para el tratamiento de los datos personales, cuando no se actualice alguno de los supuestos previstos en el artículo 22 de la Ley General.

2. Solicitar el consentimiento siempre ligado a finalidades específicas e informadas en el aviso de privacidad.

Determinar el tipo de consentimiento que se requiere: tácito, expreso o expreso y por escrito.

4. Solicitar el consentimiento expreso y por escrito para los datos personales sensibles, en caso de que no se actualice alguno de los supuestos del artículo 22 de la Ley General.

5. Solicitar el consentimiento expreso o por escrito cuando así lo requiera una ley o reglamento, se acuerde con el titular o lo determine conveniente el responsable.

6. Dar a conocer al titular el aviso de privacidad previo a la obtención del consentimiento.

7. Solicitar el consentimiento previo a la obtención de los datos personales, si éstos se recaban directamente del titular y no se actualiza alguno de los supuestos previstos en el artículo 22 de la Ley General.

8. Solicitar el consentimiento antes de utilizar los datos personales para las finalidades para las cuales se obtuvieron, si éstos se recabaron de manera indirecta y no se actualiza alguno de los supuestos previstos en el artículo 22 de la Ley General.

9. Implementar medios sencillos y gratuitos para la obtención del consentimiento, de acuerdo con el tipo de consentimiento que se requiera (tácito, expreso o expreso y por escrito).

10. Llevar un control para identificar a los titulares que negaron su consentimiento y a las finalidades concretas para las cuales no se podrán tratar los datos personales.

11. Esperar el plazo de cinco días hábiles que señala el artículo 15 de los Lineamientos Generales, para utilizar los datos personales, cuando éstos se hayan obtenido de manera indirecta, el aviso de privacidad se haya dado a conocer por un medio que no permita el contacto directo o personal con el titular y se requiera el consentimiento tácito.

Documentar su actuar para acreditar que se cumplió con el principio de consentimiento.

13. Solicitar el consentimiento si hubo cambios en las finalidades informadas en el aviso de privacidad y éstas lo requieren por no actualizarse alguno de los supuestos previstos en el artículo 22 de la Ley General.

Mecanismos para cumplir con el principio de consentimiento.

1) En el caso del consentimiento expreso y expreso y por escrito, en todos los casos, deberá conservar el documento, físico o electrónico, que permita acreditar que obtuvo el consentimiento por parte del titular.

2) En el caso del consentimiento tácito, en virtud de que no hay una manifestación expresa del titular, las pruebas podrán ser aquéllas que permitan demostrar que el responsable puso a disposición de los titulares el aviso de privacidad.

3) Consentimiento expreso otorgado por los titulares y la solicitud respectiva.

4) Aviso de privacidad y procedimiento para su puesta a disposición.

5) Solicitar el consentimiento después de que se ponga a disposición del titular el aviso de privacidad.

6) Redactar las solicitudes de consentimiento de forma tal que éste sea libre, específico e informado, y que las solicitudes sean concisas e inteligibles, estén en un lenguaje claro y sencillo acorde con el perfil del titular, y se distingan de asuntos ajenos a la protección de datos personales, cuando ello sea necesario.

7) Definir el tipo de consentimiento que se requiere, según las categorías de datos personales que se vayan a tratar o las disposiciones normativas que regulen el tratamiento.

8) Habilitar los mecanismos necesarios para solicitar el consentimiento expreso, en los términos señalados en la columna anterior, así como documentar su obtención.

9) Documentar la puesta a disposición del aviso de privacidad para la obtención del consentimiento tácito.

10) Solicitar el consentimiento previo a la obtención de los datos personales y después de la puesta a disposición del aviso de privacidad, cuando los datos personales se obtengan directamente de su titular o representante.

11) Cuando los datos personales no los proporcione personal o directamente el titular o su representante, se deberá enviar a los titulares el aviso de privacidad correspondiente al medio de contacto que tenga registrado.

Respecto de menores de edad y personas que se encuentren en estado de interdicción o incapacidad

1) Identificar los tratamientos de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley, que requieren consentimiento, según el artículo 22 de la LGPDPPSO.

2) Poner a disposición de los padres, tutores o representantes legales el aviso de privacidad, así como también, cuando ello sea posible, a los menores de edad y al titular en estado de interdicción o incapacidad declarada conforme a ley.

3) Redactar los avisos de privacidad y solicitudes de consentimiento en lenguaje sencillo, adaptado para la comprensión del menor de edad o de la persona que se encuentre en estado de interdicción o incapacidad declarada conforme a ley.

4) Implementar mecanismos que permitan tener certeza que quien otorga el consentimiento, está facultado legalmente para ello, máxime cuando el mismo no se vaya a requerir con la presencia física de los padres, tutores o representantes legales.

5) Revisar la necesidad y legalidad del tratamiento de datos personales sensibles para cumplir con la finalidad de que se trate, a fin de que quede debidamente justificada su obtención y uso.

6) Verificar que el tratamiento de datos personales no tenga como consecuencia discriminación de los titulares.

7) Privilegiar el interés superior del menor de edad, cuando de encuentre en presencia de un tratamiento de sus datos personales.

8) Conocer la Ley General de Niñas, Niños y Adolescentes, con objeto de conocer los derechos de los menores de edad y las obligaciones al respecto.

9) Poner a disposición el aviso de privacidad tanto al adulto que tenga la representación del menor, como al propio titular de los datos personales.

10) Solicitar el consentimiento del adulto que tenga la representación del menor, cuando éste se requiera, y de manera adicional solicitar la opinión del propio titular.

V. Principio de Calidad.

El responsable deberá adoptar las medidas necesarias para tratar los datos personales para la finalidad o finalidades que fueron recabados, asimismo, a efecto de mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

En relación a lo anterior, se debe entender que los datos cumplen con dichas características cuando :

- **Exactos y correctos:** cuando en posesión del responsable no presentan errores que pudieran afectar su veracidad.
- **Completos**: cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento y de las atribuciones del responsable.
- **Actualizados**: cuando los datos personales responden fielmente a la situación actual del titular.

Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario.

Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, ni aquél que se requiera para cumplir con:

- Las disposiciones legales establecidas en la Ley General de Archivos.
- Las disposiciones aplicables en la materia de que se trate.
- Los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.
- El periodo de bloqueo.

El responsable deberá establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleve a cabo, en los cuales se incluyan los periodos de conservación de conformidad con el artículo 24 de la Ley General, asimismo, se deberá incluir mecanismos que permitan cumplir con los plazos fijados para la supresión de los datos personales, así como para realizar una revisión periódica sobre la necesidad de conservar los datos personales.

Una vez concluido el plazo de conservación, y siempre que no exista disposición legal o reglamentaria que establezca lo contrario, el responsable debe proceder a la supresión de los datos personales.

Por su parte, respecto de los datos personales sensibles, se deberá prever que se limite el periodo de tratamiento al mínimo indispensable.

Obligaciones vinculadas al principio de calidad.

El responsable tiene las siguientes obligaciones en torno al principio de calidad:

1) Adoptar las medidas que considere convenientes para procurar que los datos personales cumplan con las características de ser exactos, completos, actualizados y correctos, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que el titular se vea afectado por dicha situación.

2) Conservar los datos personales exclusivamente por el tiempo que sea necesario para llevar a cabo las finalidades que justificaron el tratamiento y para cumplir con aspectos legales, administrativos, contables, fiscales, jurídicos e históricos y el periodo de bloqueo.

3) Bloquear los datos personales antes de suprimirlos, y durante el periodo de bloqueo sólo tratarlos para su almacenamiento y acceso en caso de que se requiera determinar posibles responsabilidades en relación con el tratamiento de los datos personales.

4) Suprimir los datos personales, previo bloqueo, cuando haya concluido el plazo de conservación de conformidad con lo establecido por la Ley General de Archivos.

5) Establecer y documentar procedimientos para la conservación, bloqueo y supresión de los datos personales.

6) En caso de que se requiera, demostrar que los datos personales se conservan, bloquean y suprimen cumpliendo los plazos previstos para ello, o bien, en atención a una solicitud de ejercicio del derecho de cancelación.

7) Implementar medidas para que los datos personales se actualicen y, en su caso, corrijan o completen, en las distintas bases de datos que estén a cargo de la unidad administrativa.

Mecanismos para cumplir con el principio de calidad.

1) Base de datos actualizada y correcta.

2) Constancias o anotaciones sobre la rectificación realizada, en aquellos casos en que la misma haya sido procedente.

3) Instrumentos de clasificación archivística.

4) Documentación y evidencia que se genere con la implementación de los procedimientos para la conservación, bloqueo y supresión de los datos personales.

VI. Principio de Proporcionalidad.

El responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.

El principio de proporcionalidad establece la obligación del responsable de tratar sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.

De igual forma, el responsable deberá prever que los datos personales tratados sean los mínimos necesarios para lograr la finalidad o finalidades para las cuales se obtuvieron, las cuales, deben ser acordes con las atribuciones conferidas al responsable y señaladas en el aviso de privacidad.

Obligaciones vinculadas al principio de proporcionalidad.

En síntesis, de acuerdo con lo antes expuesto, el responsable tiene las siguientes obligaciones en torno al principio de proporcionalidad:

1) Analizar y revisar que se soliciten sólo aquellos datos personales que resultan indispensables para cumplir con las finalidades de que se trate.

2) Tratar sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.

3) Limitar al mínimo posible el periodo de tratamiento de datos personales sensibles.

4) Crear bases de datos con datos personales sensibles sólo cuando se cuente con el consentimiento expreso de su titular o en su defecto, se trate de los casos establecidos en el artículo 22 de la Ley General en la materia.

Mecanismos para cumplir con el principio de proporcionalidad.

1) Avisos de privacidad.

2) Documentos, expedientes, archivos o bases de datos correspondientes al tratamiento.

3) Normatividad que establezca, en su caso, los datos personales que deberán solicitarse para el tratamiento específico.

VII.- Información.

El responsable deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto y puedan ejercer su derecho a la protección de su información personal.

En ese sentido, todo responsable que trate datos personales, sin importar la actividad que realice, requiere elaborar y poner a disposición los avisos de privacidad que correspondan a los tratamientos que lleven a cabo.

Es importante tomar en cuenta que con independencia de que se requiera o no el consentimiento del titular para el tratamiento de sus datos personales, el responsable está obligado a poner a su disposición el aviso de privacidad, por lo que se deberán tener el número de avisos de privacidad que resulten necesarios de acuerdo con los tipos de tratamientos que realicen.

La disposición del aviso de privacidad implica publicar en un lugar visible, accesible y gratuito, en el cual el titular, de manera informada, cuente con la posibilidad de conocer el tratamiento que se les dará a sus datos personales. En ese sentido, el responsable no está obligado a entregar una copia del aviso de privacidad al titular, al menos que éste lo solicite.

Obligaciones vinculadas al principio de información.

El responsable tiene las siguientes obligaciones en torno al principio de información:

1. Poner a disposición de los titulares el aviso de privacidad en los términos que fije la Ley General en la materia y sus Lineamientos, aunque no se requiera el consentimiento de los titulares para el tratamiento de los datos personales.

2. Poner a disposición del titular el aviso de privacidad previo a la obtención de los datos personales, cuando éstos se obtengan de manera personal y directa del titular.

3. Poner a disposición del titular el aviso de privacidad al primer contacto que se tenga con éste, cuando los datos personales se hayan obtenido de una transferencia

consentida, de una que no requiera el consentimiento, o bien de una fuente de acceso público.

4. Poner a disposición del titular el aviso de privacidad previo a iniciar tratamiento de los datos personales para la finalidad para la que se obtuvieron (aprovechamiento), cuando éstos no se hayan obtenido de manera directa del titular, el tratamiento no requiera del contacto con él y se cuente con datos para contactarlo.

5. Poner a disposición del titular el aviso de privacidad previo a iniciar el uso de los datos personales para las nuevas finalidades, cuando el responsable requiera tratar los datos personales para finalidades distintas y no compatibles con aquéllas para las cuales los recabó inicialmente.

6. Redactar el aviso de privacidad de manera que sea claro, comprensible, con una estructura y diseño que facilite su entendimiento, para su elaboración tomar en cuenta el perfil de los titulares y atender lo siguiente: no usar frases inexactas, ambiguas o vagas; no incluir textos o formatos que induzcan al titular a elegir una opción en específico; no premarcar casillas en las que se solicite el consentimiento del titular, y no remitir a textos o documentos que no estén disponibles.

7. Ubicar el aviso de privacidad en un lugar visible y que facilite su consulta, con independencia del medio de difusión o reproducción que se utilice.

8. Comunicar el aviso de privacidad a encargados y terceros a los que remita o transfiera datos personales.

9. Demostrar el cumplimiento del principio de información, en caso de que así se requiera.

10. Cuando se utilice la modalidad integral del aviso de privacidad, incluir todos los elementos informativos previstos de la normatividad aplicable.

11. Cuando se utilice la modalidad simplificado del aviso de privacidad, incluir todos los elementos informativos correspondientes.

12. Elaborar y tener disponible para su consulta el aviso de privacidad integral, con independencia de que se ponga a disposición de los titulares el aviso de privacidad

en su versión simplificada previo a la obtención o aprovechamiento de los datos personales.

13. No establecer cobros para la consulta del aviso de privacidad.

14. Cuando así ocurra, informar en su portal de Internet, a través de una comunicación o advertencia colocada en un lugar visible y a la cual se pueda acceder desde el momento en que se ingresa a dicho portal, que están siendo utilizadas tecnologías de rastreo, que a través de éstas se pueden recabar datos personales y la forma en cómo se pueden deshabilitar.

15. Poner a disposición de los titulares un nuevo aviso de privacidad en los siguientes casos:

- Cambie la identidad del responsable.
- Se requiera recabar nuevos datos personales sensibles, patrimoniales o financieros y se requiera el consentimiento del titular.
- Se requiera tratarlos datos personales para nuevas finalidades que requieran el consentimiento del titular.
- Se requiera realizar nuevas transferencias que requieran el consentimiento del titular.

Mecanismos para cumplir con el principio de información.

1) Aviso de privacidad.
2) Evidencia de la difusión del aviso de privacidad por el medio de comunicación masiva.
3) Procedimiento o medio para la puesta a disposición de los avisos de privacidad.
4) Lugares y medios en los que se difundieron y colocaron los avisos de privacidad.
5) Medios en que se encuentren los avisos de privacidad integrales.

8.- Responsabilidad.

El responsable deberá adoptar políticas e implementar mecanismos para asegurar el cumplimiento de los principios, deberes y obligaciones en materia de protección de datos personales. Asimismo, para cumplir con este principio los responsables

deberán rendir cuentas sobre el tratamiento y protección de datos personales a las personas titulares y a los organismos garantes.

Bajo este principio, los responsables del tratamiento están obligados a velar por la protección de los datos personales aun y cuando los datos estén siendo tratados por encargados. Asimismo, este principio supone que el responsable tome las medidas suficientes para que los términos establecidos en el aviso de privacidad sean respetados por aquéllos con los que mantenga una relación jurídica, así como al momento de realizar transferencias nacionales o internacionales de datos personales.

Asimismo, para cumplir con dicho principio el responsable, deberá implementar los mecanismos previstos en el artículo 30 de la LGPDPPSO para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la presente Ley y rendir cuentas sobre el tratamiento de datos personales en su posesión al titular e Instituto o a los Organismos garantes, según corresponda, caso en el cual deberá observar la Constitución y los Tratados Internacionales en los que el Estado mexicano sea parte; en lo que no se contraponga con la normativa mexicana podrá valerse de estándares o mejores prácticas nacionales o internacionales para tales fines.

Obligaciones vinculadas al principio de responsabilidad.

1) Prever presupuesto para la instrumentación de programas y políticas de protección de datos personales.

2) Elaborar un programa de protección de datos personales que contemple el cumplimiento obligatorio al interior de la organización del responsable.

3) Elaborar y aplicar un programa de capacitación y actualización de los servidores públicos en materia de protección de datos personales, de conformidad con el apartado de Capacitación de este Programa.

4) Establecer un sistema de supervisión y vigilancia interna y/o externa para comprobar el cumplimiento de este programa, incluyendo las medidas de seguridad, que prevea una revisión cada dos años o antes si es necesario por un cambio sustancial en el tratamiento.

5) Establecer un procedimiento para atender dudas y quejas de los titulares con las características señaladas en la columna anterior.

6) Diseñar o modificar las políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de forma tal que prevean la privacidad por diseño y por defecto descritas en la columna anterior.

7) En todos los casos generar pruebas para acreditar el cumplimiento de los principios, deberes y obligaciones que establece la LGPDPPSO, los Lineamientos Generales y demás disposiciones que resulten aplicables.

8) Velar por el cumplimiento de los principios y responder por el tratamiento de los datos personales, aún por aquéllos comunicados a encargados;

9) Adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad, y

10) Tomar medidas para que los terceros con quienes mantiene una relación jurídica que implique el tratamiento de los datos personales, respeten el aviso de privacidad en el que se establezcan las condiciones de dicho tratamiento.

Mecanismos para acreditar el cumplimiento del principio de responsabilidad.

Se debe tomar en cuenta que los mecanismos que adopte el responsable, además de garantizar el debido tratamiento, deben privilegiar los intereses del titular y su expectativa razonable de privacidad

1) Destinar recursos autorizados para tal fin para la instrumentación de programas y políticas de protección de datos personales, lo cual se deberá contemplar en el Presupuesto del ejercicio en curso, en la medida que las condiciones presupuestarias lo permitan.

2) Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable.

3) Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales.

4) Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.

5) Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

6) Establecer procedimientos para recibir y responder dudas y quejas de los titulares.

7) Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la presente Ley y las demás que resulten aplicables en la materia.

8) Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la presente Ley y las demás que resulten aplicables en la materia.

Es importante señalar que los mecanismos señalados en la normatividad no son los únicos que podría adoptar el responsable para cumplir con el principio de responsabilidad. Puede optar por medidas adicionales o distintas que contribuyan a elevar los estándares de protección de datos personales y cumplir con la normativa que regula este derecho.

CAPÍTULO IV. DEBERES EN LA PROTECCIÓN DE DATOS PERSONALES

La Ley General y los LGPDPSP establecen los deberes que observarán los responsables en el tratamiento de los datos personales los cuales se relacionan entre sí y tendrán como objetivo principal garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

I. Deber de confidencialidad.

Para el cumplimiento de este deber los responsables deberán establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto a éstos, aún después de concluir su relación con el responsable.

Para el cumplimiento del deber de confidencialidad y comunicaciones de datos personales el responsable deberá observar lo dispuesto en los artículos 22 fracción II, 42, 58, 59, 64, 65, 66, 67, 68, 69, 70 y 71 de la Ley General y 46, 71, 72, 109, 110, 111, 113, 115, 116, 117 y 118 de los LGPDPSP.

En los casos en los que el responsable cuente con un Encargado, deberá formalizar la relación respectiva mediante contrato o cualquier otro documento, en cual se establecerá como cláusula general relacionada con los servicios que este preste, el guardar confidencialidad respecto de los datos personales tratados.

En las actividades de tratamiento de datos personales, realizadas por el encargado, este no ostentará poder alguno de decisión sobre el alcance y contenido, de igual forma limitará sus actuaciones a los términos fijados por el responsable.

El responsable será corresponsable por las vulneraciones de seguridad ocurridas en el tratamiento de datos personales que efectué el encargado a nombre y por cuenta de este.

La relación entre el responsable y el encargado deberá formalizarse mediante contrato o cualquier otro instrumento jurídico que decida el responsable y que permita acreditar su existencia, alcance y contenido. El instrumento jurídico mediante el cual decida el responsable formalizar la relación de servicios que preste el encargado, deberá prever, al menos las siguientes cláusulas generales:

- Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable.

- Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable.

- Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables.

- Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones.

- Guardar confidencialidad respecto de los datos personales tratados;

- Suprimir y devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y

- Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación o por mandato expreso de la autoridad competente.

Para la prestación de los servicios del encargado, además de las cláusulas generales anteriores, el responsable deberá prever en el instrumento jurídico las siguientes obligaciones:

- Permitir al Instituto o al responsable realizar verificaciones en el lugar o establecimiento donde lleva a cabo el tratamiento de los datos personales.
- Colaborar con el Instituto en las investigaciones previas y verificaciones que lleve a cabo en términos de lo dispuesto en la Ley General y demás normatividad aplicable en la materia, proporcionando información y documentación que se estime necesaria para tal efecto, y
- Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de sus obligaciones.

Los acuerdos entre el responsable y el encargado relacionados con el tratamiento de datos personales no deberán contravenir la Ley General, las disposiciones aplicables, así como lo establecido en el aviso de privacidad que corresponda.

Al momento de realizar transferencias de datos personales nacionales o internaciones, el responsable deberá aplicar el principio de responsabilidad.

El encargado también podrá subcontratar servicios que impliquen el tratamiento de datos personales por cuenta del responsable, siempre y cuando medie autorización

expresa de este último, como consecuencia el subcontratado asumirá el carácter de encargado conforme a lo establecido en la Ley General y demás disposiciones que resulten aplicables en la materia.

Cuando en el instrumento jurídico mediante el cual se haya formalizado la relación entre el responsable y el encargado, se establezca que este último pueda llevar a cabo a su vez las subcontrataciones de servicios, la autorización a la que refiere el párrafo anterior se entenderá como otorgada a través de lo estipulado, siempre y cuando medie la autorización expresa del responsable.

Obtenida la autorización expresa del responsable, el encargado deberá formalizar la relación adquirida con el subcontratado a través de algún instrumento jurídico que decida, el cual permita acreditar la existencia, alcance y contenido de la prestación del servicio en términos de lo previsto en la Ley General.

Para los servicios de subcontratación que impliquen tratamiento de datos personales, el instrumento jurídico que suscriba el encargado con el subcontratado deberá prever, al menos las cláusulas generales y las obligaciones antes descritas.

Asimismo, para el caso en que existan tratamientos de datos personales en los que el responsable se adhiera a servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias, mediante condiciones o cláusulas generales de contratación; exclusivamente podrá utilizar servicios en los que el o los proveedores guarden confidencialidad respecto de los datos personales sobre los que se preste el servicio.

Esto es, el responsable podrá contratar o adherirse a servicios, aplicaciones e infraestructura en el cómputo en la nube, y otras materias que impliquen el tratamiento de datos personales, siempre y cuando el proveedor externo garantice políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la Ley General y demás disposiciones que resulten aplicables en la materia.

Los proveedores de servicios de cómputo en la nube y otras materias que impliquen tratamiento de datos personales, para efectos de la Ley General y demás disposiciones aplicables en la materia, tendrán el carácter de encargados.

El responsable deberá delimitar el tratamiento de los datos personales por parte del proveedor externo a través de cláusulas contractuales u otros instrumentos jurídicos.

Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente:

- Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley General y demás normatividad aplicable en la materia;
- Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;
- Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio, y
- Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.

Cuente con mecanismos, al menos, para:

- Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;
- Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;
- Establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio;
- Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable y que este último haya podido recuperarlos, e
- Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien, en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.

El responsable no podrá adherirse a servicios que no garanticen la debida protección de los datos personales.

Para el caso que el encargado y subcontratado incumplan las obligaciones contraídas con el responsable y decidan y determinen por si mismos, los fines, medios y demás cuestiones relacionadas con el tratamiento de los datos personales, asumirán el carácter de responsable de conformidad con la normatividad que les resulte aplicable en función de su naturaleza pública o privada.

Por otra parte, cuando el responsable realice algún tipo de transferencia, el receptor de los datos personales deberá llevar a cabo el tratamiento de datos personales, garantizando su confidencialidad.

Toda transferencia de datos personales sea nacional o internacional, se encuentra sujeta al consentimiento de su titular. Por regla general, el consentimiento será tácito, salvo que una ley exija al responsable recabar el consentimiento expreso del titular para la transferencia de sus datos personales.

La Ley General, establece excepciones a las transferencias de datos, en las cuales el responsable no estará obligado a recabar el consentimiento del titular.

Todas las transferencias deberán formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, conforme a la normatividad aplicable al responsable, las cuales permitirán demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes, limitando el tratamiento de los datos personales transferidos a las finalidades que la justifiquen.

Al momento de realizar transferencias de datos personales nacionales o internaciones, el responsable deberá adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la Ley General y demás disposiciones aplicables en la materia.

Los casos de excepción se dan cuando:

- Tratándose de una transferencia nacional y se realice entre responsables, en el cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos;

- Tratándose de una transferencia internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México,
- La transferencia internacional, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el responsable transferente y el responsable receptor sean homólogas, o
- Las finalidades que motivan la transferencia internacional sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento del responsable transferente.

Tanto en las transferencias nacionales como en las internacionales, el responsable, deberá comunicar al receptor de los datos personales el aviso de privacidad, mediante el cual se tratan los datos personales del titular.

Tratándose de transferencias nacionales, el receptor de los datos personales asume el carácter de responsable, y deberá tratar los datos personales comprometiéndose a garantizar la confidencialidad y únicamente los utilizará para los fines que fueron transferidos, atendiendo a lo contenido en el aviso de privacidad que le será comunicado por el responsable transferente.

Para el caso de transferencias fuera del territorio nacional, el responsable sólo podrá realizarlas cuando el tercero receptor, encargado o destinatario se obligue a proteger los datos personales conforme a los principios, deberes y demás obligaciones similares o equiparables a las establecidas en la Ley General y demás normatividad aplicable en la materia, así como los términos previstos en el aviso de privacidad que le será comunicado por el responsable transferente.

Obligaciones vinculadas al deber de confidencialidad

1) Establecer controles o mecanismos para que todas las personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad, obligación que subsistirá aún después de finalizar sus relaciones con el mismo y sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.

2) Incluir en las medidas de seguridad, controles para garantizar la confidencialidad de los datos personales.

3) Implementar los controles para la confidencialidad de los datos personales, sin perjuicio de lo establecido por la Ley General de Transparencia y Acceso a Información Pública y la Ley Federal de Transparencia y Acceso a Información Pública.

4) Establecer cláusulas en los contratos con los encargados, que obliguen a la confidencialidad de los datos personales.

5) Implementar capacitación para los servidores públicos del Instituto, a fin de generar conciencia sobre la importancia de guardar la confidencialidad de los datos personales que tratan.

Mecanismos para acreditar el deber de confidencialidad.

1) Documento de seguridad.

2) Controles definidos para la confidencialidad de los datos personales.

3) Evidencia de la aplicación de los controles.

4) Contratos celebrados con los encargados del tratamiento.

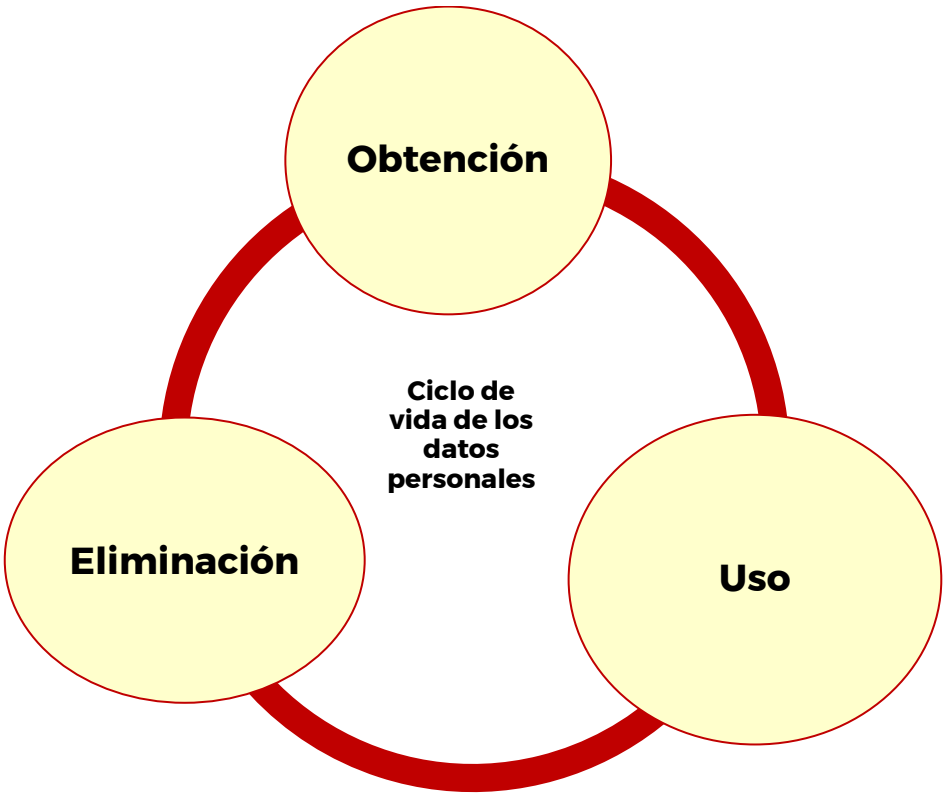
5) Documentación que acredite la capacitación de los servidores públicos.

II. Deber de seguridad

Para cumplir con dicho deber el responsable deberá establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico para la protección de datos personales en su posesión de conformidad con lo previsto en los artículos 31, 32 y 33 de la Ley General, con el objeto de impedir, que cualquier tratamiento de datos personales contravenga las disposiciones de dicho ordenamiento y los LGPDPSP.

El deber de seguridad deberá observarse durante todo el ciclo de vida de los datos personales, es decir, desde su obtención hasta su eliminación.

El ciclo de vida[1] de los datos personales es el siguiente:



Para cumplir con el deber de seguridad, todos los responsables deberán:

- Elaborar un documento de seguridad, que describa y dé cuenta de las medidas de seguridad que adopta.

[1] En la etapa de obtención: Se deberán observar los siguientes principios licitud, información, consentimiento, proporcionalidad, seguridad, confidencialidad.
En la etapa de uso: Se refiere al registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia, disposición, por lo que se deberán observar los principios de calidad, finalidad, lealtad, seguridad, confidencialidad.
En la etapa de eliminación: Se deberá observar el principio de calidad y seguridad

- Realizar diversas actividades interrelacionadas para establecer y mantener medidas de seguridad;
- Documentar las acciones relativas a las medidas de seguridad en un sistema de gestión, y
- En caso de que ocurra alguna vulneración, observar lo establecido en la Ley General y demás disposiciones aplicables en la materia.

Para cumplir con el deber de seguridad de datos personales el responsable deberá adoptar las medidas de seguridad necesarias para la protección de datos personales, las cuales son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten proteger los datos personales.

Las medidas de seguridad de conformidad con el artículo 3, fracción XX, XXI de la Ley General pueden ser:

- **Medidas de seguridad administrativas**: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.
- **Medidas de seguridad físicas:** Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:
    - Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información.
    - Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información.

  - Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización.
  - Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;
- **Medidas de seguridad técnicas:** Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:
  - Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados.
  - Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones.
  - Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.
  - Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales;

En la implementación de dichas medidas se deberán considerar:

- El riesgo inherente a los datos personales tratados;
- La sensibilidad de los datos personales tratados;
- El desarrollo tecnológico;
- Las posibles consecuencias de una vulneración para los titulares;
- Las transferencias de datos personales que se realicen;
- El número de titulares;

- Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
- El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

Asimismo, el responsable deberá realizar una revisión del marco normativo que regula el tratamiento específico de datos personales, con la finalidad de identificar medidas de seguridad adicionales y analizar la procedencia de su implementación. Dichas medidas deberán estar descritas de manera general en el documento de seguridad de cada responsable.

Obligaciones vinculadas al deber de seguridad

1) Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión.

2) Definir y comunicar las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.

3) Elaborar un inventario de datos personales y de los sistemas de tratamiento.

4) Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.

5) Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable.

6) Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.

7) Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

8) Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

9) Establecer y mantener medidas de seguridad administrativas, técnicas y físicas para la protección de los datos personales, a partir de las acciones que se describen en esta sección.

10) Revisar el marco normativo que regula el tratamiento específico de los datos personales, a fin de identificar medidas de seguridad adicionales y analizar la procedencia de su implementación.

11) Implementar el plan de monitoreo periódico en materia de protección de datos personales.

Mecanismos para acreditar el cumplimiento del deber de seguridad.

1) Programa de Protección de Datos Personales.
2) Documento de seguridad.
3) Evidencia generada en la implementación de los controles de seguridad.

4) Documentación que se genere con motivo de la implementación y evaluación del Programa de Protección de Datos Personales.

5) Documento en el que se establezcan las funciones, obligaciones y cadena de mando de cada servidor público, por unidad administrativa, que trate datos personales

6) Documento mediante el cual se haya comunicado las funciones, obligaciones y cadena de mando de cada servidor público.

7) Constancias de capacitación al personal del responsable.

8) Inventario de tratamiento de datos personales

9) Plan de trabajo elaborado.

10) Plan de monitoreo periódico.

11) Documentación que se genere a partir de la implementación del plan.

12) Programa de capacitación en materia de protección de datos personales.

13) Documentación que se genere a partir de la implementación del Programa.

CAPÍTULO V. CATÁLOGO DE DATOS PERSONALES

Con fundamento en el artículo 3, fracciones IX y X de la LGPDPPSO, para facilitar el cumplimiento del derecho al acceso a la información, así como a las obligaciones de transparencia, sin menoscabo de garantizar la protección y confidencialidad de los Datos Personales, el catálogo de datos personales se constituye como un instrumento que permita identificar las categorías, los tipos de datos, así como los documentos en los cuales se encuentran contenidos y que son responsabilidad de la unidad administrativa competente que, a nombre del INDAABIN, lleva a cabo su tratamiento, por lo que se enlista el catálogo de datos personales, de manera enunciativa mas no limitativa:

A) DATOS PERSONALES

Datos de documentos
▪ Alias, seudónimo, nombre de usuario (Nick name) ▪ Características físicas (rasgos fisonómicos) ▪ Clave de elector ▪ Clave Única del Registro de Población (CURP) ▪ Edad ▪ Fecha de nacimiento ▪ Estado civil ▪ Firma de particular(es) o tercero(s) ▪ Rúbrica de particular(es) o tercero(s) ▪ Fotografía (imagen) ▪ Videograbación (imagen) ▪ Hábitos o preferencias de consumo ▪ Lengua materna ▪ Lugar de nacimiento ▪ Matrícula del servicio militar ▪ Nacionalidad ▪ Nombre de particular(es) o ▪ tercero(s) ▪ Código OCR (reconocimiento óptico de caracteres) ▪ Ocupación ▪ Parentesco (filiación) ▪ Pregunta indicativa para recuperación de contraseña o validar acceso a software. ▪ Profesión ▪ Registro Federal de Contribuyentes (RFC) ▪ Señas particulares ▪ Usuario y contraseñas ▪ Vida familiar ▪ Sexo ▪ Origen racial o étnico ▪ Código postal ▪ Correo electrónico ▪ Domicilio ▪ Número de teléfono fijo o celular ▪ Municipio o alcaldía

- Huella dactilar
- Becas y/o estímulos otorgados
- Cédula profesional de particular(es) o tercero(s)
- Certificados de estudios
- Certificados de idiomas
- Calificaciones que revelan el aprovechamiento académico de una persona, así como los avances de créditos, tipos de exámenes, promedio
- Grado de estudios o nivel educativo
- Número de cuenta o matrícula escolar de institución educativa
- Profesión
- Cadena original del complemento de certificación digital
- Certificado de Sello Digital-Servicio de Administración Tributaria
- Código QR
- Firma electrónica
- Sello digital y/o código bidimensional

Datos Patrimoniales
▪ Beneficiarios ▪ Bienes inmuebles ▪ Capital social ▪ Código de seguridad ▪ Comprobante de pago de derechos ▪ Cuenta bancaria, número de cuenta bancaria y/o Clave Bancaria Estandarizada (CLABE) de personas físicas ▪ Cuenta bancaria, número de cuenta bancaria y/o Clave Bancaria Estandarizada (CLABE) de representantes legales de personas morales ▪ Cuenta catastral ▪ Dependientes económicos ▪ Estados de cuentas ▪ Facturas ▪ Folio y número de medidor de recibo de agua y predial y consumo ▪ Información bancaria ▪ Información relacionada con el patrimonio de una persona física ▪ Información relacionada con el Sistema de Ahorro para el Retiro (SAR) Información relacionada con estados financieros ▪ Ingresos por concepto de renta (patrimonio) ▪ Inmueble objeto de compraventa o monto de compraventa

- Inversiones
- Marca, modelo, número de motor y de serie, y placas de circulación de vehículo particular
- Número de acciones correspondiente a cada socio
- Número de póliza de seguros
- Participación societaria y nombre de socios contenidos en documentos notariados, tales como escrituras públicas, estatutos, contratos y convenios privados
- Patrimonio de una persona física
- Patrimonio de una persona moral
- Reporte de buró de crédito
- Secretos comerciales, industriales, fiscales, bancarios y fiduciarios
- Carta de naturalización
- Credencial de residencia temporal
- Credencial de residente
- Forma migratoria
- Número de identificación del extranjero (NIE)
- Situación migratoria
- Correo electrónico de trabajo de particular(es) o tercero(s)
- Cuotas sindicales
- Deducciones contenidas en recibos de pago
- Evaluaciones de desempeño
- Evolución salarial
- Montos aportados al Seguro de Separación Individualizado y/o Seguro de Vida Institucional
- Historial laboral
- Montos aportados para fondos de ahorro de los trabajadores
- Montos aportados para el Sistema de Ahorro para el Retiro
- Nombre de policías, custodios o personal de seguridad
- Número de ficha o de credencial de empleado
- Número de folio de aspirantes en concursos de acceso al Servicio Profesional de Carrera
- Número de Registro Patronal ante el Instituto Mexicano del Seguro Social
- Numero de seguridad social o número de afiliación
- Premios y/o reconocimientos

Datos sobre actos y procedimientos jurídicos

▪ Nombre de servidores públicos sujeto a procedimiento de responsabilidad administrativa ▪ Expedientes de procedimientos ▪ Nombre del actor en juicios ▪ Nombre del denunciado ▪ Nombre del denunciante(s), quejoso(s) o promovente(s) ▪ Nombre y firma del apoderado o representante legal en resoluciones y laudos ▪ Folio y número de medidor de recibo de agua y predial y consumo ▪ Medidas y colindancias de bienes inmuebles ▪ Pensiones alimenticias ▪ Régimen de sociedad conyugal

B) DATOS SENSIBLES

Datos sobre salud
▪ Alergias ▪ Certificados médicos ▪ Expediente clínico médico ▪ Estudios clínicos ▪ Grupo sanguíneo o tipo de sangre ▪ Intervenciones quirúrgicas practicadas ▪ Enfermedades y/o discapacidades ▪ Información psicológica ▪ Recetas médicas ▪ Tratamientos médicos ▪ Certificado de vacunación ▪ Información genética ▪ Sexualidad ▪ Huella dactilar o digital

Datos sensibles
▪ Orientación sexual ▪ Origen étnico y/o racial ▪ Creencias religiosas, filosóficas o morales

▪ Afiliación política y/o sindical ▪ Reconocimiento facial ▪ Reconocimiento de iris ▪ Reconocimiento de retina ▪ Reconocimiento vascular ▪ Geometría de la mano

CAPÍTULO VI. DOCUMENTOS QUE CONTIENEN INFORMACIÓN QUE PUEDE CONSIDERARSE CONFIDENCIAL Y QUE CONTIENEN DATOS PERSONALES QUE SE REFIEREN A PERSONAS FÍSICAS IDENTIFICADAS O IDENTIFICABLES.

A continuación, de manera enunciativa mas no limitativa, se enlistan los documentos que son susceptibles de contener datos personales, a efecto que el responsable los considere en el tratamiento que realice sobre estos:

Documentos que contienen información que puede considerarse confidencial
▪ Escrituras públicas ▪ Cédulas de identificación fiscal ▪ Acta de defunción ▪ Acta de matrimonio ▪ Acta de nacimiento ▪ Cartilla militar ▪ Credencial para votar ▪ Licencia de conducir ▪ Pasaporte ▪ Comprobante de domicilio ▪ Constancias de estudios ▪ Diplomas ▪ Visa ▪ Contratos laborales ▪ Constancias de trabajo ▪ Recibos de nómina ▪ Cédula de notificación ▪ Reporte de Buró de Crédito ▪ Certificados médicos ▪ Expediente clínico médico

CAPÍTULO VII. Criterios INAI en materia de protección de datos personales

El INAI es un organismo constitucional autónomo garante del cumplimiento los derechos fundamentales de acceso a la información pública y de protección de datos personales. Su órgano máximo de dirección es el Pleno y se integra por siete Comisionadas y Comisionados designados por el Senado de la República, de los cuales uno funge como Comisionado Presidente.

Asimismo, el Pleno del INAI tiene entres sus atribuciones expedir lineamientos y criterios que regulen la protección de datos personales.

Los criterios son el análisis que sobre un tema determinado ha realizado el Pleno, en materia de derecho de acceso a la información o de protección de datos personales, el cual deben aplicar los sujetos obligados del ámbito federal, mientras que para los organismos garantes de las entidades federativas sólo resulta orientador.

En ese sentido, en materia de datos personales el INAI ha emitido los siguientes criterios:

Datos personales	Sustento
Cédula profesional	Que los **Criterios 02/10 y 01/13** emitidos por el INAI se establece que la cédula profesional es un documento que tiene por objeto acreditar que una persona cuenta con la autorización para ejercer la profesión indicada en la misma; a través del conocimiento de algunos de los datos ahí contenidos se puede corroborar la idoneidad de la persona para ocupar el empleo, cargo o comisión encomendado. En tal sentido, ante una solicitud de acceso a la información que se relacione con la cédula profesional, las dependencias y entidades de la Administración Pública Federal deberán elaborar una versión pública en la que se omitirán los datos personales que no refieran al perfil profesional de su titular, tales como la Clave Única de

	Registro de Población y la firma. La fotografía de una persona física que conste en su título o cédula profesional no es susceptible de clasificarse con carácter de confidencial, en virtud del interés público que existe de conocer que la persona que se ostenta con una calidad profesional determinada es la misma que aparece en los documentos oficiales de referencia. Lo anterior es así, ya que en el momento en que una persona se somete a un registro fotográfico con el objetivo de recibir una identificación oficial que lo avala como profesionista, consiente que tanto la imagen de su rostro como su nombre y profesión, sean elementos de acreditación e identificación frente a terceros.
Clave Única de Registro de Población (CURP)	Que el **Criterio 18/17** emitido por el INAI señala que la Clave Única de Registro de Población (CURP) se integra por datos personales que sólo conciernen al particular titular de la misma, como lo son su nombre, apellidos, fecha de nacimiento, lugar de nacimiento y sexo. Dichos datos, constituyen información que distingue plenamente a una persona física del resto de los habitantes del país, por lo que la CURP está considerada como información confidencial.
Cuotas sindicales	Que el INAI en el **criterio 09/17** establece que las **cuotas sindicales** no están sujetas al escrutinio público. La información relativa a las cuotas sindicales no se encuentra sujeta al escrutinio público mandatado por la Ley General de Transparencia y Acceso a la Información Pública y la Ley Federal de Transparencia y Acceso a la Información Pública, ya que las mismas provienen de recursos privados que aportan los trabajadores afiliados.
Datos de identificación del representante o apoderado legal	Que en el **Criterio 01/09** el INAI estableció que los datos de identificación del representante o apoderado legal, es decir, el nombre, la firma y la rúbrica de una persona física que actúe como representante o apoderado legal de un tercero que haya celebrado un acto jurídico con algún sujeto obligado, es información pública, en razón de que tales datos fueron proporcionados con el objeto

	de expresar el consentimiento obligacional del tercero y otorgar validez a dicho instrumento jurídico.
Expediente clínico	Que en el **Criterio 4/09** el INAI determinó que el expediente clínico contiene información relacionada con el estado de salud del paciente -titular de los datos-, por lo que con independencia de que puedan obrar opiniones, interpretaciones y criterios de los profesionales de la salud que trataron al paciente, dicha información se ubica dentro de la definición de datos personales. Esta clasificación únicamente resulta oponible frente a terceros, pero no frente a su titular o representante legal, ya que son precisamente estos últimos quienes tienen derecho a solicitar su acceso o corrección, por tratarse de información personal concerniente a su persona y, por lo tanto, información de la que únicamente ellos pueden disponer. Por lo anterior, la información contenida en el expediente clínico debe ser protegida con fundamento en el artículo 116 primer párrafo de la LGTAIP y el artículo 113 fracción I de la LFTAIP
Información bancaria de los particulares	Que el **Criterio 10/13** emitido por el INAI determina que el número de cuenta bancaria de los particulares es información confidencial por referirse a su patrimonio. Derivado de lo anterior, se considera que dichos datos están asociados al patrimonio de una persona física, entendiendo este como es el conjunto de bienes, derechos y obligaciones correspondientes a una persona (física o moral) y que constituyen una universalidad jurídica. Por lo tanto, los datos relativos al número de cuenta, número de CLABE interbancaria y estado de cuenta bancario, constituyen información relacionada con el patrimonio de una persona física identificada y únicamente le incumbe a su titular o personas autorizadas para el acceso o consulta de información patrimonial, así como para la realización de operaciones bancarias. En este sentido, el sujeto obligado se encuentra, obligado a proteger el carácter de confidencial de la información, aunado a que su divulgación facilitaría que cualquier persona pudiera afectar el patrimonio de los particulares.

Nombres de actores en juicios laborales	Que en el **Criterio 19/13**, el INAI determinó que el nombre de actores en juicios laborales constituye, en principio, información confidencial, pues el nombre es un atributo de la personalidad y la manifestación principal del derecho a la identidad, en razón de que por sí mismo permite identificar a una persona física. Por lo que respecta al nombre de las personas que han entablado un juicio laboral, éste permite identificar a los actores que presentaron una demanda laboral y participan en un juicio, lo cual constituye una decisión personal que refleja un acto de voluntad de quien lo realiza. Las acciones legales que emprenden los actores en el ejercicio de sus derechos laborales hacen evidente la posición jurídica en la cual se han colocado por decisión propia, con relación a determinados órganos de gobierno, para la obtención de algunas prestaciones laborales o económicas, lo cual constituye cuestiones de carácter estrictamente privado. En este tenor, el nombre de los actores de los juicios laborales que se encuentran en trámite o que, en su defecto, concluyeron con la emisión de un laudo desfavorable a los intereses personales del actor constituye información confidencial. No obstante, procede la entrega del nombre de los actores en juicios laborales cuando, en definitiva, se haya condenado a una dependencia o entidad al pago de las prestaciones económicas reclamadas o la reinstalación del servidor público, en virtud de que el cumplimiento de dicho fallo se realiza necesariamente con recursos públicos a cargo del presupuesto del sujeto obligado, lo cual permite, por una parte, dar cumplimiento a las obligaciones de transparencia contenidas en la Ley y, por la otra, transparenta la gestión pública y favorece la rendición de cuentas a los ciudadanos, ya que se refiere al ejercicio de los recursos públicos y al cumplimiento que se da a las resoluciones emitidas por alguna autoridad jurisdiccional encargada de dirimir conflictos laborales.
Número de cuenta bancaria y/o CLABE	Que el **Criterio 10/17** emitido por el INAI señala que el número de cuenta bancaria y/o CLABE interbancaria

interbancaria de personas físicas y morales privadas	de particulares es información confidencial, al tratarse de un conjunto de caracteres numéricos utilizados por los grupos financieros para identificar las cuentas de sus clientes, a través de los cuales se puede acceder a información relacionada con su patrimonio y realizar diversas transacciones; por tanto, constituye información clasificada.
Número de empleado	Que en el **Criterio 06/09** el INAI acordó que cuando el número de empleado, o su equivalente, se integra con datos personales de los trabajadores o funciona como una clave de acceso que no requiere adicionalmente de una contraseña para ingresar a sistemas o bases de datos personales, procede su clasificación como información confidencial.
Registro Federal de Contribuyentes (RFC)	Que el INAI emitió el **Criterio 19/17**, el cual establece que el Registro Federal de Contribuyentes (RFC) de personas físicas es una clave de carácter fiscal, única e irrepetible, que permite identificar al titular, su edad y fecha de nacimiento, por lo que es un dato personal de carácter confidencial.

CAPÍTULO VIII. Documentos para la Protección de Datos Personales

De conformidad con el artículo 33 de la Ley General para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá emitir los siguientes documentos:

1) Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión.

2) Documento con el cual se define las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;

3) Elaborar un inventario de datos personales y de los sistemas de tratamiento.

4) Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en

su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.

5) Documento en el cual se realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable.

6) Documento que plasme un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.

7) Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

8) Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Adicionalmente, se deberá dar cumplimiento a los documentos mencionados en el anexo 8, del Instrumento Técnico de Evaluación emitido por el INAI, los cuales son:

1) Oficio o instrumento a través del cual se autoriza el destino de recursos para la instrumentación de programas y políticas de protección de datos personales.

2) Programa de protección de datos personales.

3) Política de protección de datos personales

4) Programa de capacitación de protección de datos personales.

5) Documento en el cual se especifiquen los sistemas de supervisión y vigilancia.

6) Documento en el cual el responsable establece el procedimiento para la recepción y respuesta de dudas, y quejas de los titulares en materia de protección de datos personales.

7) Documento de seguridad.

8) Políticas internas de gestión y tratamiento de los datos personales.

9) Documento mediante el cual se establecen los controles dirigidos a asegurar la confidencialidad que deben guardar todas las personas que intervienen en cualquier fase del tratamiento de datos personales.

10) Documento que contenga la relación de los instrumentos jurídicos que regulan la relación con los encargados, en cual se establecerá como cláusula general el guardar confidencialidad respecto de los datos personales tratados por el encargado.

11) Documento que contenga la relación de los instrumentos jurídicos mediante los cuales se formaliza la contratación o adhesión a servicios, aplicaciones e infraestructura en el cómputo en la nube y otras materias, en los cuales se establezcan las condiciones o cláusulas generales de contratación.

12) Documento que contenga la relación de los instrumentos jurídicos mediante los cuales se formalizan las transferencias de datos personales, y en los cuales el receptor de los datos personales se obliga a garantizar la confidencialidad de los datos personales a los que da tratamiento.

13) Documento que contiene los medios y procedimientos habilitados por el responsable para atender las solicitudes para el ejercicio de los derechos ARCO.

14) Documento mediante el cual el responsable da a conocer al público en general, los costos por la reproducción y envío de los datos personales que le sean solicitados

CAPÍTULO IX. SUPERVISIÓN EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES.

En términos de lo establecido en el artículo 84, fracción I de la Ley General el Comité de Transparencia será el encargado de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, por lo que le corresponderá establecer el sistema de supervisión y vigilancia interna y/o externa, incluyendo

auditorías, para comprobar el cumplimiento de la presente política de protección de datos personales;

Asimismo, de conformidad con el artículo 30, de la Ley General el Comité de Transparencia la presente Política se revisará de forma anual para, en su caso, determinar las modificaciones que se requieran.

TRANSITORIOS

PRIMERO. – Los presentes Lineamientos entrarán en vigor una vez que sean oficialmente notificados a las diversas áreas del INDAABIN.

SEGUNDO. – Que a través de la Unidad de Transparencia, se publiquen los presentes Lineamientos en el SIPOT de esta dependencia.