Introducción a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Av. Insurgentes Sur núm. 3211, Col. Insurgentes Cuicuilco, C.P. 04530

Del. Coyoacán, México, D.F.

Primera Edición, noviembre de 2013
Reedición, diciembre de 2016

Impreso en México / *Printed in Mexico*

Distribución gratuita

OBJETIVOS DE APRENDIZAJE

- Identificar las ideas, conceptos y definiciones básicas relacionadas con la protección de datos personales, para el mejor entendimiento del contenido de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

- Revisar la evolución del derecho a la protección de datos personales, a partir de sus orígenes en el marco del derecho a la privacidad e intimidad, hasta su reconocimiento como derecho humano autónomo e independiente.

- Reconocer los avances en la legislación nacional, así como las reformas constitucionales que motivaron la promulgación de la LFPDPPP.

- Reflexionar sobre la relevancia del derecho a la protección de datos personales, como un derecho humano de gran importancia en la era de la información, una vez revisados los antecedentes, ordenamientos internacionales y los aspectos generales que le dan su configuración actual.

- Identificar los contenidos fundamentales de la LFPDPPP, como instrumento que posibilita y garantiza la protección de datos personales en posesión de particulares en México.

INTRODUCCIÓN

Los datos personales se refieren a toda la información relativa a la persona que la identifican o la hacen identificable. Es la información que nos describe, que nos da identidad, nos caracteriza y diferencia de otros individuos.

Son datos que precisan aspectos relativos a nuestra persona, como pueden ser: nombre, edad, domicilio, correo electrónico, trayectoria profesional y laboral. Pero también, otros datos como: origen étnico, religión, preferencia sexual, ideología, situación patrimonial; así como características físicas: estatura, color de ojos o de piel, u otros como estado de salud, huella digital, datos genéticos, datos biométricos como tipo de sangre, entre otros.

UN DATO PERSONAL ES TODA AQUELLA INFORMACIÓN SOBRE MI PERSONA QUE ME IDENTIFICA O ME PUEDE IDENTIFICAR.

Los datos personales son necesarios para que una persona pueda convivir en sociedad. Le permiten interactuar y relacionarse con otros, ya sean personas, instituciones y organizaciones, sin que sea confundido con el resto de la colectividad. A menudo facilitamos nuestros datos personales, por ejemplo, para abrir una cuenta bancaria, solicitar una tarjeta de crédito, inscribirnos en un curso, solicitar una cita médica o cumplir con una obligación fiscal.

El intercambio de la información relativa a cada uno de nosotros posibilita la generación de transacciones de diversa índole, que redundan en el crecimiento económico, comercial y social de una persona, una comunidad o un país.

Ahora bien, toda esta serie de datos que me describen y a partir de los cuales me relaciono con otros, me pertenecen, son parte de mi identidad y personalidad, me identifican y diferencian de los demás, y nadie, salvo las excepciones que prevea la legislación de la materia, los puede usar sin mi autorización, yo soy el dueño de mi información personal, y por lo tanto, yo soy quien controlo el flujo de mis datos personales en mi interacción con los otros, a partir de elegir qué deseo comunicar, cuándo y con qué finalidad.

Al referirse a este poder de control que las personas debemos tener sobre nuestra información personal, José Luis Piñar Mañas, Catedrático en Derecho Administrativo, Ex Director de la Agencia Española de Protección de Datos (AEPD), señala que:

> “Este poder de control ha de ponerse en íntima relación con el consentimiento, que ha de ser el título esencial que justifique injerencias en nuestra privacidad.
>
> …Incluso estudios empíricos han demostrado que para el individuo ese control es capital: se ha constatado que quienes perciben que mantienen el control sobre el uso que se hace de sus datos tras haberlos facilitado a un tercero sienten su privacidad menos invadida que quienes piensan que

> han perdido el control sobre ellos. De hecho, la violación del derecho de una persona a controlar su esfera privada, sea ésta física o informativa, constituye el factor más importante para que se sienta invadida la privacidad. No es para ello necesario que la información sea más o menos importante o sensible. Una persona puede hacer pública información que le afecte sin que por ello considere violada su privacidad. Pero si pierde el control sobre ella, si alguien se la apropia, entonces pensará que su intimidad ha sido violada. Quien en alguna ocasión ha facilitado o ha permitido el acceso a su propia información no por ello renuncia a su privacidad[1].”

Este derecho a controlar la información que se refiere a nosotros mismos, es lo que da origen al concepto de **autodeterminación informativa** del que se hablará más adelante.

1 Piñar Mañas, José Luis, ¿Existe la privacidad?, Madrid, ed. CEU ediciones, 2008, p. 17.

TEMA I. CONCEPTOS Y DEFINICIONES BÁSICAS

Iniciaremos el recorrido de nuestro aprendizaje distinguiendo algunos conceptos que es necesario identificar: Privacidad, Intimidad y Protección Datos Personales.

CONCEPTO DE PRIVACIDAD

A continuación se presentan algunas ideas y reflexiones en torno al concepto de privacidad, planteadas por José Luis Piñar Mañas, en su artículo: ¿Existe Privacidad?

Este autor acude a las definiciones y opiniones de numerosos especialistas en el tema para realizar un recuento del significado que existe en torno al concepto de Privacidad que ha construido a lo largo de la historia, enfatizando de inicio que Robert Gellman ha advertido que "ninguna definición es posible", Judith Jarvis Thomson ha señalado que "nadie parece tener una clara idea de lo que es", y el Tribunal Europeo de Derechos Humanos precisa que éste "es un concepto amplio no susceptible de una definición exhaustiva".

Planteado lo anterior, el mismo Piñar Mañas, realiza un recorrido por distintas acepciones desarrolladas por los expertos respecto de este concepto, citando para ello lo siguiente:

En el campo del derecho refiere que es obligado ubicar el concepto que en 1888, el juez americano Thomas Cooley acuñó en torno a una definición de privacidad, señalando que ésta hace alusión al "derecho a ser dejado solo, a ser dejado en paz" (the right to be let alone). Definición retomada tiempo después por los jueces del Tribunal Supremo de Estados Unidos, Samuel D. Warren y Louis D. Brandeis en su famoso artículo "The Right to Privacy".

Posteriormente, las aportaciones realizadas por Alan F. Westin fueron de relevancia fundamental. Este autor concibe la privacidad en términos de "autodeterminación" (self determination), concepción que con posterioridad fue retomada por el Tribunal Constitucional Alemán en su sentencia del 15 de diciembre de 1983, sobre el Censo de Población, considerado éste como uno de los casos paradigmáticos que perfiló el contenido del derecho a la protección de datos personales.

Westin identificó cuatro aspectos de la privacidad que Darhl M. Pedersen amplió hasta cinco, los cuales hacen referencia a lo siguiente:

Soledad: situación en la cual los demás no pueden ver u oír lo que una persona está haciendo.

Aislamiento: implica la existencia de una distancia física para separarnos de los demás.

Reserva: significa controlar la revelación verbal de información a los otros.

Anonimato: se consigue no siendo identificado entre la multitud.

Intimidad: intimidad con los amigos e intimidad con la familia, que permitiría estar sólo con un grupo de personas excluyendo a los otros.

Ernesto Garzón Valdés por su parte, ha hecho una distinción entre lo íntimo y lo privado, se ha referido esta diferenciación en su relación también con lo público.

Sea en el ámbito de la privacidad o de la intimidad, el individuo debe poder controlar el nivel de interacción con los otros. "…**La idea de control** es la clave esencial de la privacidad, ocupa el papel central"[2], enfatiza Piñar Mañas y añade que es **Westin** quizá, quien primero y con mayor énfasis ha resaltado la importancia de este control, pues ha dicho que:

> "…la privacidad implica libertad para elegir qué se desea comunicar, cuándo y a quién, manteniendo el control personal sobre la propia información".[3]

Es por ello, que este poder de control debe estar en íntima relación con el consentimiento de la persona, consentimiento que, en su caso, justifique injerencias en nuestra vida privada. El énfasis está en ese poder de control, ese poder de disposición que tienen las personas, sobre su propia información.

Piñar Mañas agrega, citando a los expertos, que esa posibilidad de que las personas puedan actuar y expresarse libremente sin miedo a perder el control sobre su información personal genera "bienestar físico y psicológico, así como espiritual", como se ha demostrado desde la psicología. Se ha llegado incluso a afirmar que la función principal de la protección de la privacidad es salvaguardar la estabilidad y el bienestar de las personas.

Diríamos que esa facultad de controlar nuestra propia información, disminuye la posibilidad de que sean otros quienes tengan el control sobre ella. Pues somos cada uno de nosotros los que hemos de poder decidir el grado de privacidad que deseamos tener y hasta qué punto queremos abrirnos a los demás sin que existan intromisiones externas injustificadas.

En definitiva, concluye Piñar Mañas:

> "…el fundamento de la privacidad se encuentra en el respeto a la identidad y dignidad de las personas, así como a la libertad".[4]

2 Ibídem, p. 16-17.
3 Ibídem, p. 17.
4 Ibídem, p. 18.

CONCEPTO DE INTIMIDAD

Es difícil distinguir conceptualmente privacidad e intimidad pues son conceptos que están imbricados. Sin embargo, con la intención de precisar una diferenciación, que nos ayude a identificar, lo íntimo y lo privado, retomemos el planteamiento de **Ernesto Garzón Valdés**, que al respecto dice:

> "Consideraré que lo íntimo es, por lo pronto, el ámbito de los pensamientos de cada cual, de la formación de decisiones, de las dudas que escapan a una clara formulación, de lo reprimido, de lo aún no expresado y que quizás nunca lo será, no sólo porque no se desea expresarlo sino porque es inexpresable…"[5]

En el ámbito de la intimidad, dice, se encuentran aquellas acciones que no requieren de la intervención de terceros y que tampoco les generan a ellos ninguna afectación: acciones por ejemplo, de tipo fisiológico en las que la presencia de terceros no es tan sólo innecesaria sino hasta desagradable.

> "El velo protector de la intimidad puede ser llamado, parafraseando a Hobbes, el velo de la discreción. Se trata aquí de un velo de total opacidad que sólo podría ser levantado por el individuo mismo."[6]

Y agrega citando a **San Agustín** que al redactar sus confesiones dice:

"Hay muchos [...] que desean saber quién soy yo [...] los cuales, aunque hanme oído algo o han oído a otros de mí, no pueden aplicar su oído a mi corazón, donde soy lo que soy. Quieren, sin duda, saber por confesión mía lo que soy interiormente, allí donde ellos no pueden penetrar con la vista, ni el oído, ni la mente." [7]

En el ámbito de la intimidad, dice **Garzón Valdés**, es donde el individuo ejerce plenamente su autonomía personal, es el reducto último de la personalidad, es allí "**donde soy lo que soy**".

Es en la intimidad donde los individuos forjan su identidad, las ideas o planes de acción, que luego podrán manifestar en privado o en público, si así lo consideran, es por eso la importancia del respeto irrestricto a la intimidad y al desarrollo de ese proceso de construcción.

De acuerdo con **Garzón Valdés**, la esfera de la privacidad, por su parte, es el ámbito reservado a un tipo de situaciones o relaciones interpersonales en donde la selección de los participantes depende de la libre decisión de cada individuo. Es un ámbito reducido, por lo que se refiere al número de sus miembros, y en él pueden darse diversas relaciones interpersonales. En ocasiones, puede resultar un ambiente propicio para desvelar, si así se desea, parte de nuestra intimidad.

5 Cfr. Garzón Valdés, Ernesto, Lo íntimo, lo privado y lo público, México, ed. IFAI, 2005, Colección: Cuadernos de Transparencia, p. 17.
6 Idem.
7 Ibídem, pp. 17-18.

DATOS PERSONALES

El concepto de datos personales se refiere a cualquier información concerniente o relativa a una persona física identificada o identificable.

Ejemplos de datos personales son: nuestro nombre, la fecha de nacimiento, el domicilio donde residimos, nuestra dirección de correo electrónico personal, el número telefónico de casa, nuestras preferencias de entretenimiento, las creencias religiosas, por citar sólo algunos tipos de datos. Esta información da cuenta de quiénes y cómo somos, nos identifica.

Precisamente este tipo de información la proporcionamos con regularidad, incluso a veces sin percatarnos de ello, entregamos nuestros datos personales al realizar un trámite, o para obtener un servicio o beneficio, al buscar trabajo, etc.

Esta puesta a disposición de nuestra información personal en distintos espacios de la vida cotidiana, ha llevado a la reflexión sobre la importancia de contar con normas que permitan su adecuado tratamiento por quienes los tienen en su poder.

TEMA II. ORÍGEN Y EVOLUCIÓN DEL DERECHO A LA PROTECCIÓN DE LOS DATOS PERSONALES

El derecho a la autodeterminación informativa, tiene como un antecedente relevante el avance de los procesos de informatización o de penetración de las tecnologías de la información y de las comunicaciones (TIC), a partir de los años setenta. En la era de la información que cobra mayor relevancia la protección de los datos personales.

Ahora ya no basta guardar los datos en un archivero con llave o llevar un control de a quién se los dimos. Actualmente una infinidad de nuestros datos de carácter personal circulan por el ciberespacio, debido a la creciente oferta de servicios basados en Internet y a las redes sociales. El Internet es un espacio que nos brinda grandes posibilidades de comunicación, de relación, de información, de transacción, de educación, entre muchas otras oportunidades, y por esa razón, también exige para quienes lo usan o quienes proveen estos servicios, lo hagan con responsabilidad.

Los beneficios del avance de las TIC son innegables y no hay marcha atrás en este proceso evolutivo de la tecnología. Pero también es necesario tomar conciencia de que este fenómeno ha creado nuevos riesgos y amenazas para nuestra privacidad y seguridad personal, que el Estado deberá regular, proteger y prevenir.

Los riesgos que se han advertido con relación al tema de los datos personales asociados al Internet y a las redes sociales, son los conocidos como ciberdelitos, como es el caso del robo de identidad, la difamación, el uso indebido de la imagen y los fraudes, entre otros. Por otra parte, algunas empresas están adquiriendo bases de datos de carácter personal, con el propósito de armar perfiles y estrategias selectivas de mercado, con el riesgo de que ello se lleve a cabo sin supervisión y regulación alguna, lo que significa una amenaza a nuestro derecho de autodeterminación informativa, pero también se presta para una categorización basada en perfiles.

La utilización **no consentida** de nuestros datos personales como correo electrónico, domicilio, teléfono, nombre, los lugares que visitamos, lo que compramos o nuestra CURP, por citar algunos, constituye un tratamiento ilegítimo.

Esta situación había sido prevista desde finales de los años sesenta, cuando en el seno del Consejo de Europa, se llamó la atención sobre la necesidad de indagar acerca de las Tecnologías de la Información, su uso indebido y el riesgo para los derechos de las personas, especialmente con relación a su derecho a la intimidad, motivo por el cual fue formada en 1967, una Comisión Consultiva encargada de realizar un estudio al respecto.

Resultado de los trabajos de esta comisión, surgió la Resolución 509 de la Asamblea del Consejo de Europa, sobre los "Derechos humanos y nuevos logros científicos técnicos", primer antecedente de las legislaciones en materia de protección de datos personales, que fueron extendiéndose con posterioridad en el continente europeo.

Las naciones han expresado su preocupación en la formulación y ejecución de ordenamientos del más alto nivel, que garanticen el respeto a la vida privada y a la intimidad, que precisen lo relativo a la protección de los datos de carácter personal que se encuentran tanto en el sector público como en el privado. Asimismo, se ha reconocido que los flujos de información son vitales para el desarrollo de la economía global y para potenciar el comercio electrónico, por lo que es necesario regular su manejo.

A continuación, se presenta un resumen sobre los antecedentes y alcances de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

EL DERECHO A LA PRIVACIDAD EN LOS INSTRUMENTOS INTERNACIONALES

El derecho a la privacidad ha sido prácticamente incorporado en todos los instrumentos internacionales que reconocen la existencia de derechos fundamentales. En términos generales se ha establecido la protección contra injerencias arbitrarias en la vida privada, la familia, el domicilio o la correspondencia, así como contra ataques a la honra y reputación, lo cual ha sido señalado en los siguientes instrumentos:

Año	Instrumento internacional
1948	Art. 12 de la Declaración Universal de los Derechos Humanos.
1948	Art. V de la Declaración Americana de los Derechos y Deberes del Hombre.
1950	Art. 8 del Convenio para la Protección de los Derechos y las Libertades Fundamentales.
1966	Art. 17 del Pacto Internacional de los Derechos Civiles y Políticos.
1969	Art.11 apartado 2 de la Convención Americana sobre los Derechos Humanos.

ORÍGENES DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

Por lo que se refiere al derecho a la protección de datos personales, las primeras normas específicas en la materia surgen en Europa en los años setenta (Alemania, Francia, Dinamarca, Austria, Luxemburgo). En esa época se empieza a consolidar la informática como herramienta de gestión. El uso de las computadoras estaba restringido a la actividad estatal, a las universidades y a las grandes empresas, en ese contexto empieza a vislumbrarse la posibilidad de procesar y utilizar la información de las personas sin un límite explícitamente establecido en las normas.

En la década de los ochenta, se inicia el desarrollo de distintas normativas de observancia regional o internacional para los países firmantes. A continuación se presenta un resumen al respecto:

Directrices de la Organización para la Cooperación y el Desarrollo Económicos (Recomendaciones de la OCDE): establece los principios básicos aplicables al tratamiento de datos personales y a la vez garantiza la libre circulación de los mismos.[8]

Convenio 108 del Consejo de Europa: garantiza a los ciudadanos de los Estados contratantes, el respeto de sus derechos y libertades, en particular, el derecho a la vida privada frente a los tratamientos de datos personales, conciliando el libre flujo de información entre dichos Estados.[9]

Resolución 45/95 de la Asamblea General de la ONU: enumera una serie de principios en materia de protección de datos personales de aplicación mundial.[10]

Directiva 95/46/CE: amplía los principios ya recogidos en otros instrumentos internacionales e impide la creación de barreras para la libre circulación de los datos personales en todos los estados miembros de la Unión Europea.[11]

Art. 8 de la Carta de Derechos Fundamentales de la Unión Europea: reconoce el derecho a la protección de datos como un derecho fundamental y autónomo, distinto al derecho a la intimidad y la privacidad de las personas.[12]

8 **Directrices de la Organización para la Cooperación y el Desarrollo Económicos,** disponible en: http://www.oecd.org/sti/consumer/34012151.pdf, consultado el 29 de noviembre de 2016.

9 **Convenio 108 del Consejo de Europa,** disponible en: http://inicio.inai.org.mx/Estudios/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf, consultado el 22 de noviembre de 2016.

10 **Resolución 45/95 de la Asamblea General de la ONU,** disponible en: http://inicio.inai.org.mx/Estudios/D.3BIS-cp--Directrices-de-Protecci-oo-n-de-Datos-de-la-ONU.pdf, consultado el 22 de noviembre de 2016.

11 **Directiva 95/46/CE**, disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV:l14012, consultado el 22 de noviembre de 2016.

12 **Art. 8 de la Carta de Derechos Fundamentales de la Unión Europea,** disponible en: http://www.europarl.europa.eu/charter/pdf/text_es.pdf, consultado el 22 de noviembre de 2016.

Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico (APEC): busca un equilibrio entre la seguridad de la información personal y el libre flujo de ésta para fines comerciales.[13]

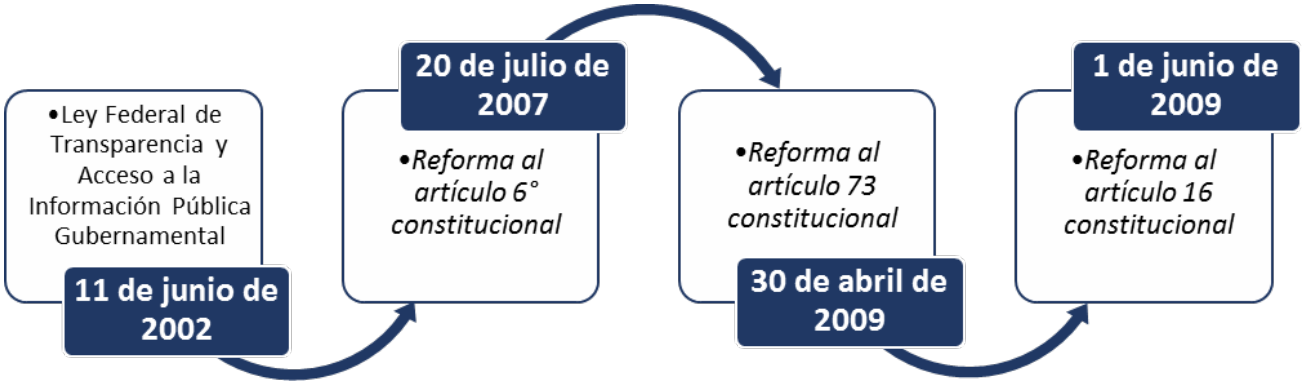
Directrices para la Armonización de la regulación de la Protección de Datos en la Comunidad Iberoamericana: ofrecen a los poderes públicos de los Estados Iberoamericanos criterios orientativos para el desarrollo de iniciativas normativas en esta materia, facilitando el establecimiento de un marco homogéneo que favorezca el intercambio de los flujos de información entre los Estados y terceros Estados bajo estándares similares de protección.[14]

Estándares Internacionales sobre Protección de Datos Personales y Privacidad. Resolución de Madrid: determina y define un conjunto de principios y derechos que garanticen la efectiva y uniforme protección de los datos personales, facilitando los flujos internacionales de éstos en un mundo globalizado.[15]

TEMA III. PROTECCIÓN DE DATOS PERSONALES EN MÉXICO

DESARROLLO NORMATIVO DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN MÉXICO

México ha consolidado avances paulatinos, pero trascendentales y contundentes en su legislación nacional, que van desde el año 2002 con la publicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), que reconoció por primera vez el derecho a la protección de datos personales en el ámbito público a nivel federal, hasta las recientes reformas constitucionales a los artículos 6, 73 y 16.



13 **Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico (APEC),** disponible en: https://www.sellosdeconfianza.org.mx/docs/marco_de_privacidad_APEC.pdf, consultado el 22 de noviembre de 2016.

14 **Directrices para la Armonización de la regulación de la Protección de Datos en la Comunidad Iberoamericana,** disponible en: http://inicio.inai.org.mx/Estudios/Directrices_de_armonizacion.pdf, consultado el 22 de noviembre de 2016.

15 **Estándares Internacionales sobre Protección de Datos Personales y Privacidad. Resolución de Madrid,** disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf, consultado el 22 de noviembre de 2016.

Estas reformas constitucionales, establecen el derecho fundamental a la protección de datos personales y lo dotan de contenido, asimismo, precisan la obligación del Congreso Federal de expedir una ley en la materia aplicable a los particulares. A partir de ellas, el Estado Mexicano dio un gran paso al reconocer, con la reforma al artículo 16, el derecho a la protección de datos personales como un derecho fundamental y autónomo, distinto del derecho a la intimidad, que cuenta con caracteres propios que dotan al individuo del poder de disposición sobre la información que le concierne. Lo anterior, contribuye sin duda, a garantizar la no injerencia y uso indiscriminado y excesivo de los datos de las personas, que circulan a diario en virtud del avance de las tecnologías de la información.

ETAPA 1. LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL

En nuestro país, el primer antecedente normativo en materia de protección de datos personales, lo constituye la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), publicada en el Diario Oficial de la Federación (DOF) el 11 de junio de 2002.

La LFTAIPG, estableció como propósito fundamental regular el derecho de acceso a la información y promover lo necesario para garantizar el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal, es decir, entes públicos en el orden federal. Aun cuando es un ordenamiento que tiene una fuerte carga hacia la regulación del derecho de acceso a la información pública, también tutela lo relativo a la protección de los datos personales en poder del sector público federal.

ETAPA 2. REFORMA AL ARTÍCULO 6° CONSTITUCIONAL

Con la reforma al artículo 6° de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), publicada en el DOF el 20 de julio de 2007, se dio un paso fundamental en el reconocimiento del derecho a la protección de datos personales. Se adicionó un segundo párrafo con siete fracciones, mismo que a continuación se incluye completo para su mejor comprensión, y sobre el cual se han resaltado las fracciones II y III, motivo de estudio de este tema. Asimismo, la fracción IV establece que deberán existir mecanismos de acceso a la información y procedimientos de revisión expeditos, así como una autoridad independiente para la atención de dichos procedimientos.

Artículo 6o

Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.

II. **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.**

III. **Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.**

IV. Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos. Estos procedimientos se sustanciarán ante órganos u organismos especializados e imparciales, y con autonomía operativa, de gestión y de decisión.

V. Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán a través de los medios electrónicos disponibles, la información completa y actualizada sobre sus indicadores de gestión y el ejercicio de los recursos públicos.

VI. Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.

VII. La inobservacia a las disposiciones en materia de acceso a la información pública será sancionada en los terminos que dispongan las leyes.

Con esta reforma:

- Por primera ocasión se hace referencia expresa al derecho a la protección de datos personales en la Constitución Política, como un derecho que debe armonizarse con el derecho de acceso a la información pública; protección cuyo ámbito de aplicación está referida a la información en poder de las autoridades, entidades, órganos y organismos de los tres órdenes de gobierno.

- El derecho a la protección de datos personales queda aquí definido como límite al derecho de acceso a la información pública.

ETAPA 3. REFORMA AL ARTÍCULO 73 CONSTITUCIONAL

Como ya se ha visto, entre las materias con las que se encuentra íntimamente vinculado el derecho a la protección de datos se encuentra el comercio internacional. Dentro de las razones históricas que justificaron la creación de este derecho y sus consecuentes instrumentos regulatorios, está el impedir la restricción de la libre circulación de los datos personales entre los Estados.

Otras razones que sirvieron de sustento para que la ley que regulara el tratamiento de datos personales en posesión de los particulares tuviera el carácter de federal, son las siguientes:

- El comercio internacional. En virtud de que el Estado Mexicano hacia el exterior es uno y como tal debe contar con una legislación uniforme en sus relaciones internacionales, independientemente del área del territorio nacional donde materialmente se estén tratando los datos personales.

- La materia de comercio es federal, de conformidad con nuestra Ley Fundamental. En lo que se refiere al comercio interno, contar con una regulación de datos personales en posesión de particulares en cada Estado de la República generaba distorsiones al flujo de datos. Una única regulación evitaría esta clase de distorsiones en el comercio interno.

Con la aprobación de esta reforma, el legislador contaría con los elementos para elaborar una ley de protección de datos personales de carácter federal, en la que las disposiciones correspondientes plasmarían los principios, derechos, procedimientos, infracciones, la existencia de una autoridad independiente y de un régimen de transferencias internacionales de datos, conforme a los estándares internacionales en esta materia. Lo anterior, no sólo garantizaría de manera homogénea el derecho a la protección de datos personales, en cualquier punto del territorio nacional también daría certeza y seguridad jurídica a los particulares cuyos datos son objeto de transferencias internacionales, lo cual atendería lo establecido en los ordenamientos internacionales de la materia que así lo exigen.

La estructura propuesta serviría de punto de partida para cualquier regulación que se emitiera en torno al derecho a la protección de datos, tanto en el ámbito público, el cual se vería fortalecido, como en el privado, considerando que hasta ese momento, no se contaba con una disposición a nivel constitucional en la que se estableciera el contenido y los alcances de este derecho, en cuanto a principios, derechos y excepciones por los que se debe regir todo tratamiento de datos personales, entre otros aspectos. La reforma señaló lo siguiente:

Artículo 73. El Congreso tiene facultad:

- I. a XXIX-N. ...
- XXIX-O. Para legislar en materia de protección de datos personales en posesión de particulares.
- XXX. ...

ETAPA 4. REFORMA AL ARTÍCULO 16 CONSTITUCIONAL

Un avance sustancial consistió en emitir un dictamen en el que se reconociera, a nivel constitucional, el derecho a la protección de datos personales, en razón de la evolución normativa experimentada hasta ese momento en nuestro país. La propuesta presentada, tenía como propósito consolidar este derecho, extendiendo su ámbito de aplicación a todos los niveles y sectores, consolidando, por una parte, la estructura edificada a través del artículo 6º fracción II de la Constitución y de la LFTAIPG, para los sistemas de datos personales en posesión de los entes públicos federales y, por la otra, reconociendo la existencia del mismo respecto de los datos personales en poder de los particulares.

Es así como el 1 de junio de 2009 se publica en el DOF, la reforma al artículo 16 de la CPEUM, adicionándose un segundo párrafo y recorriéndose los subsecuentes en su orden, para resultar de la siguiente manera:

Artículo 16

- Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.

- 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.

- No podrá librarse orden de aprehensión sino por la autoridad judicial y sin que proceda denuncia o querella de un hecho que la ley señale como delito, sancionado con pena privativa de libertad y obren datos que establezcan que se ha cometido ese hecho y que exista la probabilidad de que el indiciado lo cometió o participó en su comisión.

Con esta reforma se observan los siguientes avances normativos:

- El reconocimiento de los derechos de los titulares frente al tratamiento de sus datos, estos son, los derechos de acceso, rectificación, cancelación y oposición, denominados, por sus siglas, derechos ARCO, sin que se limite su ejercicio únicamente a los datos que se encuentren en los archivos del gobierno en sus tres órdenes.

- La existencia de principios a los que se debe sujetar todo tratamiento de datos personales.

- Los supuestos de excepción en cuanto a la aplicación de los principios y derechos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

- Se dota finalmente de contenido a esta garantía individual y se sitúa como un derecho fundamental y autónomo, ya no sólo circunscrito a su observancia por parte del Estado.

- Este nuevo derecho, consiste en la protección a la persona, con relación a la utilización que se dé a su información personal, tanto por entes públicos como privados.

Con estas reformas constitucionales, se sentaron las bases para la expedición de una ley en la materia que regulara el tratamiento de datos personales en el sector privado, una demanda latente desde 2001.

LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES (LFPDPPP)

Desde septiembre de 2001 hasta diciembre de 2009 se presentaron diversas iniciativas. Finalmente, el 5 de julio de 2010, se publica en el Diario Oficial de la Federación, el Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, ésta última vigente en tanto no se expida la Ley General en Materia de Datos Personales en Posesión de Sujetos Obligados.

El objeto de la LFPDPPP es la protección de datos personales en posesión de particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

DE ACUERDO CON EL DICTAMEN DE APROBACIÓN, ALGUNOS DE LOS BENEFICIOS QUE TIENE SU PROMULGACIÓN SON:

- Impone obligaciones a los sujetos que den tratamiento a la información de las personas, de manera que sólo utilicen los datos personales para los fines para los cuales fueron recabados, observando medidas de seguridad que eviten su pérdida, robo o acceso no autorizado.

- El titular de los datos gozará del derecho a controlar la información que sobre él detente cualquier particular: tiendas departamentales, hospitales privados, universidades, aseguradoras o bancos, entre otros.

- Los ciudadanos tendrán la posibilidad de acudir ante una autoridad independiente que les garantice pleno acceso a su información, la rectificación de sus datos en caso de estar incorrectos, pedir la eliminación o borrado de información incorrecta o innecesaria, y exigir el respeto a su derecho a oponerse a la utilización de su información, a menos que se cuente con su consentimiento.

- Al expedir esta Ley, México se coloca entre las democracias consolidadas que ya cuentan con marcos normativos en la materia.

- Esta Ley reconoce que toda persona tendrá la facultad de decidir quién, cómo y para qué usa su información personal, al ser el consentimiento uno de los principios de este derecho humano, ya que los datos sí tienen un dueño: el propio individuo.

TEMA IV. RELEVANCIA DE LA PROTECCIÓN DE DATOS PERSONALES

El derecho a la autodeterminación sobre los datos personales como prerrogativa de las personas para disponer de la información que sobre sí tienen las instituciones públicas o privadas en sus registros o bases de datos, a fin de que esa información sea veraz, íntegra, actualizada, no intrusiva, con las garantías de seguridad y de uso exclusivo para lo que fue proporcionada, constituye un replanteamiento de fondo sobre la forma en que se relaciona la persona con los datos que la identifican o la hacen identificable, pero también sobre la forma en que son administrados y protegidos por quienes los tienen para cumplir con sus funciones.

Como lo advierten los especialistas, es el propio titular el que debiera ser consciente, o al menos empezar a serlo, del valor de su información personal, en consecuencia, comenzar a actuar diligentemente respecto de su tratamiento, decidiendo personal y conscientemente qué tipo de cuidado y límites desea para su manejo.

RETOS O TENSIONES DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

Un aspecto que observa José Luis Piñar Mañas, es el relativo a las tensiones que se presentan en relación con este derecho. Señala que la privacidad se encuentra sometida a diversos riesgos y tensiones, en su relación con: la libertad de expresión, la transparencia y el acceso a la información, los intereses y evolución del mercado o la lucha por la seguridad ciudadana.[16]

Un ejemplo de lo mencionado lo constituye una ley aprobada en Estados Unidos con motivo de los hechos ocurridos el 11 de septiembre de 2001. Dicha ley es llamada Patriot Act de 2001, y constituye una prueba evidente de cómo pueden restringirse libertades y garantías constitucionales, al mismo tiempo, justificarse medidas contra la privacidad realizadas por los poderes públicos, apoyándose para ello en el uso de las nuevas tecnologías, en ocasiones, sin el conocimiento de los afectados.

Este autor considera que nunca antes se había podido invadir la privacidad de las personas como hoy en día, utilizando las tecnologías que se encuentran al alcance de casi toda persona. Pues hoy podemos conocer:

- Los contenidos de los correos electrónicos y de las llamadas efectuadas o recibidas mediante teléfonos móviles.
- Los datos genéticos pueden tratarse para múltiples finalidades.
- El uso de los datos biométricos está casi a la orden del día.
- Por medio de dispositivos de radiofrecuencia es posible además de controlar las ventas en un centro comercial, localizar personas.
- La capacidad de los ordenadores personales y sus funcionalidades se incrementan constantemente al tiempo que se reduce su costo.

16 Piñar Mañas, José Luis, op. cit., p. 13.

- Cada vez son más los casos en que se exige el tratamiento y transferencia internacional de datos, así como retenciones de datos en aras de la seguridad ciudadana.

- La sociedad corre el riesgo de verse sometida a video-vigilancia constante.

Los ejemplos citados son indicativos de la diversidad de situaciones en que nuestros datos personales pueden ser sujetos a tratamiento y sobre la importancia de contar con regulaciones adecuadas en esta materia.

BENEFICIOS

Al ubicarnos en nuestro país, podríamos señalar que algunas ventajas económicas que se tienen al contar con una regulación en esta materia son, entre otras:

- La alineación de México con los países miembros de la OCDE, la APEC y la Unión Europea, al contar con una ley que prevé los principios en esta materia, que actualmente son observados por los países miembros de dichos organismos.

- México, fue el primer país en emitir una ley que cumple con los Estándares Internacionales en materia de Privacidad, aprobados en la Conferencia Mundial de Comisionados de Privacidad y Protección de Datos de noviembre de 2009.

- Lo anterior puede derivar en flujos de inversión extranjera directa al brindar certeza jurídica en los intercambios comerciales transfronterizos, ya que se evitaría la existencia de barreras encubiertas a dichos intercambios en nombre del derecho a la protección de datos consagrado en nuestra Constitución. Situando a México en la tendencia mundial de alcanzar niveles de integración que permitan la libre circulación de mercancías, personas, bienes y capitales, al tiempo que se protege la información de las personas, por lo que este derecho se erige en un instrumento fundamental para dicha integración.

- Se prevé la existencia de mecanismos de autorregulación que faciliten la observancia de la ley dentro y fuera de las fronteras de nuestro país.

- Generación de fuentes de empleo e inversión extranjera en caso de que México contara con la aprobación por parte de la Unión Europea de país con un nivel adecuado de protección. En América Latina, únicamente Argentina cuenta con dicho reconocimiento, lo que representa para la economía de ese país ingresos anuales de mil millones de dólares aproximadamente, tan sólo en el terreno de las inversiones en el ámbito de la investigación médica y de ensayos clínicos.

- Al respecto, ya se encuentra documentado que el número de transferencias de datos personales desde Europa, a naciones con nivel adecuado de protección es notablemente mayor respecto de los que carecen de dicho estatus.

– La observancia de la Ley genera fidelidad en los clientes de una empresa. Se ha comprobado en los países que cuentan con leyes de esta naturaleza, que las campañas de difusión de la industria acerca de que los datos de sus clientes están actualizados y protegidos, ha traído como consecuencia que las personas escojan aquellas empresas que cumplan con la Ley y tal es el caso de empresas telefónicas europeas.

La divulgación de este nuevo derecho entre la población mexicana es una gran tarea que deberá realizar de manera conjunta el sector público y privado, con el fin de que las personas seamos conscientes de nuestro derecho y de la responsabilidad que tenemos con el cuidado de nuestra información personal.

La articulación de los principios, derechos y procedimientos relativos a la protección de datos personales en la dinámica cotidiana de las instituciones públicas y privadas, requerirá de acciones que observen aplicación de las responsabilidades señaladas en la Ley, mediante el establecimiento de políticas, procedimientos internos, mecanismos de seguridad, procesos de capacitación interna, entre otras acciones.

TEMA V. LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES

DISPOSICIONES GENERALES

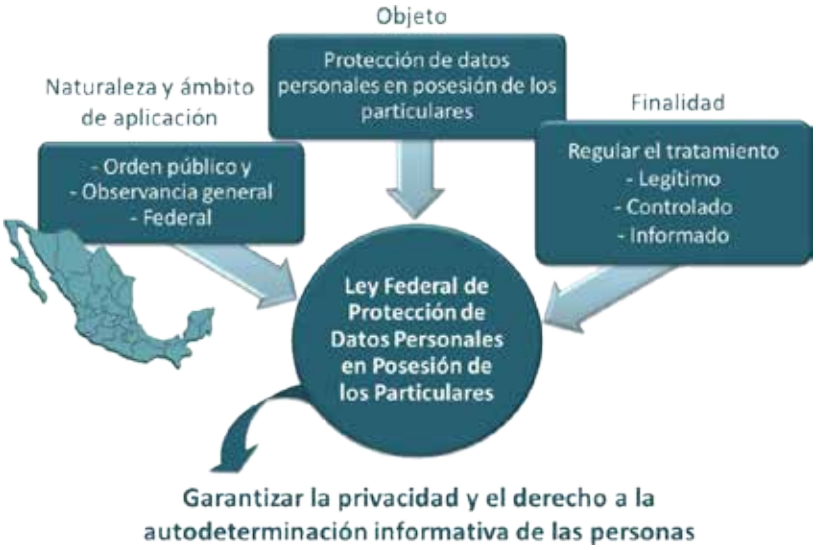
Capítulo I

Artículos 1 al 15

En este apartado se abordan los aspectos generales de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP): su naturaleza, ámbito de aplicación, objeto y finalidad; así como los sujetos que están obligados a cumplirla. Se presentan también algunas de las definiciones que serán de utilidad para la mejor comprensión de este ordenamiento legal.

CARACTERÍSTICAS GENERALES

La LFPDPPP es una Ley de orden público, pues regula un asunto que es de interés general: la protección de los datos personales que se encuentren en posesión de los particulares. Es una Ley Federal, de observancia general en toda la República Mexicana, lo que implica que debe cumplirse en todo el país.



SUJETOS REGULADOS

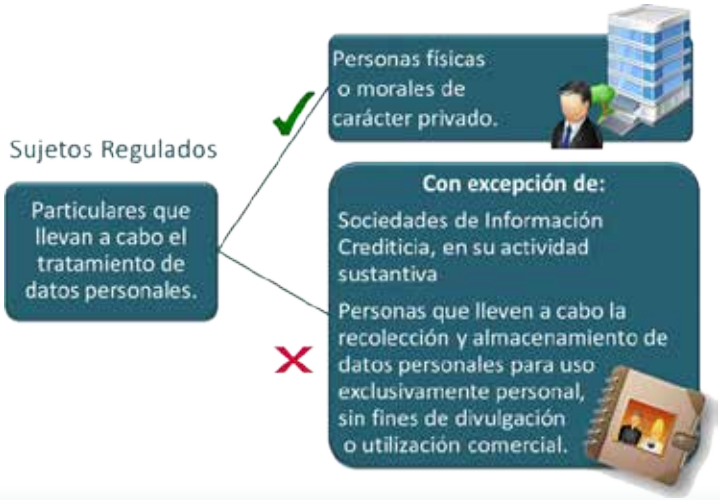
La Ley define que son sujetos regulados:

- Los particulares, personas físicas o morales de carácter privado, que lleven a cabo el tratamiento de datos personales.

Con excepción de:

- Las sociedades de información crediticia (burós de crédito) en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables.

- Las personas que lleven a cabo la recolección y almacenamiento de datos personales, para uso exclusivamente personal, esto es que no los usen con fines de divulgación o utilización comercial.



La primera excepción obedece a que existe regulación específica que dicta una serie de principios bajo los cuales este tipo de sociedades deben tratar la información objeto de sus actividades. La segunda excepción tiene como límite que la posesión de datos sea para uso doméstico, es decir, que por ningún motivo sean destinados para la obtención de un lucro o comercialización indebida.

ÁMBITO DE APLICACIÓN

Respecto al ámbito de aplicación, el Reglamento de la Ley precisa que dicho ordenamiento será de aplicación obligatoria cuando el tratamiento de datos personales:

- Sea efectuado en un establecimiento del responsable ubicado en territorio mexicano.

- Sea efectuado por un encargado, independientemente de su ubicación, a nombre de un responsable establecido en territorio mexicano.

- El responsable no esté establecido en territorio mexicano, pero le resulte aplicable la legislación mexicana, derivado de la celebración de un contrato o en términos del derecho internacional.

- El responsable no esté establecido en territorio mexicano y utilice medios situados en dicho territorio, salvo que tales medios se utilicen únicamente con fines de tránsito, que no impliquen un tratamiento. Para ello, podrá designar un representante o implementar el mecanismo que considere pertinente, siempre que a través del mismo se garantice que el responsable estará en posibilidades de cumplir de manera efectiva, en territorio mexicano, con las obligaciones que la normatividad aplicable imponen a aquellas personas físicas o morales que tratan datos personales en México.

En el caso de personas físicas:

- El establecimiento se entenderá como el local en donde se encuentre el principal asiento de su negocio o el que utilicen para el desempeño de sus actividades, por lo que podría ser, en algunos casos, su casa habitación.

Tratándose de personas morales:

- El establecimiento se entenderá como el local en donde se encuentre la administración principal del negocio.

- Si se trata de personas morales residentes en el extranjero, el local en donde se encuentre la administración principal del negocio en territorio mexicano, o en su defecto el que designen, o cualquier instalación estable que permita el ejercicio efectivo o real de una actividad.

DEFINICIONES

Como en todos los ordenamientos legales, en la LFPDPPP se enuncian las definiciones básicas que nos permiten comprender mejor su contenido, así como aquello que tutelan o regulan. Por su relevancia, incluimos, en orden alfabético, las siguientes:

Aviso de Privacidad

Documento físico, electrónico o en cualquier otro formato generado por el responsable que debe ser puesto a disposición del titular o "dueño de los datos", de manera previa a que éstos sean tratados, para hacerle saber, entre otros aspectos: quién los recabará, qué información se le solicitará, con qué finalidad se le requieren esos datos, los medios para ejercer su derecho de acceso, rectificación, cancelación u oposición, si se solicitarán datos sensibles, así como en su caso, las transferencias que se efectuarán.

Bases de datos

Es el conjunto ordenado de datos personales referentes a una persona identificada o identificable.

> El Reglamento de la Ley precisa que sus disposiciones serán aplicables al tratamiento de datos personales que obren en soportes físicos o electrónicos, que hagan posible el acceso a los datos personales con arreglo a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Bloqueo

Este concepto hace referencia a que:

- Una vez que se ha cumplido la finalidad para la cual fueron recabados los datos personales, su identificación y conservación únicamente tendrá el propósito de determinar posibles responsabilidades con relación a su tratamiento, hasta el plazo de prescripción legal o contractual de dichas responsabilidades.

- Por tal motivo, durante dicho periodo, los datos personales tendrán un tratamiento modulado, "estarán bloqueados" y una vez transcurrido éste, se procederá a su cancelación.

Consentimiento

Este concepto hace referencia a uno de los principios fundamentales de la protección de datos personales y es el eje central de todas las normativas en esta materia, pues el titular o dueño de los datos es quien puede decidir: quién, cómo, cuándo y para qué se tratan sus datos, es quien consiente la entrega de éstos porque así lo requiere para la realización de un trámite, la obtención de un servicio, la recepción de un beneficio, el cumplimiento de una obligación, etc.

Los estudiosos del tema señalan que en la facultad de consentimiento radica la sustancia de la autodeterminación informativa que tienen las personas sobre sus datos.

La Ley define el consentimiento como la manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de sus datos personales.

Datos personales

Como hemos abordado al inicio, los Datos Personales son cualquier información concerniente a una persona física identificada o identificable.

El Reglamento señala que los datos personales podrán estar expresados en forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo.

Y precisa que una persona física puede ser identificable cuando su identidad pueda determinarse, directa o indirectamente mediante cualquier información.

Agrega que una persona física no se considerará identificable si para ello se requieren plazos o actividades que resulten desproporcionadas.

Los Datos personales pueden depositarse en:

Datos personales sensibles

Son aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

En particular, se consideran sensibles aquéllos que puedan revelar aspectos como:

- Origen racial o étnico.
- Estado de salud presente y futuro.
- Información genética.
- Creencias religiosas, filosóficas y morales.
- Afiliación sindical.
- Opiniones políticas.
- Preferencia sexual, entre otros.

Disociación

Procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado en que se desagreguen, la identificación del dueño de los datos.

Fuente de acceso público

Aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, sin más requisito que, en su caso, el pago de una contraprestación

El Reglamento señala que tendrán el carácter de fuente de acceso público, las siguientes:

- Medios remotos o locales de comunicación electrónica, óptica y de otra tecnología, siempre que el sitio donde se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general.
- Directorios telefónicos en los términos de la normatividad específica.
- Diarios, gacetas o boletines oficiales, de acuerdo con su normativa.
- Medios de comunicación social.

Para que éstos sean considerados fuentes de acceso público, será necesario que su consulta pueda ser realizada por cualquier persona no impedida por una norma limitativa o sin más exigencia que, en su caso, el pago de una contraprestación, derecho o tarifa.

No se considera fuente de acceso público aquella que contenga información que sea o tenga una procedencia ilícita.

El tratamiento de datos personales obtenidos a través de este tipo de fuentes, respetará la expectativa razonable de privacidad.

Responsable

Persona física o moral de carácter privado que **decide** sobre el tratamiento de datos personales. El responsable de los datos personales asume en el marco de la LFPDPPP, funciones y obligaciones sustantivas para su debido cumplimiento.

Encargado

Es la persona física o jurídica que sola o conjuntamente con otras trate datos personales **por cuenta** del responsable.

El Reglamento complementa esta definición de la siguiente manera: es la persona física o moral pública o privada, **ajena a la organización del responsable**, que sola o conjuntamente con otras, trata datos personales por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Tercero

Persona física o moral, nacional o extranjera, a la que se **transfieren datos**, distinta del titular o del responsable del tratamiento de los datos personales.

Titular
Persona física a quien corresponden los datos personales, es el dueño de los datos, somos todas las personas.

Tratamiento
Esta es otra de las definiciones clave de la Ley, pues se refiere a todo manejo que se le dé a un dato personal por cualquier medio, pudiendo ser:

- La obtención.
- El uso, que abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.
- La divulgación.
- El almacenamiento de datos personales.

Remisión

El Reglamento define remisión como la **comunicación de datos personales** entre el responsable y el encargado dentro o fuera del territorio mexicano.

Dicha remisión tendrá por objeto la realización de un tratamiento por el encargado a cuenta del responsable.

Transferencia

Toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento.

Al respecto, el Reglamento señala que la transferencia implica la comunicación de datos personales dentro o fuera del territorio nacional, realizada a persona distinta del titular, del responsable o del encargado.

La Ley define que los principios y derechos previstos en ella tendrán únicamente como límite a su observancia y ejercicio:

- La protección de la seguridad nacional.
- El orden, la seguridad y la salud pública.
- Los derechos de terceros.

Supletoriedad

Se establece que de no existir una disposición expresa en la Ley, se aplicarán de manera supletoria las disposiciones del Código Federal de Procedimientos Civiles y de la Ley Federal de Procedimiento Administrativo.

Asimismo, se establece que para la substanciación de los procedimientos de protección de derechos, de verificación e imposición de sanciones se observarán las disposiciones contenidas en la Ley Federal de Procedimiento Administrativo.

LOS PRINCIPIOS. SUS IMPLICACIONES Y APLICACIÓN

Capítulo II

Artículos 6 al 21

En este apartado se explicarán los principios que rigen la protección de datos personales y que deben ser observados por los sujetos regulados.

Se explicará brevemente la forma en que la Ley y el Reglamento establecen su concreción y las implicaciones que conllevan.

La Ley establece que los responsables en el tratamiento de datos personales deberán observar los siguientes principios:

- Licitud
- Lealtad
- Consentimiento
- Finalidad
- Proporcionalidad
- Calidad
- Información
- Responsabilidad

LICITUD

Se refiere a que los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas en la Ley y demás normas aplicables, tanto las contenidas en la legislación mexicana como en el derecho internacional. Es decir, con pleno cumplimiento de la legalidad y respeto de la buena fe y los derechos del individuo, cuya información es sometida a tratamiento. Todo tratamiento de datos personales no debe contravenir ninguna disposición normativa.

LEALTAD

El tratamiento de datos personales debe realizarse en atención a lo acordado, tomando en consideración la expectativa razonable de privacidad del titular de los datos, sin causar perjuicio alguno a los intereses del titular.

Lo anterior tiene que ver con que la obtención o conservación de datos personales no se realice a través de medios engañosos o fraudulentos, de forma que el individuo no pueda conocer con propiedad los términos y condiciones vinculados a ese tratamiento.

El Reglamento señala que se actúa de manera fraudulenta o engañosa cuando:

- Exista dolo, mala fe o negligencia en la información proporcionada al titular respecto del tratamiento de los datos personales.
- Se vulnere la expectativa razonable de privacidad de los datos personales del titular.
- Las finalidades no fueron las informadas en el Aviso de Privacidad.

CONSENTIMIENTO[17]

Se refiere a que todo tratamiento de datos personales estará sujeto al consentimiento del titular de los datos, salvo en el caso de las excepciones que establece la Ley. Las personas tienen la facultad de decidir sobre el tratamiento de sus datos personales (derecho a la autodeterminación informativa).

Dado que el derecho a la protección de datos consiste en el poder de decisión y control de que goza el individuo sobre el tratamiento de sus datos personales, la manifestación de ese poder decisorio se sitúa como la principal forma de legitimar el tratamiento.

El Reglamento establece que, lo que se refiere a manifestación de la voluntad, el consentimiento debe ser:

- **Libre**: que no medie error, mala fe, violencia o dolo, que puedan afectar la manifestación de voluntad del titular.
- **Específico**: que se refiera a una o varias finalidades determinadas que justifiquen el tratamiento.
- **Informado**: que el titular tenga conocimiento del Aviso de Privacidad, previo al tratamiento a que serán sometidos sus datos personales y las consecuencias de otorgar su consentimiento.

La Ley establece que el consentimiento podrá ser:

- **Tácito**: Cuando al ponerse a disposición del titular de los datos el Aviso de Privacidad, éste no manifieste oposición a su tratamiento.
- **Expreso**: Cuando se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología o por signos inequívocos.

17 Para mayor referencia consultar los artículos 10 y 37 de la LFPDPPP.

El consentimiento expreso también deberá ser inequívoco, es decir, que existan elementos que de manera indubitable demuestren su otorgamiento. Se trata de una acción u omisión que implique la existencia del consentimiento por parte del titular.

El consentimiento podrá ser revocado en cualquier momento, sin que se le atribuyan efectos retroactivos.

Para que pueda llevarse a cabo la revocación del consentimiento, se deberán establecer en el Aviso de Privacidad los mecanismos y procedimientos correspondientes.

Cabe señalar que los datos financieros o patrimoniales requerirán de consentimiento expreso del titular, salvo las excepciones señaladas en los Artículos 10 y 37 de la Ley, en donde se refieren los supuestos en los que **no** será necesario solicitar el consentimiento para su tratamiento (Artículo 10) y se definen las excepciones al consentimiento en caso de transferencias nacionales e internacionales (Artículo 37), mismos que se describirán en líneas posteriores.

Consentimiento tácito

El Reglamento precisa que salvo que la Ley exija el consentimiento expreso del titular, será válido el consentimiento tácito como regla general.

Consentimiento expreso

Señala que el responsable deberá obtener el consentimiento expreso del titular de los datos cuando:

- Lo exija una ley o reglamento.
- Se trate de datos financieros o patrimoniales.
- Se trate de datos sensibles.
- Lo solicite el responsable para acreditar dicho consentimiento.
- Lo acuerden así el titular y el responsable.

Consentimiento para datos personales sensibles

En caso de que se trate 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, electrónica o cualquier otro mecanismo de autenticación que se establezca.

Cuando se trate de datos personales sensibles, **no** podrán crearse bases de datos sin que exista una justificación de su creación para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.

Por ejemplo, las instituciones de salud recaban datos personales de esta naturaleza y es de suponerse que, en términos generales, esa obtención tiene un fin legítimo.

Con relación a la creación de bases de datos que contengan este tipo de datos, el Reglamento precisa que sólo podrán crearse cuando:

- Obedezca a un mandato legal.
- Se justifique en términos del artículo 4 de la Ley (la seguridad nacional, el orden, la seguridad o la salud públicos; derechos de terceros).
- El responsable lo requiera para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persiga.

Consentimiento expreso verbal

El Reglamento señala que se considerará que el consentimiento expreso se otorga verbalmente cuando el titular lo externa al responsable de manera presencial o a través de cualquier tecnología que permita este tipo de interlocución.

Consentimiento expreso escrito

El consentimiento expreso se otorga de manera escrita cuando el titular lo externe en un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por la normatividad aplicable.

En el entorno digital, podrá ser a través de firma electrónica o cualquier otro mecanismo o procedimiento que al efecto se establezca, permitiendo identificar al titular y recabar su consentimiento.

Para acreditar la obtención del consentimiento, la carga de probarlo será siempre del responsable.

Excepciones al consentimiento

No será necesario el consentimiento para tratar datos personales cuando:

- Se encuentre previsto en una Ley.
- Los datos personales se encuentren en fuentes de acceso público.
- Los datos personales se hayan disociado.
- Exista un propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular de los datos y el responsable.
- Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o bienes.

- Sean indispensables para la atención médica, la prevención, diagnóstico, la atención de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, siempre y cuando el titular no esté en condiciones de otorgar su consentimiento, en términos de lo que establece la Ley General de Salud y demás disposiciones jurídicas aplicables y que el tratamiento se realice por una persona sujeta al secreto profesional u obligación equivalente.

- Se dicte resolución de autoridad competente.

FINALIDAD

El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades para las cuales se hayan obtenido, mismas que deben estar previstas en el Aviso de Privacidad.

En caso de que el responsable pretenda tratar los datos para una finalidad distinta que no sea compatible o análoga a la señalada en el Aviso de Privacidad, deberá obtener nuevamente el consentimiento del titular.

En el caso del tratamiento de datos personales sensibles, el responsable deberá realizar esfuerzos razonables para limitar el periodo de tratamiento a efecto de que sea el mínimo indispensable.

Al respecto, el Reglamento precisa que la finalidad o finalidades deberán ser determinadas.

La finalidad o finalidades del tratamiento es determinada cuando con claridad, sin lugar a confusión y de manera objetiva, se especifique para qué objeto serán tratados los datos personales.

También indica que el responsable **identificará y distinguirá en el Aviso de Privacidad, las finalidades que originaron el tratamiento y son necesarias para la relación jurídica entre el responsable y el titular, de aquéllas que no lo son**.

PROPORCIONALIDAD

Se refiere a que el tratamiento de datos personales será el que resulte necesario, adecuado y relevante en atención a las finalidades previstas en el Aviso de Privacidad.

En el caso de los datos sensibles, el responsable deberá realizar esfuerzos razonables para limitar el periodo de tratamiento a fin de que sea el mínimo indispensable.

CALIDAD

Este principio se refiere a que los datos personales que se traten deben ser pertinentes, correctos y actualizados para la finalidad para la cual fueron recabados.

El Reglamento señala que se considerarán correctos los datos personales proporcionados directamente por el titular hasta que éste no manifieste y acredite lo contrario, o bien, el responsable cuente con evidencia objetiva que los contradiga.

El responsable deberá adoptar los mecanismos necesarios para procurar que los datos personales que trate atiendan a este principio, con el 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.

Cuando los datos hayan dejado de ser necesarios para las finalidades previstas en el Aviso de Privacidad y las disposiciones legales aplicables, deberán cancelarse.

Cumplida la finalidad o finalidades, y no exista disposición legal o reglamentaria contraria, el responsable deberá cancelar los datos, previo bloqueo de éstos, para su posterior supresión. Para realizar lo anterior, los responsables procurarán establecer y documentar los procedimientos para la conservación, bloqueo y supresión señalando los periodos de conservación en atención a las disposiciones procedentes en materia administrativa, contable, fiscal o por cualquier otra obligación jurídica e histórica de la información.

INFORMACIÓN

Se refiere a la obligación del responsable de hacer saber a los titulares de los datos personales la información que se recaba de ellos, con qué fines y el tratamiento que dará a los datos, lo que se realizará a través del Aviso de Privacidad.

El Reglamento precisa que el Aviso de Privacidad deberá ser sencillo, con la información necesaria, expresado en lenguaje claro, comprensible, estructurado y con un diseño que facilite su entendimiento.

AVISO DE PRIVACIDAD

Es un documento físico, electrónico o en cualquier otro formato (visual, sonoro, etc.) generado por el responsable de manera sencilla, con un lenguaje claro y comprensible, que se pone a disposición del titular, previo al tratamiento de sus datos personales.

Objetivo

- Establecer los términos, alcances y condiciones del tratamiento de los datos personales.
- Informar al titular para que pueda tomar decisiones informadas sobre sus datos, a efecto de mantener el control y disposición sobre ellos.

– Debe ser sencillo y con la información necesaria.
– Expresado en español.
– Utilizar un lenguaje claro y comprensible.
– Para su redacción tomar en cuenta el perfil del titular.

– No usar frases inexactas, ambíguas o vagas.
– No incluir textos o formatos que introduzcan al titular a elegir una opción en específico.
– No incluir casillas previamente marcadas.
– No remitir a textos o documentos que no estén disponibles para el titular.

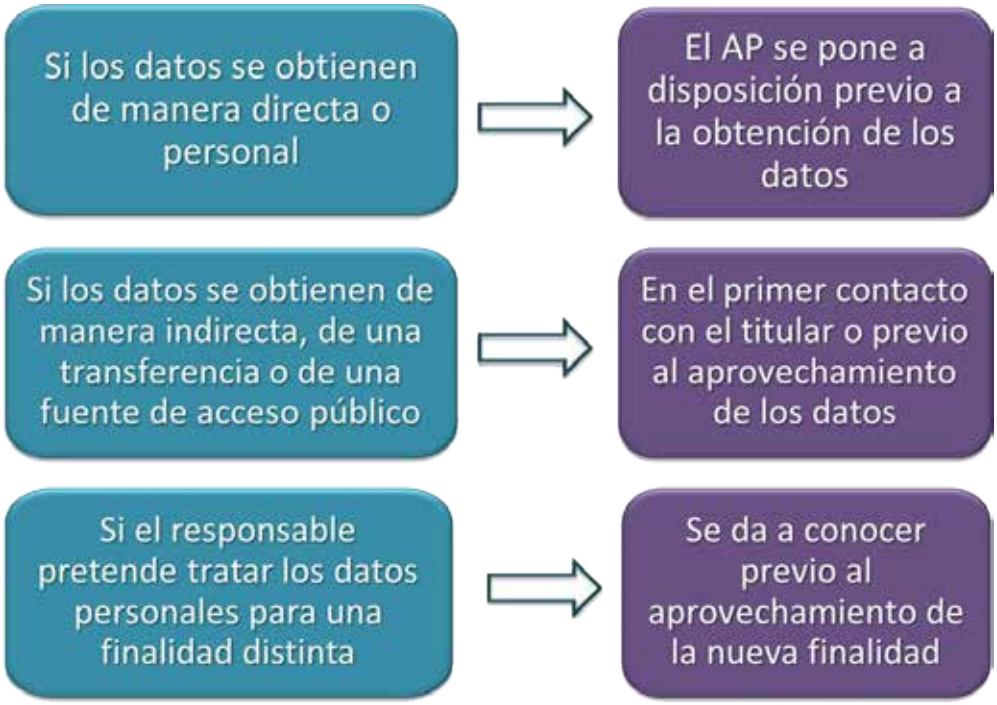
Contenido mínimo del Aviso de Privacidad

	Elementos del Aviso de Privacidad
1	Identidad y domicilio del responsable.
2	Los datos personales que serán sometidos al tratamiento.
3	El señalamiento expreso de los datos sensibles que se recaban.
4	Las finalidades del tratamiento (incluyendo las mercadotécnicas, publicitarias o de prospección comercial).
5	Los mecanismos para que el titular manifieste su negativa para el tratamiento de datos que no son necesarios para cumplir con la relación jurídica con el responsable.
6	Las transferencias que en su caso se efectúen, incluyendo el nombre de los terceros receptores y la finalidad de las mismas.
7	La cláusula que indica si el titular acepta o no la transferencia.
8	Los medios y procedimientos para el ejercicio de los derechos ARCO.
9	Los mecanismos y procedimientos para poder revocar el consentimiento.
10	Las opciones y medios para limitar el uso o divulgación de datos personales.
11	Informar sobre el uso de mecanismos en medios remotos o locales de comunicación que permitan recabar datos de manera automática y simultánea cuando el titular hace contacto con los mismos.
12	Los procedimientos y medios para comunicar cambios al Aviso de Privacidad.

Momentos para la puesta a disposición del Aviso de Privacidad

El momento en que el responsable debe poner a disposición de los titulares el Aviso de Privacidad depende de la forma en que se obtengan los datos personales, es decir, si éstos se recaban personal, directa o indirectamente del titular.

A partir de lo anterior, tenemos que el Aviso de Privacidad (AP) se pone a disposición en los siguientes momentos:



RESPONSABILIDAD

Corresponderá al responsable velar por el cumplimiento de los principios establecidos en la Ley, debiendo adoptar las medidas necesarias, lo cual aplicará aún y cuando estos datos fueren tratados por un tercero a solicitud del responsable. El responsable deberá garantizar que en todo momento el Aviso de Privacidad sea respetado por él o por terceros con los que tenga alguna relación jurídica.

Este principio implica que el responsable deberá rendir cuentas al titular en caso de incumplimiento, independientemente de quién realice el tratamiento, y si fue dentro o fuera del país donde se recabó la información.

Este principio es una garantía para el titular, quien deposita su confianza en el responsable, mismo que deberá tomar todas las previsiones para que los datos sean tratados de acuerdo con la voluntad del dueño de la información.

Así, dado que existe un tráfico de datos intenso y en muchas ocasiones éste se da fuera de las fronteras de nuestro país, la persona tendrá la tranquilidad de que si su información ha trascendido a manos de terceros en otras latitudes, estará enterada de las medidas con que debe tratar su información.

La Ley señala que el responsable deberá, entre otras obligaciones:

- Procurar que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.

- Cancelar los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el Aviso de Privacidad y las disposiciones aplicables.

- Eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de 72 meses, mismo que se contará a partir de la fecha en que se presente el incumplimiento.

- Establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Estas medidas no deberán ser menores a aquellas que mantengan para el manejo de su información. Se deberá tomar en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

- Realizar esfuerzos razonables para limitar el periodo de tratamiento de los datos personales sensibles, a efecto de que sea el mínimo indispensable.

- Comunicar a los titulares de cambios al Aviso de Privacidad, de conformidad con lo previsto en la Ley.

- El Reglamento precisa que en términos del artículo 14 de la Ley, el responsable deberá adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.

- Señala que entre las medidas que podrá adoptar el responsable se encuentran, por lo menos, las siguientes:

  - Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.

  - Poner en práctica un programa de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales.

  - Establecer un sistema de supervisión y vigilancia interna, así como verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.

  - Destinar recursos para la instrumentación de los programas y políticas de privacidad.

- Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.

- Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.

- Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.

- Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.

- Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y el presente Reglamento, o

- Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.

RELACIÓN ENTRE EL RESPONSABLE Y EL ENCARGADO

La relación entre el responsable y el encargado deberá establecerse en cláusulas contractuales u otro instrumento jurídico que decida el responsable, en el que se acredite su existencia, alcance y contenido.

El encargado tendrá las siguientes obligaciones:

- Tratar únicamente los datos personales conforme a las instrucciones del responsable.

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

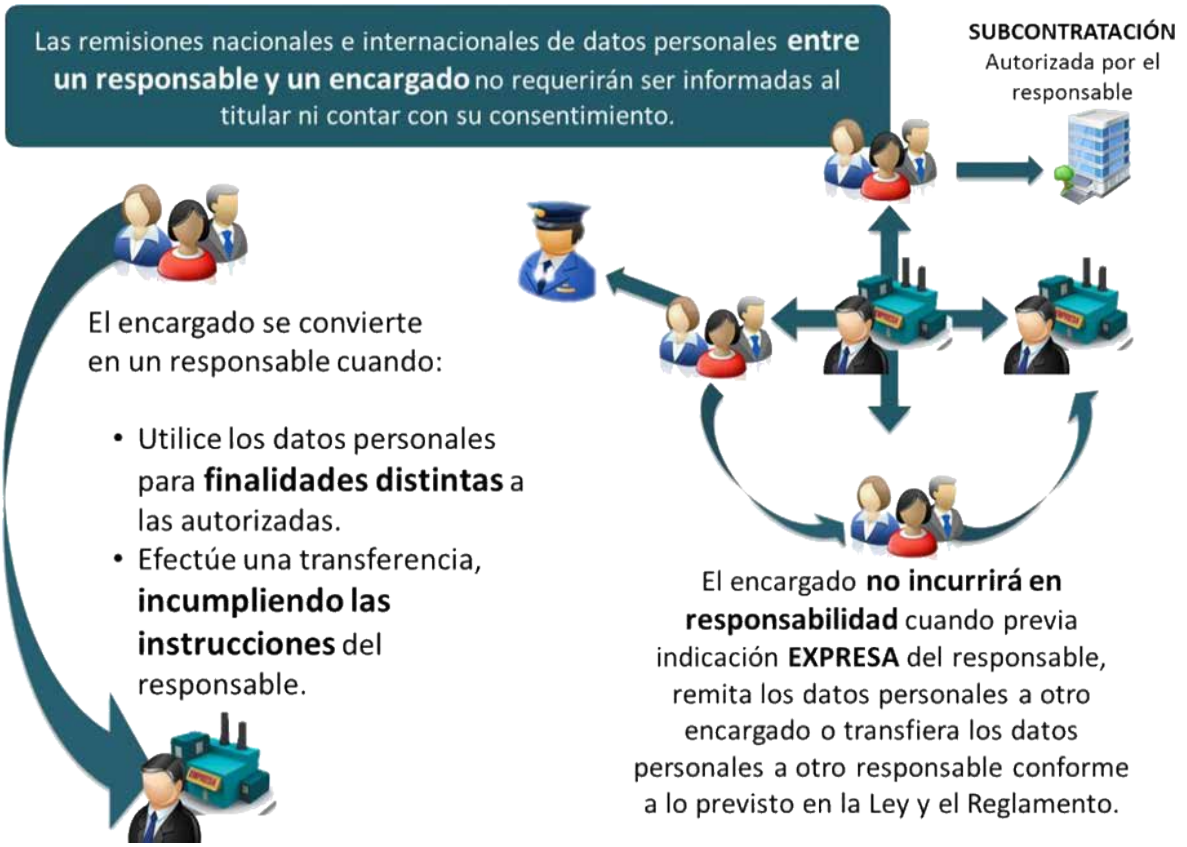
- Implementar las medidas de seguridad conforme a la Ley, el Reglamento y las demás disposiciones aplicables.

- Guardar confidencialidad respecto de los datos personales tratados.

- Suprimir los datos personales objeto de tratamiento, una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre que no exista una previsión legal que exija su conservación.

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

Cabe advertir que en el Reglamento, se precisa además lo relativo a la figura del encargado, las condiciones en que se realizarán remisiones entre un responsable y un encargado, así como lo relativo a la subcontratación de servicios.



SOBRE LAS MEDIDAS DE SEGURIDAD

El Reglamento establece que el responsable y, en su caso, el encargado deberán establecer y mantener las medidas de seguridad administrativas, físicas y, en su caso, técnicas para la protección de los datos personales, con independencia del sistema de tratamiento.

Se entenderá por medidas de seguridad: el control o grupo de controles de seguridad para proteger los datos personales.

Para garantizar el establecimiento y mantenimiento efectivo de dichas medidas, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien contratar a una persona física o moral para tal fin.

El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, tomando en consideración los siguientes factores:

- El riesgo inherente por tipo de dato personal.
- La sensibilidad de los datos personales tratados.
- El desarrollo tecnológico.
- Las posibles consecuencias de una vulneración para los titulares.

DE LOS DERECHOS DE LOS TITULARES DE DATOS PERSONALES

Capítulo III y IV

Artículos **22 al 27 -** De los derechos ARCO
28 al 35 - Del ejercicio de los derechos ARCO

En este capítulo revisaremos a qué se refieren los derechos de acceso, rectificación, cancelación y oposición, denominados por sus siglas como: derechos ARCO, así como los requisitos para su ejercicio, tiempos de respuesta y los casos en que podrá ser negado su ejercicio.

La Ley establece que cualquier titular o su representante legal, podrá ejercer los derechos de acceso, rectificación, cancelación y oposición: ARCO.

Precisa que el ejercicio de alguno de ellos no es requisito ni impide el desarrollo de cualquiera de los otros.

Para ello, enfatiza que los datos personales deben ser resguardados de tal manera que permitan al titular, el ejercicio de estos derechos sin dilación.

Todos los titulares o en su caso, el representante legal podrá ejercer los derechos de:

Acceso — A los DP , al aviso y las generalidades del tratamiento

Rectificación — DP inexactos o incompletos.

Cancelación — Cuando no se cumplan los **principios y deberes** (finalidad, proporcionalidad, calidad...)

Oposición — Impedir tratamiento por razones legítimas de manera justificada. ***Listados de exclusión** (gratuito y constancia de inscripción)*

El ejercicio de cualquiera de ellos, NO es requisito previo ni impide el ejercicio de otro.

DE LOS DERECHOS ARCO

La incorporación de estos derechos permite al titular tener la posibilidad de:

Acceso

- Acceder a sus datos personales en poder del responsable.
- Conocer el Aviso de Privacidad al que está sujeto el tratamiento de sus datos.

Rectificación

- Rectificarlos cuando sean inexactos o incompletos.
- La solicitud de rectificación deberá indicar a qué datos personales se refiere, así como la corrección que haya de realizarse y deberá ir acompañada de la documentación que ampare la procedencia de lo solicitado.

Cancelación

- También, en todo momento, el titular tendrá derecho a que se supriman sus datos personales.
- Sobre este derecho, el Reglamento señala que en todo momento el titular podrá solicitar al responsable, la cancelación de los datos personales cuando considere que los mismos no están siendo tratados conforme a los principios y deberes que establece la Ley y dicho Reglamento.

Por ejemplo, cuando los datos tratados resulten inadecuados, innecesarios o irrelevantes con relación a la finalidad para la cual fueron recabados (principio de proporcionalidad) o estén siendo utilizados para fines no autorizados o incompatibles con la finalidad que justificó su tratamiento (principio de finalidad).

Bloqueo

La cancelación dará paso al denominado periodo de bloqueo, después del cual se procederá a la supresión del dato.

El responsable podrá conservar los datos sólo para efectos de atender las responsabilidades nacidas del tratamiento.

El periodo en que los datos permanecerán bloqueados será el equivalente al plazo en que prescriban las acciones derivadas de la relación jurídica con fundamento en la cual se tratan los datos y en términos de la Ley aplicable en la materia.

Cancelado el dato o datos, se comunicará al titular de la supresión.

Cuando los datos personales hubiesen sido transmitidos con anterioridad a la fecha de rectificación o cancelación, y sigan siendo tratados por terceros, el responsable deberá hacer del conocimiento de dicho tercero, la solicitud de rectificación o cancelación, para que proceda a efectuarla también.

El responsable no estará obligado a cancelar los datos personales cuando:

- Se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento.
- Deban ser tratados por disposición legal.
- Obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas.
- Sean necesarios para:
  - Proteger los intereses jurídicamente tutelados del titular.
  - Realizar una acción en función del interés público.
  - Cumplir con una obligación legal adquirida por el titular.
- Sean objeto de tratamiento para la prevención, para diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto.

Oposición

El titular tendrá en todo momento y por causa legítima, el derecho a oponerse al tratamiento de sus datos.

De ser procedente la solicitud de oposición, el responsable no podrá tratar los datos relativos al titular.

Al respecto, el Reglamento señala que el titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo cuando:

- Exista causa legítima y su situación específica así lo requiera, lo cual debe justificar que aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un perjuicio al titular.
- Requiera manifestar su oposición para el tratamiento de sus datos personales a fin de que no se lleve a cabo el tratamiento para fines específicos.

DEL EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN

El titular o su representante podrán solicitar al responsable en cualquier momento el acceso, rectificación, cancelación u oposición, respecto de los datos personales que le conciernen.
Para lo cual, el responsable deberá:

Designar a una persona o departamento de datos personales, que estará a cargo de dar trámite a las solicitudes de los particulares y de fomentar la protección de datos personales al interior de la organización.

Para este fin, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y la Secretaría de Economía, desarrollaron las Recomendaciones para la designación de la persona o departamento de datos personales, que se pueden consultar en la página del INAI.[19]

Requisitos que deberá contener la solicitud:

- Nombre del titular, domicilio u otro medio para comunicarle la respuesta.
- Documentos que acrediten la identidad del titular, o en su caso, la identidad y la representación legal de quien promueva en su nombre.
- Descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO.
- Cualquier otro elemento o documento que facilite la localización de los datos personales.

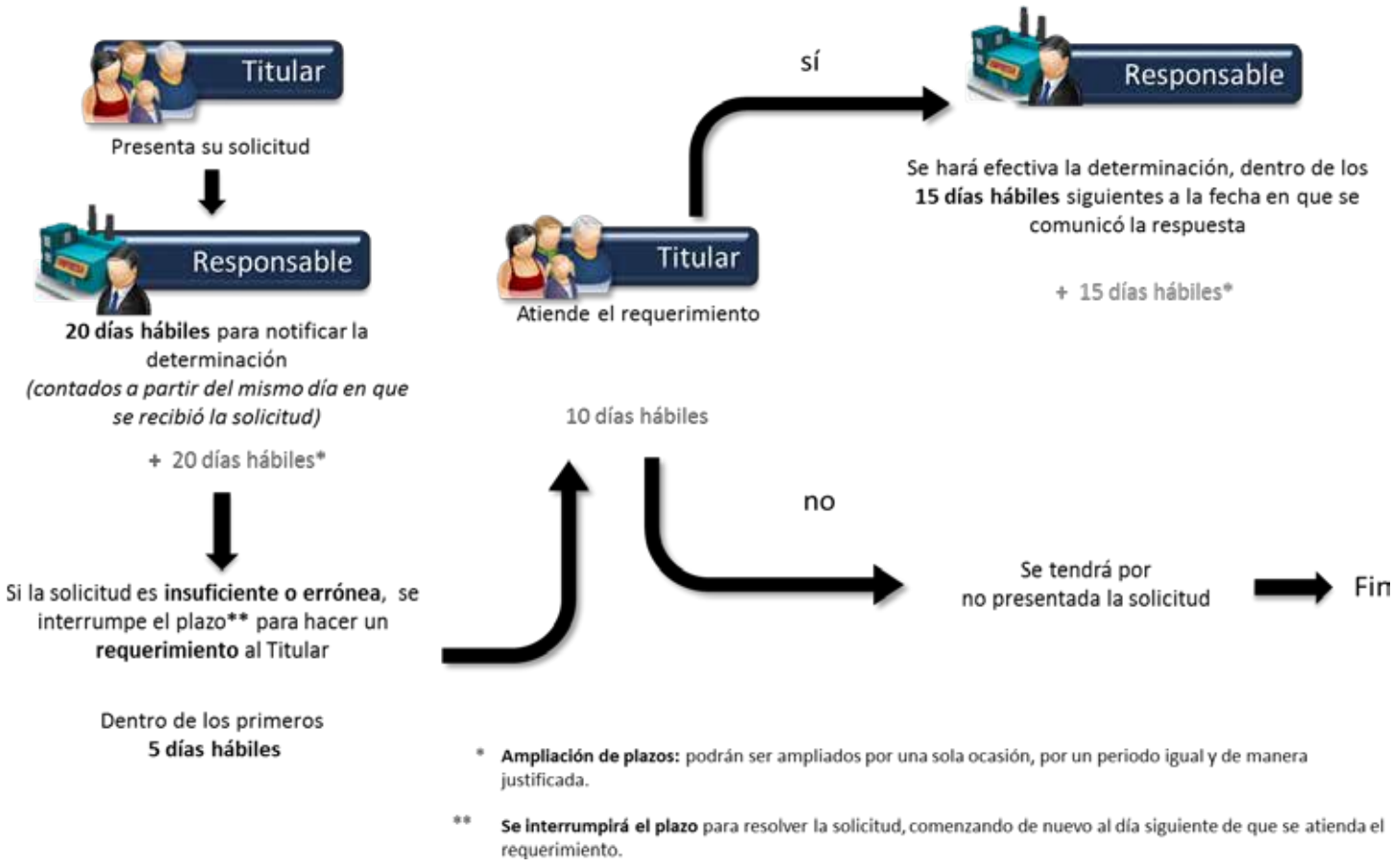
Requisitos en caso de Rectificación:

- Señalar las modificaciones a realizarse.
- Aportar la documentación que dé sustento a su petición.

La obligación de acceso a la información se da por cumplida cuando:

- Se pongan a disposición del titular los datos personales.
- Se expidan las copias simples, documentos electrónicos o cualquier otro medio que defina el responsable en el Aviso de Privacidad.
- Si se presenta una solicitud de acceso a datos ante una persona que resulta no ser el responsable de atenderla, sólo tendrá que indicarle esta situación al titular por cualquiera de los medios señalados, para que se tenga por cumplida la solicitud.

18 INAI, sección “Datos Personales”, disponible en: http://inicio.inai.org.mx/DocumentosdeInteres/privacidadresponsable.pdf, consultado el 22 de noviembre de 2016.



Costos

El ejercicio de los derechos ARCO será gratuito, previa acreditación de su titular.

El titular sólo cubrirá: los gastos justificados de envío y los costos de reproducción (copias u otros formatos).

Si la persona reitera su solicitud en un periodo menor de doce meses, los costos no serán mayores a 3 días de Salario Mínimo General Vigente en el D.F. (SMGVDF), a menos que existan modificaciones sustanciales al Aviso de Privacidad que generen nuevas consultas.

Medios para el ejercicio de los derechos

El Reglamento establece que para el ejercicio de los derechos ARCO, el titular o su representante podrán presentar su solicitud ante el responsable conforme a los medios establecidos en el Aviso de Privacidad. Para tal fin, el responsable pondrá a disposición del titular, medios remotos o locales de comunicación electrónica u otros que considere pertinentes.

Asimismo podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el Aviso de Privacidad.

El responsable podrá negar el acceso a los datos personales, realizar la rectificación, cancelación o conceder la oposición al tratamiento de los mismos en los siguientes casos:

- Cuando el solicitante no sea el titular de los datos personales o el representante legal no esté debidamente acreditado.
- Cuando los datos personales no se encuentren en la base de datos del responsable.
- Cuando se lesionen derechos de un tercero.
- Cuando exista un impedimento legal o la resolución de una autoridad competente.
- Cuando la rectificación, cancelación u oposición hubiese sido previamente realizada.

Es muy importante señalar que esta negativa puede ser parcial, y que el responsable deberá informar el motivo de su decisión al titular.

Si el titular lo considera, podrá presentar una solicitud de protección de derechos por la respuesta recibida o por la falta de respuesta.

TRANSFERENCIA A TERCEROS NACIONALES O EXTRANJEROS DISTINTOS DEL ENCARGADO

Capítulo V

Artículos 36 al 37

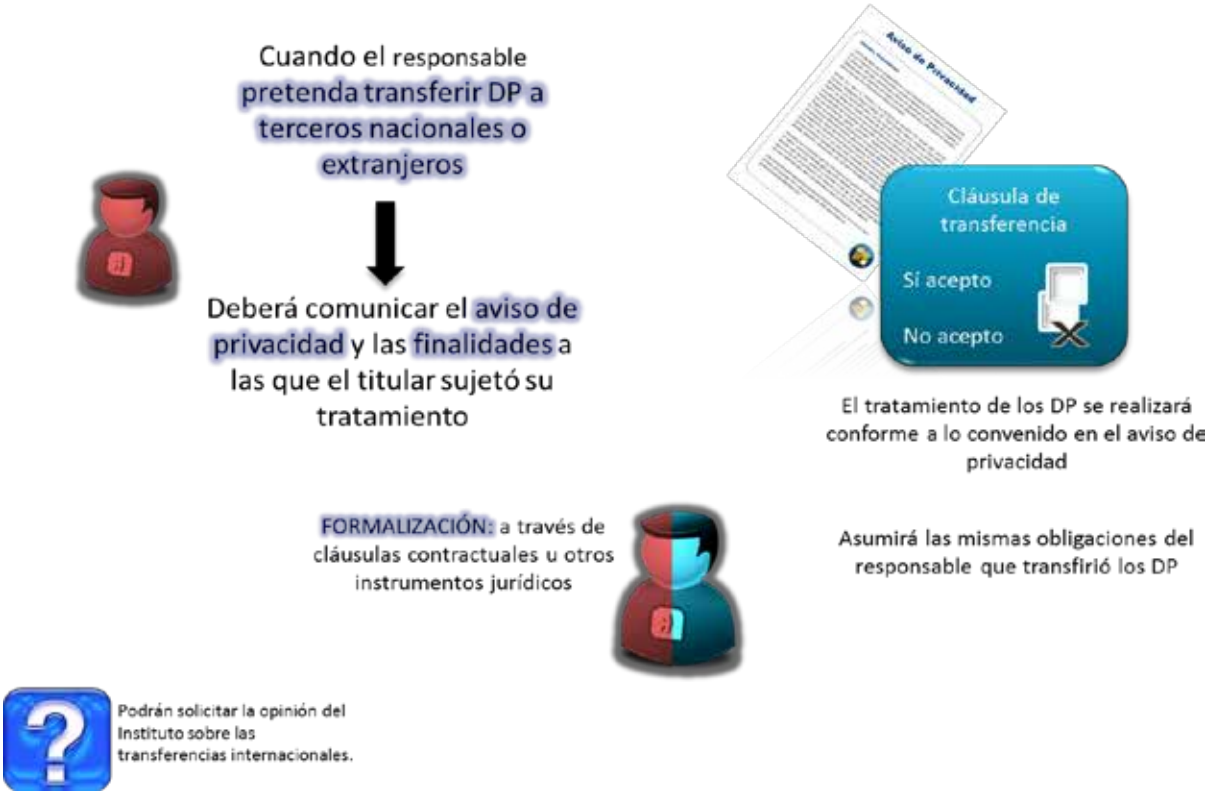
La Ley establece que cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, les deberá hacer saber el contenido del Aviso de Privacidad y las finalidades a las que el titular sujetó su tratamiento.

El tratamiento de los datos deberá realizarse conforme a lo convenido en el Aviso de Privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.

El Reglamento señala que la transferencia:

- Implica la comunicación de datos personales dentro o fuera del territorio nacional, realizada a persona distinta del titular, del responsable o del encargado.

- Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en el artículo 37 de la Ley, y le deberá ser informada mediante el Aviso de Privacidad y limitarse a la finalidad que la justifique.



Recordemos que el término de **remisión** se refiere a la comunicación de datos personales entre el responsable y el encargado, dentro o fuera del territorio mexicano, que tendrá por objeto la realización de un tratamiento por el **encargado** a cuenta del responsable.

Transferencias nacionales o internacionales sin el consentimiento del titular

Las transferencias nacionales o internacionales de datos personales podrán llevarse a cabo sin el consentimiento del titular, cuando se presente alguno de los siguientes supuestos:

Cuando la transferencia:

- Esté prevista en una Ley o Tratado en los que México sea parte.
- Sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios.
- Sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas.
- Sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero.
- Sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia.
- Sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- Sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.

DE LAS AUTORIDADES

Capítulo VI

Artículos 38 al 44

En este apartado se exponen las atribuciones del órgano garante de la protección de datos personales, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y de la Secretaría de Economía como dependencia sectorial a cargo de la política pública en materia de comercio, así como de las dependencias públicas que, en su caso, emitan regulación específica en la materia.

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

De conformidad con lo dispuesto en el artículo 6º, apartado A, fracción VIII, de la Constitución Política de los Estados Unidos Mexicanos, el Instituto es un organismo constitucionalmente autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados, cuyo funcionamiento se rige bajo los principios de certeza, legalidad, independencia, imparcialidad, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad.

Por lo que se refiere a la LFPDPPP, el Instituto tendrá por objeto:

- Difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana.
- Promover el ejercicio del derecho a la protección de datos personales.
- Vigilar la debida observancia de las disposiciones previstas en la Ley y las que de ella se deriven, particularmente las relativas al cumplimiento de obligaciones por parte de los sujetos regulados.

Tendrá las siguientes atribuciones:

- Vigilar y verificar el cumplimiento de las disposiciones contenidas en la Ley, en el ámbito de su competencia, con las excepciones previstas por la legislación.
- Interpretar la LFPDPPP en el ámbito administrativo.
- Proporcionar apoyo técnico a los responsables que lo soliciten, para el cumplimiento de las obligaciones establecidas en la Ley.
- Emitir los criterios y recomendaciones necesarias para el funcionamiento y operación de la Ley.

- Divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información, en atención a la naturaleza de los datos, las finalidades del tratamiento, las capacidades técnicas y económicas del responsable.

- Conocer y resolver los procedimientos de protección de derechos y de verificación e imponer las sanciones correspondientes.

- Cooperar con otras autoridades de supervisión y organismos nacionales e internacionales, a efecto de coadyuvar en materia de protección de datos.

- Rendir al Congreso de la Unión un informe anual sobre sus actividades.

- Acudir a foros internacionales en la materia.

- Elaborar estudios de impacto sobre la privacidad previos a la puesta en práctica de una nueva modalidad de tratamiento de datos personales o a la realización de modificaciones sustanciales a tratamientos ya existentes.

- Desarrollar, fomentar y difundir análisis, estudios e investigaciones en materia de protección de datos personales y brindar capacitación a los sujetos regulados.

- Las demás que le confieran esta ley y demás ordenamientos aplicables.

DE LAS AUTORIDADES REGULADORAS

Dependencias

La LFPDPPP sólo será el marco normativo que las dependencias deberán observar en el ámbito de sus propias atribuciones, para la emisión de la regulación que corresponda. En virtud de que la Ley “es una ley de mínimos”, que requiere ser complementada con una regulación sectorial que prevea condiciones a tratamientos específicos que por las características de cada sector así lo requieran.

Sobre este aspecto, el Reglamento define que cuando la dependencia competente, en atención a las necesidades que advierta sobre su sector, determine la necesidad de normar el tratamiento de datos personales en posesión de los particulares, podrá en el ámbito de su competencia, emitir o modificar la regulación específica, en coadyuvancia con el Instituto.

Asimismo, cuando el Instituto derivado del ejercicio de sus atribuciones advierta la necesidad de emitir o modificar regulación específica para normar el tratamiento de datos personales en un sector o actividad determinada, podrá proponer a la dependencia competente la elaboración de un anteproyecto.

Para lo anterior, la dependencia de que se trate y el Instituto establecerán los mecanismos de coordinación correspondientes.

Secretaría de Economía

La Secretaría de Economía tendrá como función:

- Difundir el conocimiento de las obligaciones en torno a la protección de datos personales entre la iniciativa privada nacional e internacional con actividad comercial en territorio mexicano.

- Promover las mejores prácticas comerciales en torno a la protección de los datos personales como insumo de la economía digital, y el desarrollo económico nacional en su conjunto.

En lo relativo a las bases de datos de comercio, la regulación que emita la Secretaría, sólo será aplicable a aquellas bases de datos automatizadas o en proceso de automatización.

Atribuciones de la Secretaría de Economía

- Difundir el conocimiento respecto a la protección de datos personales en el ámbito comercial.

- Fomentar las buenas prácticas comerciales en materia de protección de datos personales.

- Emitir los lineamientos correspondientes para el contenido y alcances de los avisos de privacidad en coadyuvancia con el Instituto.

- Emitir, en el ámbito de su competencia, las disposiciones administrativas de carácter general para el desarrollo de regulación específica por parte de las dependencias públicas respectivas, en coadyuvancia con el Instituto.

- Fijar los parámetros necesarios para el correcto desarrollo de los mecanismos y medidas de autorregulación referidas en la Ley, incluida la promoción de Normas Mexicanas o Normas Oficiales Mexicanas, en coadyuvancia con el Instituto.

- Llevar a cabo los registros de consumidores en materia de datos personales y verificar su funcionamiento.

- Celebrar convenios con cámaras de comercio, asociaciones y organismos empresariales en lo general, en materia de protección de datos personales.

- Diseñar e instrumentar políticas y coordinar la elaboración de estudios para la modernización y operación eficiente del comercio electrónico, así como para promover el desarrollo de la economía digital y las tecnologías de la información en materia de protección de datos personales.

- Acudir a foros comerciales nacionales e internacionales en materia de protección de datos personales, o en aquellos eventos de naturaleza comercial.

– Apoyar la realización de eventos, que contribuyan a la difusión de la protección de los datos personales.

LA AUTORREGULACIÓN

En lo relativo a la Autorregulación, la LFPDPPP es una "ley de mínimos", que tendrá que complementarse además de lo señalado sobre la regulación sectorial por esquemas de autorregulación; establece que las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales nacionales o extranjeras, esquemas de autorregulación vinculante en la materia, que complementen lo dispuesto por la Ley, el Reglamento y las disposiciones que se emitan por las dependencias en el ámbito de sus atribuciones.

Para mayor profundidad en el conocimiento del tema, le proponemos, consultar el Manual del Participante del curso de Autorregulación, de distribución y consulta gratuita. Así como el curso en línea: Autorregulación en México en Materia de Datos Personales, disponible en el Campus Iniciativa Privada del Centro Virtual de Formación INAI (CEVINAI).

PROCEDIMIENTO DE PROTECCIÓN DE DERECHOS

Capítulo VII

Artículos 45 al 58

En caso de que el titular de los datos considere que el ejercicio de sus derechos ARCO, no ha sido satisfecho plenamente por el responsable, la LFPDPPP establece un procedimiento de tutela o protección de derechos que debe presentarse ante el INAI, denominado:

Procedimiento de protección de derechos, mismo que procederá ante las inconformidades derivadas del ejercicio de los derechos ARCO.

MOTIVOS POR LOS QUE PUEDE PRESENTARSE UNA SOLICITUD DE PROTECCIÓN DE DERECHOS

De acuerdo con la Ley y su Reglamento, el titular puede interponer una solicitud de protección de derechos, cuando:

– No entregue al titular los datos personales solicitados o lo haga en un formato incomprensible.
– Se niegue a efectuar modificaciones o correcciones a los datos personales.
– No otorgue acceso a los datos personales solicitados o lo haga en un formato incomprensible.
– Se niegue a cancelar los datos personales.
– Persista en el tratamiento a pesar de haber procedido la solicitud de oposición, o bien, se niegue a atender la solicitud de oposición.

El titular:

- No esté conforme con la información entregada por considerar que es incompleta o no corresponde a la información requerida.
- No haya recibido respuesta por parte del responsable.
- No esté conforme con el costo o modalidad de la reproducción.

Que también podrá presentarse por otras causas que, juicio del Instituto, sean procedentes conforme a la Ley o el Reglamento.

Plazos para la presentación de una solicitud de protección de derechos:

- Por inconformidad con la respuesta recibida, el titular podrá presentar su solicitud de protección de derechos, dentro de los 15 días siguientes a la fecha en que le fue comunicada la respuesta.
- Cuando el titular no haya recibido respuesta a su solicitud para el ejercicio de los derechos ARCO, podrá presentar su solicitud de protección de derechos, a partir de que haya vencido el plazo previsto para que el responsable emitiera dicha respuesta.

Medios para presentar la solicitud de protección de derechos

La solicitud podrá interponerse:

- Por escrito libre o a través de los formatos que para tal efecto se aprueben.
- Por el sistema electrónico que al efecto proporcione el Instituto.

Requisitos

Es indispensable que la solicitud cuente con los siguientes datos:

- Nombre del titular o de su representante legal, así como el del tercero interesado, si lo hay.
- Nombre del responsable ante el cual se presentó la solicitud de ARCO.
- Domicilio para oír y recibir notificaciones.
- Fecha en que se le dió a conocer la respuesta del responsable.

- Actos que motivan la solicitud de protección de derechos.

- Demás elementos que se considere procedente hacer del conocimiento del Instituto.

A la solicitud de protección de derechos, deberá anexarse la solicitud y la respuesta que se recurre o, en su caso, los datos que permitan su identificación. Y en el caso de falta de respuesta sólo será necesario presentar la solicitud.

La Ley establece que el titular deberá expresar claramente el contenido de su reclamación y los preceptos de dicha norma que se consideran vulnerados.

El Reglamento señala que el titular deberá adjuntar a la solicitud de protección de derechos los siguientes documentos:

- Copia de la solicitud del ejercicio de derechos que corresponda, y en su caso, copia de los documentos anexos para cada una de las partes.

- El documento que acredite que actúa por su propio derecho o en representación del titular.

- En su caso, el documento en que conste la respuesta del responsable.

- En el supuesto en que impugne la falta de respuesta del responsable, deberá anexar una copia en la que obre el acuse o constancia de recepción de la solicitud del ejercicio de derechos por parte del responsable.

- Las pruebas documentales que ofrece para demostrar sus afirmaciones.

- El documento en el que señale las demás pruebas que ofrezca, tales como:

    - La documental pública o privada.
    - La inspección, siempre y cuando se realice a través de la autoridad competente.
    - La presuncional, en su doble aspecto, legal y humana.
    - La pericial o testimonial, que para ser válidas, deberán precisar los hechos sobre los que deban versar, señalando los nombres y domicilios del perito o de los testigos, exhibiéndose el cuestionario o interrogatorio respectivo en preparación de las mismas.
    - Las fotografías, páginas electrónicas, escritos y demás elementos aportados por la ciencia y tecnología.

- Cualquier otro documento que considere procedente someter a juicio del Instituto.

En los casos en que el titular no pudiera acreditar que acudió con el responsable, ya sea porque éste se hubiere negado a recibir la solicitud de ejercicio de derechos ARCO o a emitir el acuse de recibido, el Reglamento señala, que el titular deberá hacerlo del conocimiento del Instituto mediante escrito, el cual dará vista al responsable para que manifieste lo que a su derecho convenga, a fin de garantizar al titular el ejercicio de sus derechos ARCO.

Asimismo, señala que cuando la solicitud de protección se presente por medios que no sean electrónicos, se deberá acompañar de las copias de traslado suficientes.

PROCEDIMIENTOS A SEGUIR

A fin de que la solicitud de protección de derechos sea atendida:

- El titular de los datos o su representante legal presenta su solicitud de protección de derechos ante el INAI.

- Si al recibir una solicitud de protección de derechos, ésta no satisface alguno de los requisitos y el Instituto no cuenta con elementos para subsanarlo, se prevendrá al solicitante, por una sola ocasión, para que subsane las omisiones en un plazo no mayor a 5 días, teniendo por no presentada la solicitud si no se recibe respuesta alguna por parte del solicitante. La prevención tendrá el efecto de interrumpir el plazo que tiene el Instituto para resolver el recurso.

- Una vez que la solicitud de protección de derechos reúne todos los requisitos, se realiza la notificación al responsable.

- En un plazo de 15 días, el responsable deberá: emitir respuesta, ofrecer las pruebas que estime pertinentes y manifestar por escrito lo que a su derecho convenga.

PROCEDIMIENTO CUANDO UNA SOLICITUD DE PROTECCIÓN DE DERECHOS ES PROCEDENTE

Realizado lo anterior, el Instituto:

- Admitirá las pruebas que estime pertinentes y procederá a su desahogo.

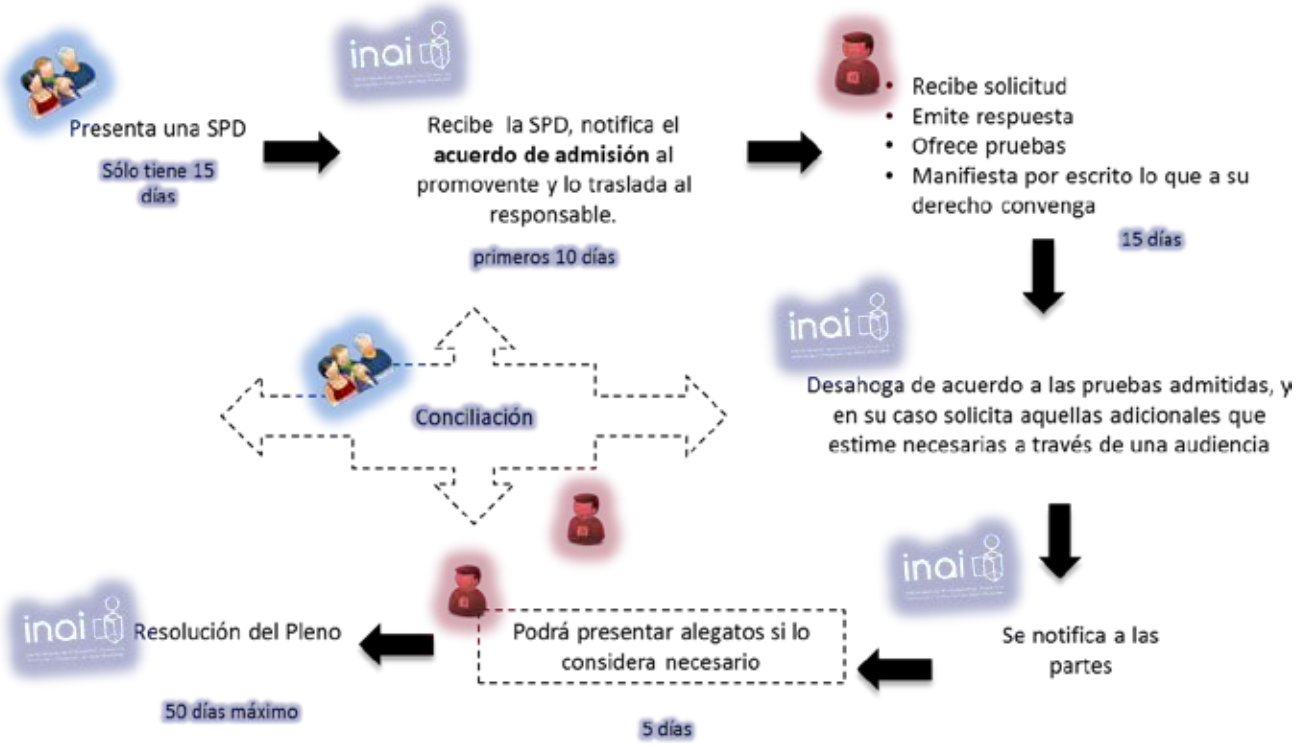
- Podrá solicitar al responsable las demás pruebas que estime necesarias.

- Concluido el desahogo de las pruebas, notificará al responsable el derecho que tiene para que, de considerarlo necesario, presente sus alegatos dentro de los 5 días siguientes a su notificación.

- Para el debido desahogo del procedimiento, el Instituto resolverá sobre la solicitud de protección de derechos formulada, una vez analizadas las pruebas y demás elementos de convicción que estime pertinentes, como pueden serlo aquéllos que deriven de la o las audiencias que se celebren con las partes.

- Finalmente el Instituto emitirá su resolución, teniendo para ello un plazo máximo de 50 días, contados a partir de la fecha de la presentación de la solicitud de protección.

- Cuando exista causa justificada, el Pleno del INAI podrá ampliar este plazo, por una vez, y hasta por un periodo igual.



Prevención

Si la solicitud de protección de derechos no satisface alguno de los requisitos citados, y el Instituto no cuenta con elementos para subsanarlo:

- Prevendrá al titular, por una sola ocasión, dentro de los 20 días siguientes a que presentó su solicitud de protección de derechos, para que subsane las omisiones.

- El titular tendrá 5 días para subsanar las omisiones.

- Transcurrido este plazo, sin que el titular desahogue la prevención, la solicitud de protección de derechos se tendrá por no presentada.

La prevención tendrá como efecto la interrupción del plazo que tiene el Instituto para resolver la solicitud de protección de derechos.

Suplencia de la deficiencia de la queja

El Instituto suplirá las deficiencias de la queja en los casos que así se requiera, siempre y cuando:

- No se altere el contenido original de la solicitud presentada ante el responsable.
- No se modifiquen los hechos o peticiones expuestos en dicha solicitud.
- No se modifiquen los hechos o peticiones expuestos en la solicitud de protección de derechos.

Consideraciones sobre el procedimiento por falta de respuesta

Cuando la solicitud de protección de derechos se presente ante la falta de respuesta por parte del responsable, a una solicitud para el ejercicio de los derechos ARCO:

- Bastará que el titular acompañe a su solicitud el documento que pruebe la fecha en que presentó la solicitud para el ejercicio de los derechos ARCO.
- El Instituto dará vista al citado responsable para que en un plazo no mayor a 10 días:

  a) Acredite haber respondido en tiempo y forma la solicitud.

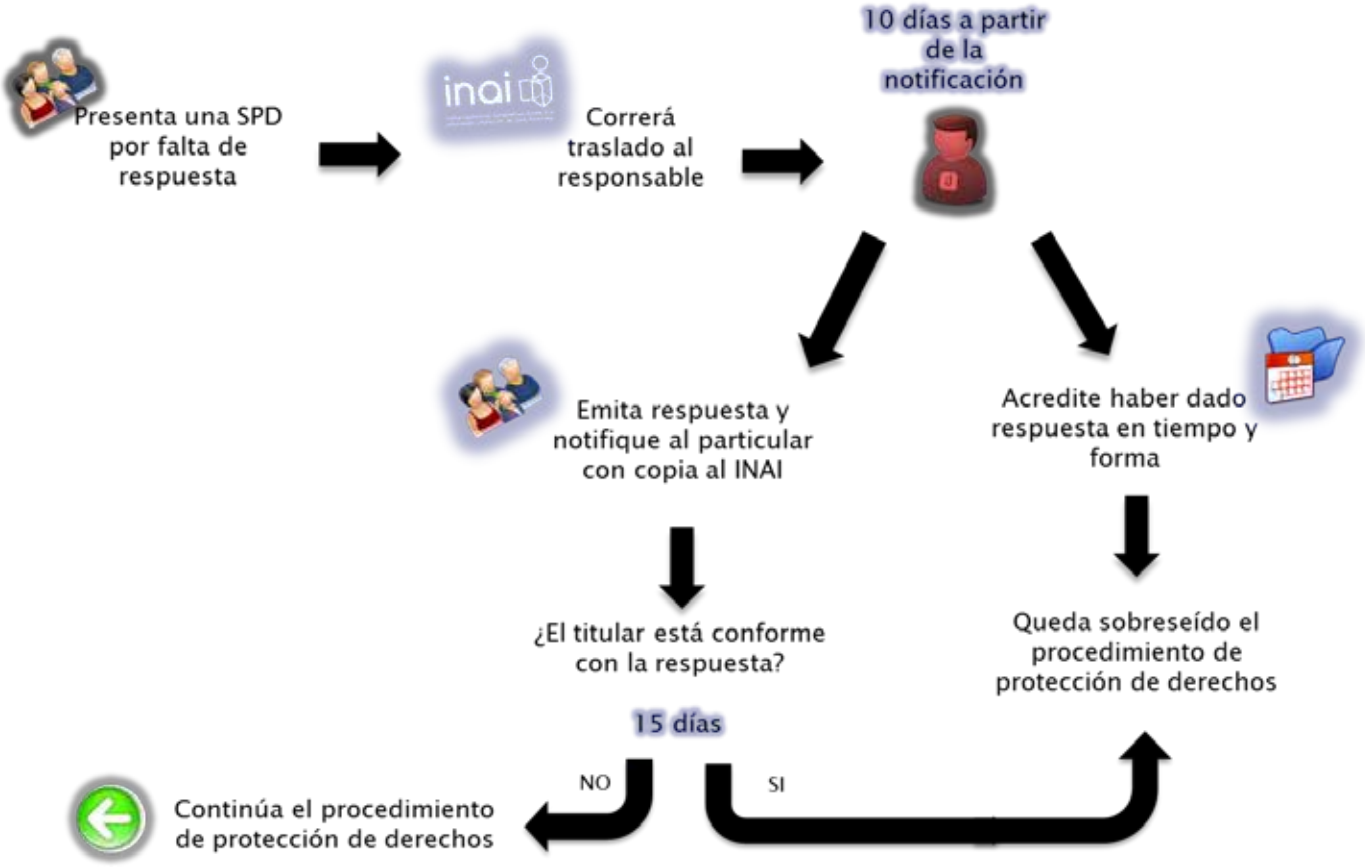
  - En este caso, la solicitud de protección de derechos se considerará improcedente y el Instituto deberá sobreseerlo.

  b) Dé respuesta a la misma.

  - En este segundo caso, el Instituto emitirá su resolución con base en el contenido de la solicitud original y la respuesta que haya dado el responsable.
  - Si la resolución del Instituto a que se refiere el punto anterior, determina la procedencia de la solicitud, el responsable:
    - Procederá a su cumplimiento, **sin costo alguno para el titular**.
    - Cubrirá (el responsable) todos los costos generados por la reproducción correspondiente.

El Reglamento establece los supuestos o condiciones en que, ante la presentación de una solicitud de protección de derechos por falta de respuesta, procederá el sobreseimiento o por el contrario se deberá dar continuidad a dicho procedimiento de protección.

Procedimiento de protección de derechos por falta de respuesta



RESOLUCIONES DEL INSTITUTO

El Instituto tendrá un plazo máximo de 50 días para emitir la resolución a la solicitud de protección de derechos, mismo que por causa justificada podrá ampliarse por una vez y hasta por un periodo igual.

Las resoluciones del Instituto podrán:

- Sobreseer o desechar la solicitud de protección de derechos por improcedente.
- Confirmar, revocar o modificar la respuesta del responsable.

Desechar

La solicitud de protección de derechos será desechada por improcedente cuando:

- El Instituto no sea competente.
- El Instituto haya conocido anteriormente de la solicitud de protección de derechos contra el mismo acto y resuelto en definitiva respecto del mismo recurrente.
- Se esté tramitando, ante los tribunales competentes, algún recurso o medio de defensa interpuesto por el titular que pueda tener por efecto modificar o revocar el acto respectivo.
- Se trate de una solicitud de protección de derechos ofensiva o irracional.
- Sea extemporánea.

Sobreseer

Una solicitud será sobreseída si las causas que la originaron ya no subsisten, lo cual de acuerdo con la Ley sucederá cuando:

- El titular fallezca.
- El titular se desista de manera expresa de continuar con el procedimiento.
- Admitida la solicitud de protección de derechos, se presente una causal de improcedencia, de las que se revisaron en el punto anterior.
- Por cualquier motivo quede sin materia la misma.

Confirmar, revocar o modificar

- El Instituto podrá confirmar la respuesta que haya emitido el responsable.
- Asimismo, podrá revocarla o modificarla.

En el caso de que la resolución de protección de derechos sea favorable para el titular de los datos:

- El Instituto requerirá al responsable para que en un plazo de 10 días, siguientes a la notificación o cuando así se justifique, uno mayor que fije la propia resolución, se haga efectivo el ejercicio de los derechos objeto de protección.
- El responsable deberá informar de dicho cumplimiento al INAI, dentro de los siguientes 10 días.

Es importante señalar que:

- Contra las resoluciones del Instituto, los particulares podrán promover el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.

- Todas las resoluciones del Instituto serán susceptibles de difundirse públicamente en versiones públicas, eliminando aquellas referencias al titular de los datos que lo identifiquen o lo hagan identificable.

- Los titulares que consideren que han sufrido un daño o lesión en sus bienes o derechos por parte del responsable o el encargado, podrán ejercer los derechos que estimen pertinentes para efectos de la indemnización que proceda, en términos de las disposiciones legales correspondientes.

LA CONCILIACIÓN

El Instituto podrá promover la conciliación entre el titular de los datos y el responsable, en cualquier etapa del procedimiento de protección de derechos:

- De llegarse a un acuerdo de conciliación entre ambos, éste se hará constar por escrito y tendrá efectos vinculantes.

- La solicitud de protección de derechos quedará sin materia y el Instituto verificará el cumplimiento del acuerdo respectivo.

El reglamento de la Ley, establece que:

El Instituto

- En el acuerdo de admisión de la solicitud de protección de derechos, el Instituto requerirá a las partes que manifiesten su voluntad de conciliar, en un plazo no mayor a diez días contados a partir de la notificación del acuerdo referido.

- El acuerdo contendrá un resumen de la solicitud de protección de derechos y de la respuesta del responsable, si la hubiere, señalando los puntos en común y los de controversia.

La conciliación podrá celebrarse:

- Presencialmente.

- Por medios remotos o locales de comunicación electrónica.

- Por cualquier otro medio que determine el Instituto.

En cualquier caso, la conciliación habrá de hacerse constar por el medio que permita acreditar su existencia.

Una vez que las partes han aceptado la posibilidad de conciliar, el Instituto:

- Señalará el lugar o medio, día y hora para la celebración de una audiencia de conciliación.

- La audiencia deberá realizarse dentro de los veinte días siguientes en que el Instituto haya recibido la manifestación de la voluntad de conciliar de las partes, en la que se procurará avenir los intereses entre el titular y el responsable.

El conciliador

- Podrá, en todo momento en la etapa de conciliación, requerir a las partes que presenten, en un plazo máximo de cinco días, los elementos de convicción que estimen necesarios para la conciliación.

- Podrá suspender cuando lo estime pertinente o a instancia de ambas partes la audiencia de conciliación hasta en dos ocasiones. En caso de que se suspenda la audiencia, el conciliador señalará día y hora para su reanudación.

- De toda audiencia de conciliación se levantará el acta respectiva, en la que conste el resultado de la misma. En caso de que el responsable o el titular o sus respectivos representantes no firmen el acta, ello no afectará su validez, debiéndose hacer constar dicha negativa.

Las partes

- Si alguna de las partes no acude a la audiencia y justifica su ausencia en un plazo de tres días, será convocada a una segunda audiencia de conciliación; en caso de que no acuda a esta última, se continuará con el procedimiento de protección. Asimismo, si alguna de las partes no acude a la audiencia sin justificación alguna, se continuará con el procedimiento referido.

Si no hay un acuerdo

- De no existir acuerdo en la audiencia de conciliación, se continuará con el procedimiento de protección de derechos.

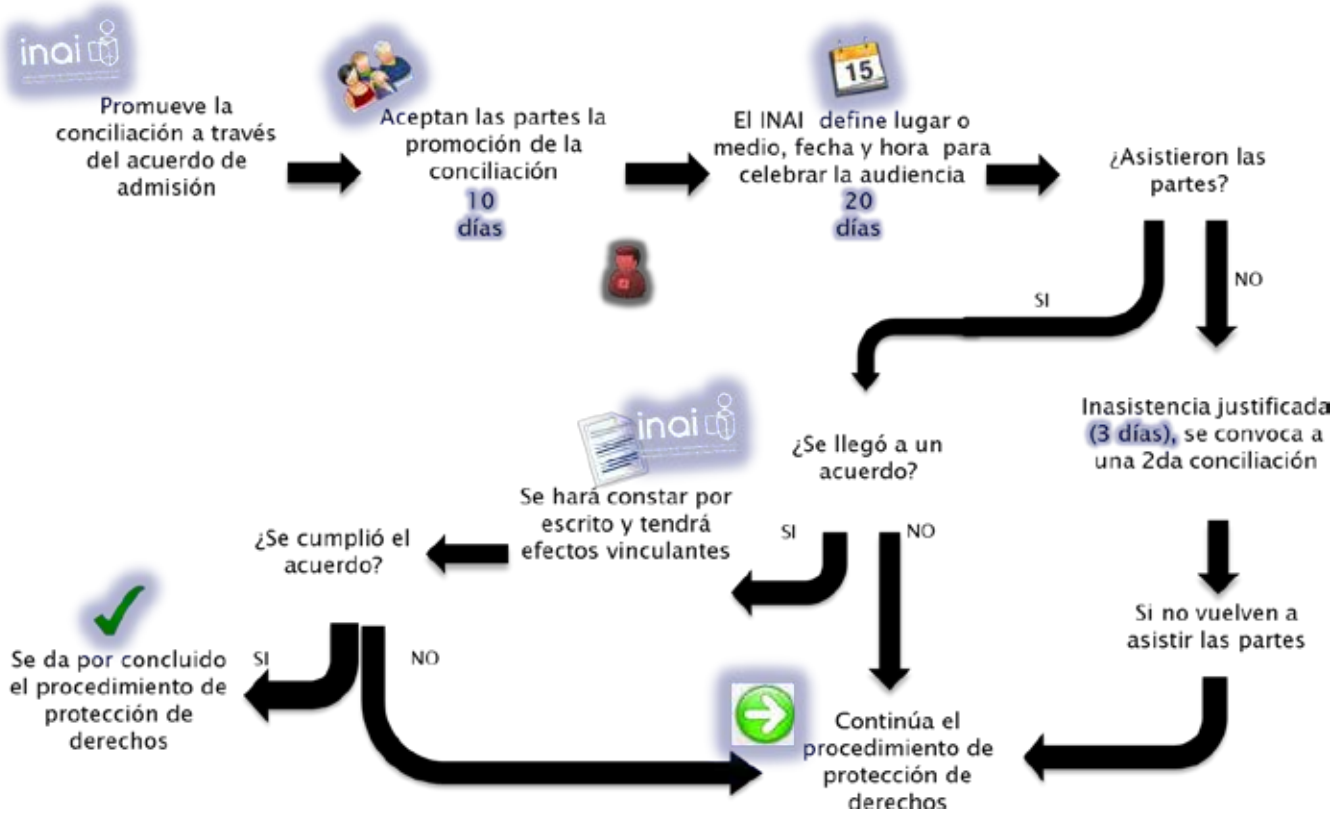
Si hay un acuerdo

- En caso de que en la audiencia se logre la conciliación, el acuerdo deberá constar por escrito, tendrá efectos vinculantes y señalará, en su caso, el plazo de su cumplimiento.

- Durante el periodo de cumplimiento del acuerdo de conciliación, el plazo de 50 días que tiene el Instituto para resolver, quedará suspendido.

- El cumplimiento del acuerdo dará por concluido el procedimiento de protección de derechos, en caso contrario, el Instituto reanudará el procedimiento.

LA CONCILIACIÓN



PROCEDIMIENTO DE VERIFICACIÓN

Capítulo VIII LFPDPPP

Artículos 59 al 60

El INAI tiene atribución para verificar el cumplimiento de la misma, así como de la normatividad y reglamentación que derive de ésta.

La verificación podrá iniciarse:

- De oficio.
- A petición de parte mediante una denuncia.

De oficio

La verificación de oficio procederá por:

- El incumplimiento a resoluciones dictadas con motivo de procedimientos de protección de derechos.
- Cuando se presuma fundada y motivadamente la existencia de violaciones a la LFPDPPP.

A petición de parte (denuncia)

De acuerdo con el Reglamento de la LFPDPPP, cualquier persona podrá denunciar ante el Instituto las presuntas violaciones a las disposiciones previstas en la Ley, y demás ordenamientos aplicables, siempre que no se ubiquen en los supuestos de procedencia del procedimiento de protección de derechos.

En ambos casos, el Pleno determinará, de manera fundada y motivada, la procedencia de iniciar la verificación correspondiente.

Requisitos para presentar una denuncia

La denuncia deberá indicar lo siguiente:

- Nombre del denunciante.
- Domicilio o medio para recibir notificaciones, en su caso.
- Relación de los hechos en los que basa su denuncia.
- Elementos probatorios con los que cuente.
- Nombre del denunciado, domicilio del mismo o en su caso, datos para su ubicación.

La denuncia podrá presentarse en los mismos medios establecidos para el procedimiento de protección de derechos.

PROCEDIMIENTO DE VERIFICACIÓN

Procedimiento de verificación inicia de acuerdo del Pleno. Con el objeto de comprobar el cumplimiento de las disposiciones previstas en la Ley o en la regulación de que se deriven, se podrá requerir al responsable toda la documentación que se considere necesaria o realizar las visitas en el establecimiento en donde se encuentren las bases de datos respectivas.

De igual forma se destaca que desde el inicio y durante el desarrollo del procedimiento, el Instituto puede solicitar la documentación que estime oportuna al denunciante, denunciado, autoridades o terceros interesados.

En el procedimiento de verificación, el Instituto tendrá acceso a la información y documentación que considere necesarias, de acuerdo a la resolución que lo motive.

Los servidores públicos federales estarán obligados a guardar confidencialidad sobre la información que conozcan, derivada de la verificación correspondiente.

Plazos

El procedimiento de verificación, como lo determina el Reglamento, tendrá una duración máxima de 180 días, éstos serán:

- Contados a partir de la fecha en que el Pleno hubiera dictado el acuerdo de inicio y concluirá con la determinación del mismo.
- El Pleno del Instituto podrá ampliar este plazo por una vez y hasta por un periodo igual.
- Este plazo deberá ser notificado al responsable o encargado y, en su caso, al denunciante.
- Puede usted omitir lo relativo al procedimiento de verificación, en el capítulo IX del Reglamento a la LFPDPPP.

DEL PROCEDIMIENTO DE IMPOSICIÓN DE SANCIONES

Capítulo IX - X - XI

Artículos	**61 al 62**	Procedimiento de imposición de sanciones
	63 al 66	De las infracciones y sanciones
	67 al 69	De los delitos en materia de tratamiento indebido de datos personales

La Ley establece que, si con motivo del desahogo del procedimiento de protección de derechos o del procedimiento de verificación que realice el Instituto, se tuviera conocimiento de un presunto incumplimiento de alguno de los principios o disposiciones de la Ley que son susceptibles de ser sancionados, se iniciará el procedimiento de imposición de sanciones.

PROCEDIMIENTO

El procedimiento de imposición de sanciones:

- Iniciará con la notificación del INAI al presunto infractor, sobre los hechos que motivaron el inicio del procedimiento.
- La notificación irá acompañada de un informe que describa los hechos constitutivos de la infracción.
- El presunto infractor tendrá un plazo de 15 días para rendir pruebas y manifestar por escrito lo que a su derecho convenga.
- En caso de no rendirlas, el Instituto resolverá conforme a los elementos de convicción de los que disponga.

El Instituto

- Admitirá las pruebas que estime pertinentes y procederá a su desahogo.
- Podrá solicitar del presunto infractor las demás pruebas que estime necesarias.
- Concluido el desahogo de las pruebas, notificará al presunto infractor el derecho que le asiste para que, de considerarlo necesario, presente sus alegatos dentro de los 5 días siguientes a su notificación.

Infractor

De acuerdo con el Reglamento, el infractor en su contestación:

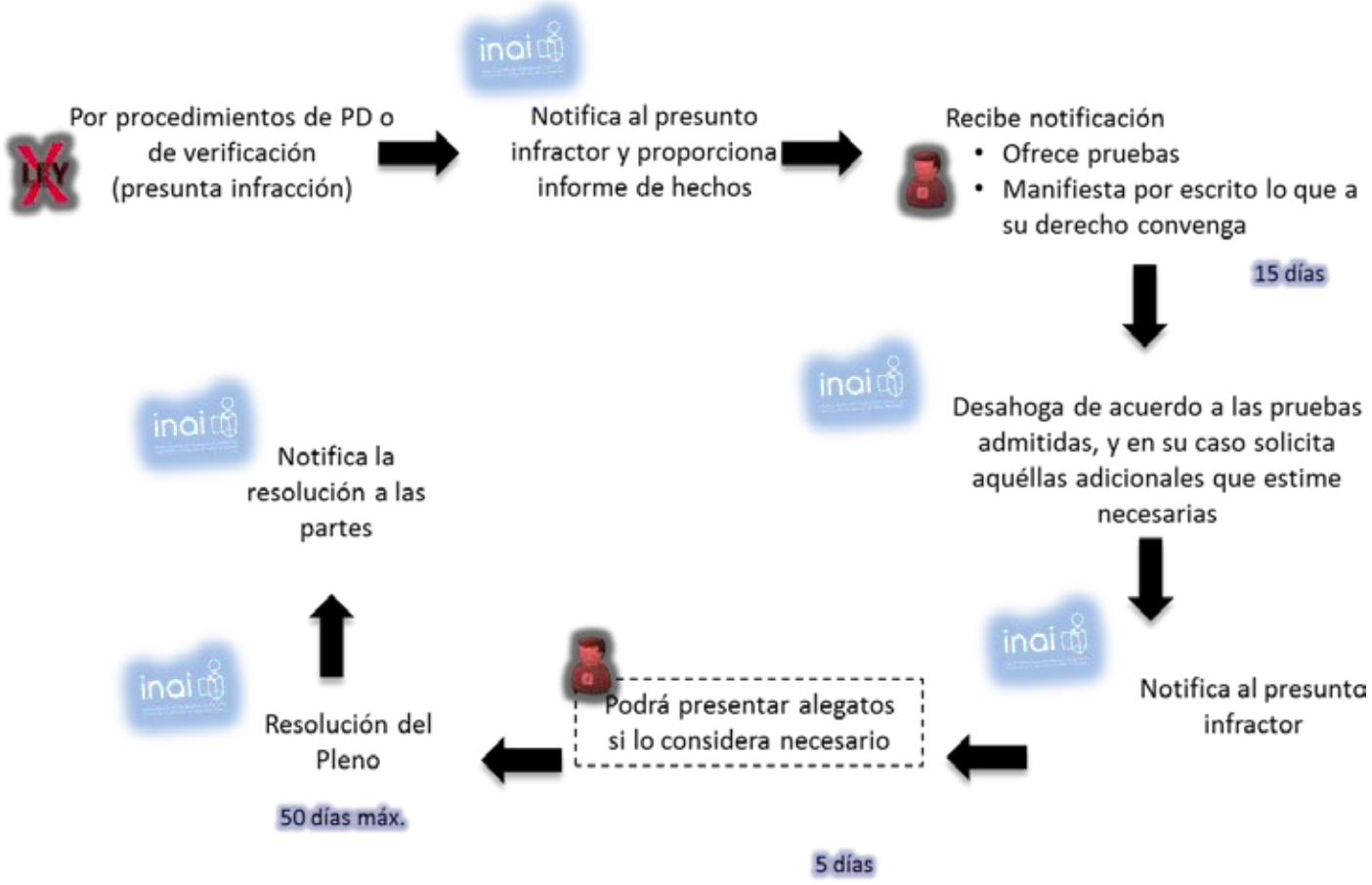
- Se manifestará concretamente respecto de cada uno de los hechos que se le imputen de manera expresa, afirmándolos, negándolos, señalando que los ignora por no ser propios o exponiendo cómo ocurrieron, según sea el caso.
- Presentará los argumentos por medio de los cuales desvirtúe la infracción que se le imputa y las pruebas correspondientes.
- En caso de que se ofrezca prueba pericial o testimonial, se precisarán los hechos sobre los que deban versar y se señalarán los nombres y domicilios del perito o de los testigos, exhibiéndose el cuestionario o interrogatorio respectivo en preparación de las mismas. Sin estos señalamientos se tendrán por no ofrecidas dichas pruebas.

El Instituto, una vez analizadas las pruebas y demás elementos de convicción que estime pertinentes:

- Resolverá en definitiva dentro de los 50 días siguientes a la fecha en que inició el procedimiento sancionador. Cuando haya causa justificada, el Pleno del Instituto podrá ampliar por una vez y hasta por un periodo igual este plazo.

- La resolución será notificada a las partes.

En contra de la resolución al procedimiento de imposición de sanciones procede el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.



INFRACCIONES Y SANCIONES

Infracción (Artículo 63)	Multas (Artículo 64)
La Ley establece que constituirán infracciones, las siguientes conductas llevadas a cabo por el responsable	Las infracciones serán sancionadas por el Instituto con
I. No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada, en los términos previstos en la Ley.	El apercibimiento para que el responsable lleve a cabo los actos solicitados por el titular.
II. Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales. III. Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable. IV. Dar tratamiento a los datos personales en contravención a los principios establecidos en la LFPDPPP. V. Omitir en el Aviso de Privacidad, alguno o todos los elementos que debe contener, de acuerdo a lo señalado en el artículo 16. VI. Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan, cuando resulten afectados los derechos de los titulares. VII. No cumplir con el apercibimiento para que el responsable lleve a cabo los actos solicitados por el titular.	Multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal.

Infracción (Artículo 63)	Multas (Artículo 64)
I. No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada, en los términos previstos en la Ley.	El apercibimiento para que el responsable lleve a cabo los actos solicitados por el titular.
II. Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales. III. Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable. IV. Dar tratamiento a los datos personales en contravención a los principios establecidos en la LFPDPPP. V. Omitir en el Aviso de Privacidad, alguno o todos los elementos que debe contener, de acuerdo a lo señalado en el artículo 16. VI. Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan, cuando resulten afectados los derechos de los titulares. VII. No cumplir con el apercibimiento para que el responsable lleve a cabo los actos solicitados por el titular.	Multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal.

De acuerdo a la fracción XIX del artículo 63, será considerada como infracción cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo que la misma Ley prevé (fracción XIX).

Si de forma reiterada persisten las infracciones señaladas, se impondrá una multa adicional de 100 a 320 000 días de SMVDF.

Si se trata de infracciones cometidas en el tratamiento de datos personales sensibles, las sanciones podrán incrementarse hasta por 2 veces.

Resoluciones del Instituto

El Instituto fundará y motivará sus resoluciones, considerando:

- La naturaleza del dato.
- La notoria improcedencia de la negativa del responsable, para realizar los actos solicitados por el titular.
- El carácter intencional o no, de la acción u omisión constitutiva de la infracción.
- La capacidad económica del responsable.
- La reincidencia.

TRATAMIENTO INDEBIDO DE DATOS PERSONALES

En lo que se refiere a delitos en materia del tratamiento indebido de datos personales:

Delito	Prisión
Provocar una vulneración de seguridad a las bases de datos bajo su custodia.	3 meses a 3 años
Tratamiento de DP mediante el engaño, aprovechándose del error del titular o del responsable.	6 meses a 5 años
Tratándose de datos personales sensibles.	Penas anteriores **x2**

Delitos llevados a cabo con ánimo de lucro

FUENTES ELECTRÓNICAS CONSULTADAS

BLANCO ANTÓN, María José, Globalización de la privacidad: hacia unos estándares comunes –transferencias internacionales de datos- conferencia realizada durante el VI Encuentro Iberoamericano de Protección de Datos, realizado en Cartagena de Indias, Colombia, del 27 al 30 de mayo de 2008. Disponible en:
http://www.agpd.es/portalwebAGPD/internacional/red_iberoamericana/encuentros/VI_Encuentro/common/mjb_globalizacion_privacidad_vi_encuentro_iberoam.pdf

GARZÓN VALDÉS, Ernesto. Lo íntimo, lo privado y lo público, Cuadernos de Transparencia, núm. 06, México, Instituto Federal de Acceso a la Información Pública (INAI), 2008.
Disponible en:
http://docplayer.es/67546-Ernesto-garzon-valdes-lo-intimo-lo-privado-y-lo-publico.html

Protección de Datos Personales, Compendio de lecturas y legislación, México, H. Cámara de Diputados/IFAI/ Instituto Tecnológico Autónomo de México, 1ª edición, Tiro Corto Editores, 2010.
Disponible en:
http://www.inai.org.mx/Publicaciones/publicaciones

Protección de Datos Personales. Compendio de lecturas y legislación, México, H. Cámara de Diputados/IFAI/ Instituto Tecnológico Autónomo de México, 2ª edición, Alonso Editores, 2010.

REMOLINA-ANGARITA, Nelson ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?, 16 International Law, Revista Colombiana de Derecho Internacional, 2010. Disponible en:
http://www.scielo.unal.edu.co/scielo.php?script=sci_arttext&pid=S1692-81562010000100015&lng=es&nrm

Dictamen de las Comisiones Unidas de Puntos Constitucionales y de Estudios Legislativos que contiene Proyecto de Decreto que adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, consultado en Gaceta del Senado número 308, 4 de diciembre de 2008, Primer Periodo Ordinario. Disponible en:
http://www.senado.gob.mx/index.php?ver=sp&mn=2&sm=2&id=11800&lg=60

De la Comisión de Puntos Constitucionales, con Proyecto de Decreto que adiciona un párrafo segundo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, consultado en Gaceta Parlamentaria, Cámara de Diputados, número 2653-II, 11 de diciembre de 2008. Disponible en:
http://gaceta.diputados.gob.mx/

Dictamen de las Comisiones Unidas de Puntos Constitucionales y de Estudios Legislativos, Segunda, respecto a la Minuta Proyecto de Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, consultado en Gaceta del Senado número 308, 4 de diciembre de 2008, Primer Periodo Ordinario. Disponible en:
http://www.senado.gob.mx/index.php?ver=sp&mn=2&sm=2&id=11798&lg=60

Proyecto de Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del capítulo II, del Título Segundo de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, consultado en Diario de los Debates, Legislatura LXI, Año I, Diario 24, Segundo Periodo Ordinario, 22 de abril de 2010. Disponible en:
http://www.senado.gob.mx/index.php?ver=sp&mn=3&sm=3&lg=LXI_I&id=1518

Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, consultado en Diario de los Debates, Legislatura LXI, Año I, Diario 25, Segundo Periodo Ordinario, 27 de abril de 2010. Disponible en:
http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05%2F07%2F2010

Decreto por el que se adiciona un segundo párrafo con siete fracciones al Artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, Diario Oficial de la Federación, 20 de julio de 2007. Disponible en:
http://dof.gob.mx/nota_detalle.php?codigo=4994148&fecha=20/07/2007

Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, Diario Oficial de la Federación, 30 de abril de 2009. Disponible en:
http://dof.gob.mx/nota_detalle.php?codigo=5089047&fecha=30/04/2009

Decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, Diario Oficial de la Federación, 01 de junio de 2009. Disponible en:
http://dof.gob.mx/nota_detalle.php?codigo=5092143&fecha=01/06/2009

Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, Diario Oficial de la Federación, 5 de julio de 2010. Disponible en:
http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010

NOTAS

NOTAS

NOTAS

NOTAS

NOTAS

NOTAS

NOTAS

NOTAS

NOTAS

NOTAS

NOTAS

NOTAS

NOTAS

NOTAS

NOTAS

NOTAS