CURSO: Introducción a la **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**

Manual del Participante

Presentación.

El presente manual, constituye un apoyo para el participante del Curso Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Este material, busca constituirse en una herramienta de consulta y apoyo para las actividades que realizas de manera cotidiana en la materia.

En relación con el uso de tu manual, te recomendamos:

• Utilizar el manual como un material de apoyo y consulta, debido a que contiene los elementos más importantes revisados durante el curso.

• Coloca notas, escribe lo que consideres fundamental o relevante para tus actividades cotidianas.

• Enriquece tu manual con definiciones, conceptos y palabras clave que te parezcan relevantes.

• Si algún tema te interesa, busca información adicional. Te recomendamos visitar la sección de publicaciones, localizada en la página electrónica del INAI.

ÍNDICE

CAPÍTULO I

El Derecho a la Protección de Datos Personales en México

Orígenes de la Protección de los Datos Personales

La protección de los datos personales surge con la Sociedad de la Información en el mundo industrializado durante los años 70. Se convirtió en la política pública adoptada frente al creciente uso de las tecnologías de la información. Estas tecnologías habían demostrado su gran capacidad de producir riqueza a partir del uso de la información personal. Al mismo tiempo, también habían mostrado que los gobiernos podían utilizarlas para invadir la vida privada de los ciudadanos y ejercer un mayor control sobre ellos. Con el fin de conciliar estas dos necesidades opuestas, se emitieron las primeras leyes de protección de datos personales.

Estas leyes han tenido como objetivo:

- Establecer reglas orientadas al tratamiento o utilización de los datos personales por organizaciones públicas y privadas
- Proteger a la persona respecto al uso de su información personal
- Salvaguardar la privacidad, dignidad y autonomía de las personas.
- Facilitar el tratamiento de la información personal que hacen las organizaciones públicas y privadas.

La protección de los datos personales ha sido la política pública adoptada en el mundo para proteger la privacidad de los ciudadanos sin impedir la libre circulación de la información personal.

El Derecho a la Protección de Datos Personales

Con el tiempo ha venido surgiendo en diversos países (incluido México) la noción de que los seres humanos tenemos un derecho a la protección de los datos personales autónomo e independiente del derecho a la privacidad. Este derecho a la protección de datos personales se encuentra previsto en el segundo párrafo del artículo 16 de la Constitución mexicana y:

- Le confiere a las personas control sobre su información personal.
- Faculta al individuo a decidir quién, cómo, cuándo y hasta qué punto utilizará su información personal.

El derecho a la protección de los datos personales protege la dimensión informativa de nuestra vida privada.

Límites Democráticos al Ejercicio del Derecho de Protección de Datos Personales

Al ser un derecho constitucional, el derecho a la protección de datos personales no es absoluto. Sólo admite aquellas restricciones *prescritas en ley* que resulten razonables en una sociedad democrática:

- seguridad nacional,
- disposiciones de orden público,
- seguridad y salud públicas
- para proteger los derechos de terceros.

El derecho a la protección de datos personales sólo se limita por excepción prevista en la ley.

Derecho a la Privacidad

El derecho a la protección de los datos personales es distinto del derecho a la privacidad. Este último podría definirse como el derecho que todo individuo tiene a separar aspectos de su vida privada del escrutinio público.[1] Es un derecho complejo, difícil de definir, pues cada persona es quién decide qué aspectos de su vida personal hace del conocimiento de los demás. El derecho a la privacidad se encuentra previsto en el primer párrafo del artículo 16 de la Constitución mexicana.

Dado que es un concepto difícil de definir, algunos autores señalan que a la privacidad simplemente "la entiendes cuando la pierdes".

Componentes del Derecho a la Privacidad

El derecho a la privacidad tiene dos componentes:

1) Derecho a aislarte. Esta dimensión fue articulada por Samuel Warren y Louis Brandeis en 1890.[2] Implica que, como seres humanos, podemos escudarnos física y psicológicamente de las entrometedoras miradas de los demás.

[1] García Ricci, Diego, *El derecho a la privacidad*, México, Nostra, 2017, p. 15.
[2] Warren, Samuel y Louis Brandeis, "The Right to Privacy" en *Harvard Law Review*, vol. IV, núm. 5, 1890, p. 205.

2) Derecho a controlar la información personal. Esta dimensión fue articulada por Alan Westin en 1967.[3] Implica que nosotros mismos somos los que controlamos nuestra información personal, incluso después de haberla divulgado. Esto nos permite poder participar activamente en sociedad.

Son dos aspectos de un mismo derecho que se encuentran intrínsecamente vinculados.

Diferencias entre el Derecho a la Privacidad y el Derecho a la Protección de los Datos Personales

El derecho a la privacidad:

1) Protege al individuo de intromisiones arbitrarias o ilegales en su vida privada.
2) Protege diversas áreas relacionadas con la vida privada del individuo:

    - Domicilio
    - Comunicaciones
    - Familia
    - Cuerpo
    - Información personal

El derecho a la protección de los datos personales:

1) Le confiere al individuo la facultad de participar en el tratamiento que otros hacen de sus datos personales.
2) Protege el manejo justo de su información personal al garantizarle el acceso, rectificación y cancelación de sus datos personales, así como al permitirle manifestar su oposición al tratamiento de los mismos (derechos ARCO).

El derecho a la protección de datos personales implica el poder de disposición y control sobre sus datos personales y, en consecuencia, confiere al titular una serie de derechos, acceso, rectificación, cancelación y oposición, a partir de ese poder de disposición y control.

Derecho de Acceso a la Información Pública

[3] Westin, Alan, *Privacy and Freedom,* Nueva York, Ateneum, 1967, p. 7.

Es el derecho que todo individuo tiene a acceder a la información que obra en los archivos públicos. Este derecho está previsto en el artículo 6, apartado A de la Constitución mexicana.

El derecho de acceso a la información pública garantiza la participación democrática de los ciudadanos.

Diferencias entre el Derecho de Acceso a la Información Pública y el Derecho a la Protección de Datos Personales

El derecho de acceso a la información pública:

- Le permite al individuo acceder a la información que obra en los archivos de los poderes públicos siempre que dicha información no se encuentre clasificada como reservada o confidencial.

El derecho a la protección de datos personales:

- Le confiere al individuo la facultad de acceder a los datos personales que sobre su persona obran en poder de los poderes públicos, así como rectificarlos, cancelarlos y oponerse a que sean tratados.

El derecho de acceso a la información pública:

- No limita el ejercicio del derecho de protección de datos personales salvo en casos excepcionales, p.ej. causas de interés público.

El derecho a la Protección de Datos Personales:

- Limita el ejercicio del derecho de acceso a la información pública salvo casos excepcionales, p. ej. causas de interés público.

Se trata de dos derechos distintos pero, en ocasiones, relacionados.

CAPÍTULO II

Marco Jurídico Nacional e Internacional del Derecho a la Protección de Datos Personales

Fundamento Constitucional

> El segundo párrafo del artículo 16 constitucional se reformó en 2009 para darle al *derecho a la protección de los datos personales* un estatus constitucional. También se reconocieron los derechos de acceso, rectificación y cancelación de los datos personales, así como el derecho a manifestar su oposición al tratamiento de los mismos. A estos derechos se les conoce como derechos ARCO, por el acrónimo formado a partir de las iniciales de las palabras acceso, rectificación, cancelación y oposición.

Con la reforma constitucional de 2009, la dimensión informacional de los datos personales de los mexicanos quedó protegida a través del derecho a la protección de datos personales.

El segundo párrafo del artículo 16 constitucional señala textualmente:

> "*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*".

El ejercicio del derecho a la protección de datos personales será determinado por la ley.

Fundamentos Legales del Derecho a la Protección de Datos Personales

El derecho a la protección de datos personales está regulado por las leyes siguientes:

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

- Leyes estatales de protección de datos personales (una por cada entidad federativa).

Se trata de un mismo derecho pero regulado por leyes distintas.

Instrumentos Internacionales de Protección de Datos Personales

La protección de datos personales tiene una dimensión internacional. Ésta se encuentra prevista en diversos instrumentos normativos los cuales ejercen una influencia importante en las legislaciones de todos los países del mundo. A continuación, se enlistan los más relevantes:

- OCDE—Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales (1980).
- Consejo de Europa—Convenio del CoE para la protección de las personas con respecto al tratamiento automatizado de carácter personal (Convenio 108) (1981).
- ONU—Directrices para la regulación de los ficheros computarizados de datos personales (Resolución 45/95 de la Asamblea General) (1990).
- Unión Europea—Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos (1995).
- APEC—Marco de privacidad del Foro de Cooperación Económica Asia-Pacífico (2005).
- Conferencia de Autoridades de Privacidad—Resolución de Madrid (2009).

Actualizaciones

- OCDE—Actualización de las Directrices (2013).
- Consejo de Europa—Convenio 108 (en modernización).
- ONU—Resoluciones de la Asamblea General 68/167 (2013) y 69/166 (2014) llamadas *El derecho a la privacidad en la era digital.*
- Unión Europea—Reglamento general de protección de datos (2016), en vigor a partir del 2018.
- Red Iberoamericana de Protección de Datos Personales—Estándares de protección de datos personales para los Estados iberoamericanos (2017).

Aunque casi todos los instrumentos internacionales en materia de protección de datos personales no vinculan jurídicamente a los países, dichos instrumentos han

ejercido una influencia muy importante en las legislaciones de todo el mundo, incluida la mexicana.

El único instrumento internacional que actualmente vincula jurídicamente a México es el Convenio 108 del Consejo de Europa, referido líneas arriba.

Este Convenio cuenta con dos protocolos:

- Protocolo de autoridades de control (2001)
- Protocolo de modernización (2018)

Tras haberlo solicitado, México fue invitado formalmente a adherirse al Convenio en 2017.

La Cámara de Senadores aprobó tanto el Convenio como el Protocolo de autoridades de control el 12 de junio de 2018.

Con la adopción del Convenio 108, se fortalece la protección de los datos personales en el país y México se adhiere a una red de cooperación y asistencia integrada por más de 50 Estados Parte.

La protección de los datos personales va más allá de nuestras fronteras

Reforma Constitucional en Derechos Humanos

Esta reforma se publicó en el *Diario Oficial de la Federación* el 10 de junio de 2011. Su efecto fue incorporar a la Constitución mexicana los derechos humanos reconocidos en los tratados internacionales suscritos por el Estado mexicano. La reforma también introdujo dos herramientas hermenéuticas*:*

- Interpretación conforme
- Principio pro persona

Se trata de un nuevo paradigma de protección de derechos humanos.

Estas herramientas hermenéuticas podrían definirse de la siguiente manera:

- *Interpretación conforme*—Normas de derechos humanos deben interpretarse conforme a la Constitución mexicana y tratados internacionales en la materia*.*
- *Principio pro persona*—Normas de derechos humanos deben interpretarse favoreciendo la interpretación más amplia.

Herramientas diseñadas para expandir nuestra esfera de derechos y libertades fundamentales.

La reforma constitucional de 2011 ha comenzado a influir positivamente en la normatividad secundaria en materia de datos personales. Los Lineamientos Generales de Protección de Datos Personales para el Sector Público
(en adelante, Lineamientos Generales), por ejemplo, establecen:

> Artículo 5. En el tratamiento de datos personales de menores de edad, el responsable debe privilegiar el *interés superior* de las niñas, niños y adolescentes.

Esta disposición hace suyo el principio de proteger el interés superior del menor previsto en la Convención de los Derechos del Niño de 1989.

Se fortalece la protección de grupos vulnerables.

Implicaciones de la Reforma Constitucional en Derechos Humanos en materia de protección de la privacidad.

El derecho a la privacidad previsto en los tratados internacionales en materia de derechos humanos quedó incorporado al texto de la Constitución en virtud de la reforma constitucional del 10 de junio de 2011. Dos son los artículos que prevén este derecho:

- Art. 11 de la Convención Americana de Derechos Humanos
- Art. 17 del Pacto Internacional de Derechos Civiles y Políticos

La jurisprudencia de la Corte Interamericana de Derechos Humanos también se convirtió en una fuente normativa importante, pues la Suprema Corte de Justicia de la Nación declaró, al resolver la Contradicción de tesis 293/2011, que dicha jurisprudencia es jurídicamente vinculante para México.

Los tratados internacionales son pues instrumentos normativos aliados en la protección de los datos personales en México.

Implicaciones de la Reforma Constitucional en Derechos Humanos en Materia de Datos Personales

Aquellos tratamientos de datos personales que tengan como efecto una violación a los derechos humanos podrían ser inconstitucionales o inconvencionales.

Derechos humanos que podrían ser violentados a través de un tratamiento de datos personales:

- derecho a la privacidad
- derecho a la no discriminación
- derecho de asociación

La reforma constitucional garantiza que los tratamientos de datos personales respeten la dignidad humana.

CAPÍTULO III

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

Competencia en Materia de Datos Personales

La jurisdicción en materia de datos personales es de tipo concurrente. Esto quiere decir que tanto la federación como las entidades federativas 'concurren' en esta materia. Sus facultades legislativas, no obstante, son distintas. A cada una le compete legislar, en materia de datos personales, lo siguiente:

- Federación:
  - Sector público
  - Sector privado

- Entidades Federativas:
  - Sector público

En México existe una jurisdicción dual en la materia de datos personales para el sector público.

Distribución de Competencias en el Sector Público

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley) establece la distribución de competencias al definir:

- Facultades para las autoridades federales.
- Facultades para las entidades federativas.

Uno de los objetivos de la Ley General es distribuir competencias entre el INAI y los organismos garantes estatales, así como entre los Organismos garantes de la Federación y las Entidades Federativas, en materia de protección de datos personales en posesión de sujetos obligados;

Se trata de una ley marco que establece estándares mínimos.

Sujetos Obligados

Son sujetos obligados por esta Ley, en el ámbito federal, estatal y municipal:

- Cualquier autoridad, entidad, órgano y organismo de los Poderes
  - Ejecutivo,
  - Legislativo y

- Judicial,

❖ Órganos autónomos,

❖ Partidos políticos,

❖ Fideicomisos y fondos públicos

❖ Los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal serán responsables de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares.

En todos los demás supuestos diferentes a los mencionados en el párrafo anterior, las personas físicas y morales se sujetarán a lo previsto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Conceptos Clave de la Ley

La Ley maneja diversos conceptos claves entre los que destacan:

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

- Datos personales sensibles: aquellos que se refieren a la esfera más íntima de una persona, p. ej. Origen racial o étnico, salud, religión, orientación política, preferencia sexual.

- Tratamiento: operación manual o automatizada aplicada a los datos personales. Sirvan como ejemplo a manera enunciativa más no limitativa: obtención, uso, registro, organización, conservación, difusión, transferencia, entre otros.

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

Se trata de actividades propias en la sociedad de la información.

Figuras Clave de la Ley

La Ley también prevé algunas figuras claves para la protección de los datos personales:

- **Titular:** Persona física a quien corresponden los datos personales.

- **Responsable:** Son los sujetos obligados por la Ley General que deciden sobre determinado tratamiento de datos personales, cuestión que implica determinar el tipo de datos personales a tratar, la categoría de titular, las finalidades o usos a que serán sometidos los datos personales, entre otras decisiones.

- **Encargado:** Persona física o jurídica, pública o privada, ajena a la organización del responsable, que trata datos personales a nombre y por cuenta de éste.

Son partes en las relaciones construidas para el tratamiento de los datos personales.

Protección Multi-Instancial

En la protección de datos personales participan diversas autoridades con roles distintos. Estas autoridades son:

Responsables

Los Responsables son instancias públicas, no personas físicas. Tienen el poder de decisión respecto al tratamiento de datos personales: uso, finalidades, tipo de datos. Son quienes reciben las solicitudes para el ejercicio de los derechos ARCO.

Comité de Transparencia

El Comité de Transparencia es la autoridad máxima en materia de protección de datos personales. Cada Responsable cuenta con un Comité de Transparencia, el cual se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable.

Organismos Garantes

- El INAI y los Institutos locales en las entidades federativas. Tienen autonomía constitucional: Arts. 6 y 116-VIII de la Constitución mexicana. Es la autoridad

que se encarga de garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales, así como vigilar el cumplimiento de las obligaciones previstas en la las leyes estatales en la materia.

INAI:

- Interpreta la Ley General en el ámbito administrativo. Tiene también la facultad de atracción de recursos de revisión. Esto suele tener lugar en aquellos asuntos que, por su interés y trascendencia, resulta más conveniente que sean resueltos por la autoridad nacional de datos personales. El INAI también resuelve los recursos de inconformidad hechos valer ante las resoluciones de recursos de revisión emitidas por los órganos garantes de las entidades federativas.

Estas autoridades llevan a cabo funciones distintas pero complementarias.

Primeros contactos de los Titulares

De acuerdo con la Ley, todos los responsables deben contar con las áreas siguientes:

- Unidad de Transparencia:
  - Integrada conforme a la Ley General de Transparencia y Acceso a la Información Pública.
  - Gestiona las solicitudes de ejercicio de derechos ARCO presentadas por los titulares.
  - Asesora a las áreas adscritas sobre datos personales.

- Comité de Transparencia:
  - Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable.
  - Integrado conforme a la Ley General de Transparencia y Acceso a la Información Pública.
  - Autoridad máxima en la materia de protección de datos personales.
  - Confirma, modifica o revoca declaraciones de inexistencia de datos personales o negativas de ejercicio de derechos ARCO

La obligación principal de estas áreas es: *facilitar el ejercicio de los derechos ARCO,* garantizar un adecuado tratamiento de los datos personales como son el cumplimiento de los principios y deberes, la realización de transferencias, la contratación de prestadores de servicios que impliquen el tratamiento de los datos personales, entre otras cuestiones.

CAPÍTULO IV

Principios, Deberes y Responsabilidades de los Sujetos Obligados por la Ley

Principios de Protección de Datos Personales

De acuerdo con la Ley, los responsables deben observar los principios de protección de datos personales, los cuales les imponen deberes muy específicos. Estos principios son los siguientes:

- **Principio de licitud (Art. 17):**
  Implica el deber de identificar en la normatividad aplicable las facultades que autorizan a los responsables a tratar datos personales.

- **Principio de finalidad (Art. 18):**

Implica el deber de determinar el uso concreto, lícito, explícito y legítimo que se le va a dar a los datos personales. ¿Cambios? Requieren el consentimiento de los titulares. Los responsables podrán tratar los datos personales para finalidades distintas a aquéllas que motivaron el tratamiento de los datos personales cuando cuenten con el consentimiento del titular y con atribuciones conferidas en ley

- **Principio de consentimiento (Arts. 20, 21, 22):**
  Implica el deber de recolectar información personal sólo con la autorización, expresa o tácita, según corresponda, del titular (salvo excepciones).

- Principio de lealtad (Art. 19):
  Implica el deber de no actuar de manera engañosa o fraudulenta: sin dolo, error o mala fe.

- Principio de calidad (Arts. 23 y 24):

  Implica el deber de asegurar que los datos personales se mantengan exactos, completos y actualizados para los fines que persigue determinado tratamiento de datos personales. Implica establecer y documentar procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales. Este principio también implica suprimir los datos personales una vez cumplida la finalidad que motivó su tratamiento.

- Principio de proporcionalidad (Art. 25):
  Implica el deber de recabar y utilizar sólo aquellos datos que resulten estrictamente necesarios para el fin propuesto.

- Principio de información (Arts. 26, 27 y 28):

Implica el deber de informar a los titulares la existencia y características principales del tratamiento al que serán sometidos sus datos personales, mediante un "aviso de privacidad".

- Principio de responsabilidad (Arts. 29 y 30):

Implica el deber de implementar políticas, programas y mecanismos obligatorios y exigibles al interior de la organización del responsable que acrediten el cumplimiento de los principios, deberes y obligaciones previstos en la Ley. El responsable está obligado a la rendición de cuentas ante el titular y el INAI u organismos garantes, según corresponda

Principios que garantizan un manejo justo de la información

Por su parte, los Lineamientos Generales se han dado a la tarea de pormenorizar la aplicación de los principios de protección de datos personales. Establecen, por ejemplo, lo siguiente:

Principio de finalidad:

> Artículo 10. Cuando cambien las finalidades de un tratamiento de datos personales, el Responsable debe considerar: la expectativa razonable de privacidad; la naturaleza de los datos personales; las consecuencias para el titular por un tratamiento posterior; y las medidas adoptadas para dicho tratamiento.

Principio de consentimiento:

> Artículo 20 Titular puede revocar, en cualquier momento, el consentimiento otorgado para el tratamiento de sus datos a través de los derechos de cancelación y oposición.

Principio de calidad:

> Artículo 23. Supresión de datos personales usando atributos como irreversibilidad, seguridad y confidencialidad y favorabilidad con el medio ambiente.

Principio de proporcionalidad:

> Artículo 25. Responsable debe realizar esfuerzos razonables para limitar los datos personales tratados al mínimo necesario en relación con el fin del tratamiento.

Efectiva aplicación de los principios de protección de datos personales.

Aviso de Privacidad

Este documento informa a los titulares las características principales o los términos y condiciones a que son sometidos sus datos personales. Puede ser difundido a través de medios electrónicos y físicos. Existen dos tipos de aviso de privacidad:

- Simplificado
- Integral

Aviso de Privacidad Simplificado

La puesta a disposición del aviso de privacidad simplificado al titular, no exime al responsable de poner a disposición el aviso de privacidad integral

Debe contener la siguiente información:

- Denominación del responsable.
- Finalidades del tratamiento.
- En caso de transferencias que requieran consentimiento del titular, informar:

  a) a quien se transfieren los datos personales y

  b) finalidades de la transferencia.

- Medios para que el titular manifieste su negativa al tratamiento y transferencia de sus datos personales. Estos medios deben estar disponibles previo al tratamiento o la transferencia de los datos personales.
- Sitio para consultar el aviso de privacidad integral.

Aviso de Privacidad Integral

Debe contener la información del simplificado y al menos:

- Domicilio del responsable.
- Datos personales sometidos a tratamiento, identificando aquellos que sean sensibles.
- Fundamento legal del tratamiento.
- Finalidades del tratamiento, señalando aquellas que requieran el consentimiento del titular.
- Mecanismos, medios y procedimientos para ejercer los derechos ARCO.
- Domicilio de la Unidad de Transparencia.
- Medios para comunicar cambios en el aviso de privacidad.

El aviso de privacidad garantiza un respeto adecuado a la autonomía de los individuos respecto a sus datos personales.

Por su parte, los Lineamientos Generales se han dado a la tarea de pormenorizar la forma como debe elaborarse el Aviso de Privacidad. Establecen, por ejemplo, las reglas siguientes:

A) Objeto del Aviso de Privacidad

Artículo 27. El objeto del Aviso de Privacidad es el de Informar al Titular los alcances y condiciones del tratamiento de los datos personales, para que pueda tomar decisiones informadas, manteniendo el control y disposición de los mismos.

Efectivo control de la información

B) Características del Aviso de Privacidad

Artículo 28. El Aviso de Privacidad debe ser escrito de forma sencilla, con la información necesaria, en lenguaje claro y comprensible, con una estructura y diseño que facilite su entendimiento.

Información clara y precisa

C) Prohibiciones en el Aviso de Privacidad

Artículo 28, segundo párrafo. El Responsable deberá abstenerse de:

- Usar frases inexactas, ambiguas o vagas.
- Incluir textos o formatos que induzcan a los titulares a elegir una opción en específico.
- Marcar previamente casillas.
- Remitir a textos o documentos no disponibles para el Titular.

Evitar errores al momento de informar

D) Manifestación de una negativa en el Aviso de Privacidad

Artículo 33. El Responsable debe dar opciones al titular para manifestar su negativa al tratamiento de datos personales en el aviso de privacidad, ya sea a través de casillas u opciones de marcado.

El Titular debe contar con la oportunidad de manifestar, *inequívocamente, su conformidad o inconformidad con el tratamiento que otros hacen de sus datos personales.*

Los Lineamientos Generales también establecen otra regla de gran relevancia en materia probatoria:

> Artículo 45. La carga de la prueba respecto a la puesta a disposición del aviso de privacidad recae en el responsable.

El tratante de la información tiene una mayor responsabilidad frente al Titular.

Medidas de Seguridad Previstas por la Ley

Los responsables deben adoptar medidas de seguridad que permitan proteger los datos personales contra daño, pérdida, alteración o destrucción; uso, acceso o tratamiento no autorizados; así como aquellas que garanticen la confidencialidad, integridad y disponibilidad de éstos.

Factores para determinar y establecer las medidas de seguridad de carácter:

- Administrativas
- Físicas
- Técnicas

Las medidas de seguridad administrativas se refieren al establecimiento de políticas y procedimientos para:

> a) la gestión, soporte y revisión de la seguridad de la información a nivel organizacional;
>
> b) la identificación, clasificación y borrado de la información.

Las medidas de seguridad físicas se refieren al establecimiento de políticas y procedimientos para:

> a) Prevenir el acceso no autorizado al perímetro de la organización, instalaciones físicas, áreas críticas, recursos e información;
>
> b) Prevenir daño o interferencia a instalaciones físicas, áreas críticas de la organización, recursos e información;
>
> c) Proteger recursos móviles, portátiles, soportes físicos o electrónicos que salgan de la organización;
>
> d) Proveer a equipos que almacenan datos personales de mantenimiento eficaz.

Las medidas de seguridad técnicas se refieren al establecimiento de políticas y procedimientos para:

a) asegurar que el acceso a las bases de datos sea por usuarios identificados y autorizados;
b) generar privilegios o perfiles de acceso a los datos personales en función de las atribuciones y funciones de cada usuario.

c) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

d) revisar la configuración de seguridad del software y hardware;

e) gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales

La Ley prevé además otras medidas de seguridad tales como:

A) Establecer medidas especiales en función de ciertos factores—riesgo inherente de los datos, su sensibilidad, el desarrollo tecnológico, las transferencias que se hagan y las vulneraciones a seguridad ya ocurridas;

B) Implementar un sistema de gestión de la seguridad de los datos personales. Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley y las demás disposiciones que le resulten aplicables en la materia.

C) Elaborar un documento de seguridad que describa los elementos indispensables que permitirán asegurar un cuidado adecuado de los datos personales Deberá contener al menos lo siguiente:

I. El inventario de datos personales y de los sistemas de tratamiento;

II. Las funciones y obligaciones de las personas que traten datos personales;

III. El análisis de riesgos;

IV. El análisis de brecha;

V. El plan de trabajo;

VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y

VII. El programa general de capacitación.

Se trata de garantizar la confidencialidad, integridad y disponibilidad de los datos personales *y que los responsables lleven a cabo un manejo cuidadoso de los datos personales.*

Las medidas de seguridad adoptadas por el responsable deberán considerar: (**artículo 32.)**:

I. El riesgo inherente a los datos personales tratados;

II. La sensibilidad de los datos personales tratados;

III. El desarrollo tecnológico;

IV. Las posibles consecuencias de una vulneración para los titulares;

V. Las transferencias de datos personales que se realicen;

VI. El número de titulares;

VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y

VIII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

Por su parte, los Lineamientos Generales se han dado a la tarea de pormenorizar la forma como deben instrumentarse algunas medidas de seguridad. Establecen, por ejemplo, las reglas siguientes:

A) Deber de seguridad:

Artículo 55. El Responsable debe establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico. Las medidas señaladas por la Ley son "mínimos exigibles". Podrán adoptarse otras medidas adicionales que brinden una mejor garantía en la protección de datos personales.

Preservación de la seguridad de la información

B) Política interna de gestión y tratamiento de datos personales:

Artículo 56. El Responsable debe incluir en sus políticas internas de gestión y tratamiento de datos personales:

- el cumplimiento de los principios deberes y derechos;
- los roles y responsabilidades de los involucrados internos y externos;
- las sanciones por incumplimiento;
- la identificación del ciclo de vida de los datos personales;
- el proceso general para el establecimiento y actualización de los mecanismos y medidas de seguridad; y
- el proceso de atención de los derechos ARCO.

Preservación de la seguridad de la información

C) Funciones y obligaciones del Responsable

Artículo 57. El Responsable debe establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todos los que traten datos personales en su organización, de acuerdo con el sistema de gestión.

Todos los participantes tienen responsabilidad en el tratamiento de datos personales

D) Inventario de datos personales

Artículo 58. El Responsable debe elaborar un inventario de datos personales considerando:

- catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos;
- finalidades del tratamiento;
- catálogo del tipo de datos;
- catálogo de formatos de almacenamiento;
- servidores públicos con acceso a sistemas de tratamiento;
- nombre o denominación del encargado;
- destinatarios o terceros receptores en casos de transferencias, así como sus finalidades.

Aspectos relevantes para la protección de datos personales

E) Ciclo de vida de los datos personales:

Artículo 59. En el ciclo de vida de los datos personales, el Responsable debe considerar:

- la obtención de los datos personales;
- el almacenamiento de dichos datos;
- el uso de los mismos conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento;
- su divulgación;

- el bloqueo que, en su caso, proceda;
- la cancelación, supresión o destrucción de los datos personales.

Seguimiento permanente en el tratamiento de datos personales

F) Análisis de riesgos

Artículo 60. En su análisis de riesgos, el Responsable debe considerar:

- los requerimientos obligatorios, códigos de conducta o mejores prácticas del sector;
- el valor de los datos personales conforme a su clasificación y ciclo de vida;
- el valor y exposición de los activos involucrados en el tratamiento de datos personales;
- las consecuencias negativas para los titulares en casos de vulneraciones a la seguridad de los datos.

Diversos aspectos que deben ser considerados para minimizar los riesgos

G) Análisis de brecha:

Artículo 61. En su análisis de brecha, el Responsable debe considerar:

- las medidas de seguridad existentes y efectivas;
- las medidas de seguridad faltantes;
- la existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles que ya se encuentren implementados.

Medidas que deben revisarse periódicamente

Vulneración a la Seguridad de los Datos Personales

Esta vulneración tiene lugar cuando, intencionada o no intencionadamente, se liberan datos personales en un ambiente no confiable. Puede ocurrir en cualquier fase del tratamiento de datos y podría afectar los derechos patrimoniales o morales de los titulares.

De manera enunciativa más no limitativa, los tipos de vulneraciones que pueden ocurrir pueden ser:

A) Pérdida o destrucción no autorizada.

B) Robo, extravío o copia no autorizada.

C) Uso, acceso o tratamiento no autorizado.

D) Daño, alteración o modificación no autorizada.

Se trata de vulneraciones a la seguridad de los datos personales que pueden comprometer la de forma significativa los derechos patrimoniales o morales, de las personas.

Obligaciones por la Vulneración a la Seguridad de los Datos Personales

La Ley establece que en caso de que ocurra una vulneración a la seguridad de los datos personales, aquellas que afecten de forma significativa los derechos personales y patrimoniales de los titulares, el responsable está obligado a comunicar tal situación al titular y al organismo garante, sin dilación alguna, en cuanto tenga confirmado que dicha vulneración en verdad ocurrió. Concretamente, el responsable deberá informar:

A) La naturaleza del incidente.

B) Los datos personales comprometidos.

C) Las recomendaciones que el titular puede adoptar para protegerse.

D) Las acciones correctivas realizadas de forma inmediata.

E) Los medios donde podrá obtener más información al respecto.

La Ley señala, además, que el responsable debe llevar una bitácora en la que describa las vulneraciones de seguridad ocurridas en su organización. En ella se tiene que registrar:

A) Fecha en que ocurrió la vulneración.

B) Motivo.

C) Acciones correctivas implementadas, de forma inmediata y definitiva.

El responsable no deberá ocultar la vulneración a la seguridad de los datos personales sino informarla tanto al titular como al organismo garante *cuando* afecten de manera significativa los derechos patrimoniales o morales del titular.

Por su parte, los Lineamientos Generales señalan, en relación con las vulneraciones a la seguridad de los datos personales, lo siguiente:

Plazo de notificación

Artículo 40 El Responsable debe notificar al INAI y al Titular aquellas vulneraciones a la seguridad de datos personales que significativamente afecten sus derechos patrimoniales o morales dentro de un plazo máximo de 72 horas contado a partir de la ocurrencia de dichas vulneraciones.

Facilitarle al titular la toma de decisiones oportunas

Obligaciones de Confidencialidad

La Ley también establece que el responsable está obligado a establecer controles o mecanismos que garanticen que toda persona que intervenga en un tratamiento de datos personales guardará confidencialidad respecto de ellos aún después de finalizar sus relaciones con el responsable. Ejemplos:

A) Suscripción de cláusulas de confidencialidad con quienes intervengan en el tratamiento.

B) Sanciones por la revelación no autorizada de datos personales.

Se debe dejar claro que existe un deber de confidencialidad en el manejo de los datos personales y que quien incumpla con ese deber podría ser sancionado.

Encargado

El encargado es un prestador de servicios que efectúa el tratamiento de datos personales a nombre y cuenta de un responsable.

- Puede ser una persona física o jurídica, ajena a la organización del responsable, que sola o conjuntamente trata datos personales atendiendo las instrucciones del responsable
- No tiene poder de decisión sobre el alcance y contenido del tratamiento de los datos personales
- Debe limitar sus actuaciones a las instrucciones del responsable

.

Obligaciones de los Encargados

La Ley señala que el responsable debe formalizar su relación con el encargado a través de la suscripción de un contrato o cualquier otro instrumento jurídico, de acuerdo con la normatividad que le resulte aplicable en materia de contrataciones, con cláusulas que indiquen:

A) Las instrucciones del responsable

B) La abstención del encargado de tratar datos personales para finalidades no autorizadas por el responsable

C) La implementación de medidas de seguridad

D) La obligación de informar en casos de vulneración de la seguridad de datos personales

E) La obligación de guardar confidencialidad

F) La obligación de suprimir o devolver los datos cuando concluya la relación con el responsable

G) La abstención de transferir datos personales sin autorización.

El responsable además debe autorizar expresa y previamente los casos en los que el encargado podría subcontratar los servicios de tratamiento de datos personales. El subcontratado adquiere la calidad de encargado.

El responsable también podrá contratar o adherirse a servicios, aplicaciones e infraestructura de cómputo en la nube cuando el proveedor cuente con políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la Ley General y demás disposiciones que resulten aplicables.

Finalmente, la Ley señala que el responsable no está obligado a informar a los titulares sobre aquellas comunicaciones de datos personales que les haga a los encargados ni a solicitar su consentimiento.

Cuando el encargado incumpla las instrucciones del responsable y decida por sí mismo sobre el tratamiento de los datos personales, asumirá el carácter de responsable conforme a la legislación en la materia que le resulte aplicable (**Artículo 60).**

Lo que la Ley busca es garantizar, en todas las fases de un tratamiento, una adecuada protección de los datos personales.

En este tema, los Lineamientos Generales señalan:

> Artículo 108. El Responsable es corresponsable con el encargado cuando ocurran vulneraciones de seguridad.
>
> Artículo 112. Si el Encargado y subcontratado incumplen con las obligaciones contraídas con el Responsable, se considerarán como Responsables.

Se amplían las responsabilidades tanto del Responsable como del Encargado frente al Titular.

Transferencia

La Ley define a la transferencia como toda comunicación de datos personales dentro o fuera del territorio mexicano realizada a persona distinta del titular, del responsable o del encargado.

Lo que la Ley busca es permitir las comunicaciones seguras de la información personal.

Toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes. (Artículo 66)

Lo dispuesto en el párrafo anterior, no será aplicable en los siguientes casos:

I. Cuando la transferencia sea nacional y se realice entre responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos, o

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

Obligaciones para la realización de Transferencias

La Ley señala que, por regla general, el responsable debe requerir el consentimiento del titular antes de efectuar una transferencia, salvo las excepciones previstas expresamente en dicho ordenamiento.

El responsable podrá realizar transferencias de datos personales sin necesidad de requerir el consentimiento del titular, en los siguientes supuestos (**artículo 70).**

I. Cuando la transferencia esté prevista en esta Ley u otras leyes, convenios o Tratados Internacionales suscritos y ratificados por México;

II. Cuando la transferencia se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;

III. Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia;

IV. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última;

V. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados;

VI. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular;

VII. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;

VIII. Cuando se trate de los casos en los que el responsable no esté obligado a recabar el consentimiento del titular para el tratamiento y transmisión de sus datos personales, conforme a lo dispuesto en el artículo 22 de la presente Ley, o

IX. Cuando la transferencia sea necesaria por razones de seguridad nacional.

El responsable está obligado a formalizar la transferencia mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico.

La Ley señala que el responsable también debe comunicarle al receptor de los datos personales su aviso de privacidad.

Se debe informar puntualmente al titular los casos en los que exista una transferencia.

En relación con las transferencias, los Lineamientos Generales precisan, entre otras cosas, lo siguiente:

> Artículo 113. En casos de transferencias, por regla general, el consentimiento será tácito.
>
> Artículo 112. Cuando se requiera consentimiento expreso, deberá obtenerse de forma previa a la transferencia.
>
> Artículo 117. Responsable puede solicitarle opinión al INAI en caso de transferencias internacionales

Se busca dotar de una protección máxima a los datos personales.

Mecanismos Preventivos de Protección de Datos Personales

Estos mecanismos preventivos coadyuven a robustecer los controles de protección de datos personales implementados. Son instrumentos previstos en la Ley que los responsables podrán utilizar para prevenir o mitigar riesgos en los tratamientos de datos personales.

- Dos tipos:

    A) Evaluación de impacto en la protección de datos personales

    B) Esquemas de mejores prácticas

La Ley recurre a la prevención como un mecanismo de protección de los datos personales.

Evaluación de Impacto en la Protección de Datos Personales

Es el documento mediante el cual aquel responsable que pretende poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, valora los impactos reales respecto de dicho tratamiento, a efecto de identificar y mitigar riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de ese responsable y, en su caso, encargado.

Lo que busca este documento es evitar invasiones innecesarias a la privacidad.

Obligaciones Vinculadas con la Evaluación de Impacto en la Protección de Datos Personales

La Ley señala que el responsable debe realizar y presentar, ante el organismo garante, una evaluación de impacto a la protección de datos personales cuando pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales.

- Plazos:
    - Responsable—30 días hábiles antes de la puesta en operación o modificación.
    - Organismo garante—30 días hábiles para emitir recomendaciones no vinculantes.

El Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales emitirá la normatividad respectiva para la presentación, contenido y valoración de las evaluaciones de impacto en la protección de datos personales.

Se trata de un mecanismo que garantiza la participación conjunta de los responsables y los organismos garantes.

Los Lineamientos Generales, al respecto, señalan:

> Artículo 120. Para que se considere tratamiento intensivo o relevante de datos personales, deberá concurrir cada una de las siguientes condiciones:
>
> - Valor potencial, cuantitativo o cualitativo, de los datos para una tercera persona no autorizada para su posesión; categorías de titulares; volumen total de datos personales tratados; posibilidad de cruzamiento de datos con múltiples plataformas, entre otras.
> - Datos personales sensibles.
> - Transferencias de datos personales dentro o fuera de territorio mexicano.

Tratamientos de datos personales sujetos a un mayor escrutinio.

Los Lineamientos Generales también disponen:

> Artículo 121 — En caso de que se lleven a cabo tratamientos relevantes o intensivos, Responsable podrá designar a un oficial de protección de datos personales, quien será:
>
> - designado en función de sus conocimientos especializados.
> - la persona encargada de asesorar al Comité de Transparencia en materia de datos personales.

Funcionario especializado en materia de protección de datos personales

Esquemas de Mejores Prácticas

La Ley también señala que el responsable puede adoptar—en lo individual o con el acuerdo de otros responsables, encargados u organizaciones—esquemas de mejores prácticas que tienen por objeto:

A) Elevar el nivel de protección de los datos personales.

B) Armonizar el tratamiento de datos personales en un sector específico.

C) Facilitar el ejercicio de los derechos ARCO por parte de los titulares.

D) Facilitar las transferencias de datos personales.

E) Complementar las disposiciones previstas en la normatividad de datos personales.

F) Demostrar ante el organismo garante el cumplimiento de esa normatividad.

El objetivo principal de los esquemas de mejores prácticas es optimizar la seguridad de los datos personales a partir de establecer un estándar de protección de datos personales mayor a las obligaciones previstas en la Ley General.

Obligaciones Vinculadas con los Esquemas de Mejores Prácticas

La Ley establece que el responsable cuando adopte esquemas de mejores prácticas debe someterlos a evaluación y, en su caso, validación y reconocimiento por los organismos garantes. Para ello necesita:

- Cumplir con los parámetros que éstos emitan.
- Notificar ante los organismos garantes dichos esquemas para su evaluación y, en su caso, validación e inscripción en el registro correspondiente.

El organismo garante deberá:

Emitir las Reglas de Operación de los registros

La Ley General no prevé un esquema de acompañamiento en la evaluación, validación y, en su caso, registro de los esquemas de mejores prácticas.

Sobre los Esquemas de Mejores Prácticas, los Lineamientos Generales señalan:

> Artículo 119. El INAI definirá los alcances, objetivos, características y conformación del sistema de mejores prácticas en materia de protección de datos personales, el cual incluirá:
>
> - Un modelo de certificación.
> - Requisitos mínimos que deben satisfacer los esquemas de mejores prácticas, para su evaluación, validación o reconocimiento por el INAI e inscripción en el registro.

Reglas claras para lograr un mejor tratamiento de los datos personales.

CAPÍTULO V

Derechos ARCO, Medios de Impugnación y Facultad de Verificación

Los derechos incluidos en el derecho a la protección de datos personales son los derechos ARCO. Cualquier individuo tiene derecho a:

- **A**cceder a sus datos personales, así como a conocer la información relacionada con las condiciones y generalidades de su tratamiento.
- **R**ectificar sus datos personales. El titular tendrá derecho a solicitar al responsable la rectificación o corrección de sus datos personales, cuando estos resulten ser inexactos, incompletos o no se encuentren actualizados
- **C**ancelar sus datos personales. El titular tendrá derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.
- **O**ponerse al tratamiento de sus datos personales. El titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando:

    I. Aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular, y

    II. Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

La portabilidad de sus datos personales (artículo 57).

Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.

Cuando el titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitir dichos datos

personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales.

El Sistema Nacional establecerá mediante lineamientos los parámetros a considerar para determinar los supuestos en los que se está en presencia de un formato estructurado y comúnmente utilizado, así como las normas técnicas, modalidades y procedimientos para la transferencia de datos personales.

Derechos ARCO

- Pueden ejercerse en cualquier momento por su titular.
- El ejercicio de estos derechos será gratuito—sólo aplican costos de reproducción, certificación o envío de datos personales.
- El ejercicio de uno no es requisito previo ni impide el ejercicio de otro.
- El titular debe presentar ante la Unidad de Transparencia del responsable una solicitud de ejercicio de derechos ARCO, ya sea en escrito libre, formatos, medios electrónicos o cualquier otro medio que determine el organismo garante.

En su solicitud, el titular debe señalar:

A) Su nombre, domicilio o cualquier otro medio para recibir notificaciones.

B) Los documentos que acrediten su identidad o la personalidad e identidad de su representante.

C) De ser posible, el área responsable que trata los datos personales y ante la cual se presenta la solicitud.

D) La descripción clara y precisa de los datos personales respecto de los que busca ejercer alguno de los derechos ARCO, excepto el derecho de acceso.

E) Cualquier otro elemento o documento que facilite la localización de los datos personales.

F) La modalidad de entrega de datos personales que prefiera. Este requisito sólo es aplicable para el ejercicio del derecho de acceso a datos personales.

Si falta alguno de estos requisitos y el responsable no cuenta con elementos para subsanarlos, debe prevenir al titular quien tendrá 5 días para subsanar la omisión.

La Ley señala tiempos muy precisos para el ejercicio y cumplimiento de los derechos ARCO:

- Para presentar solicitud: cualquier momento
- Para responder solicitud sobre la procedencia o improcedencia de los derechos ARCO: 20 días hábiles

  Ampliación—10 días hábiles (por una sola vez y siempre que las circunstancias del caso así lo ameriten).
- Para hacer efectivos los derechos ARCO por el responsable: 15 días hábiles

Los derechos ARCO no son absolutos

No procede su ejercicio cuando:

A) El titular o representante no estén debidamente acreditados.

B) Los datos personales no estén en posesión del responsable.

C) Exista un impedimento legal.

D) Se lesionen los derechos de un tercero.

E) Se obstaculicen actuaciones judiciales o administrativas.

F) Exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición.

G) La cancelación u oposición haya sido previamente realizada.

H) El responsable no sea competente.

I) Sea necesario para proteger intereses jurídicos del titular.

J) Sea necesario para dar cumplimiento a obligaciones legales del titular.

K) Sea necesario para mantener la integridad, estabilidad y permanencia de México.

L) Sea información otorgada al responsable por entidades financieras.

Por su parte, los Lineamientos Generales señalan, en relación con el ejercicio de derechos ARCO, lo siguiente:

Mecanismos y medios para ejercer los derechos ARCO

Artículo 40. El Responsable debe informar a los Titulares los mecanismos, medios y procedimientos habilitados para atender las solicitudes de ejercicio de derechos ARCO.

Facilitar el ejercicio del derecho

Medios de Impugnación Previstos por la Ley

La Ley prevé dos medios de impugnación que buscan garantizar el debido ejercicio del derecho a la protección de datos personales. Estos medios de impugnación son el recurso de revisión y el recurso de inconformidad.

1) Recurso de revisión:

- Se hace valer por el titular ante el organismo garante ;
- Tiene un plazo de 15 días para hacerse valer;
- Procede en los siguientes supuestos:

a) Se clasifiquen indebidamente como confidenciales los datos personales;

b) Se declare su inexistencia;

c) Se declare la incompetencia por el responsable;

d) Se entreguen datos personales incompletos;

e) Se entreguen datos personales que no correspondan a lo solicitado;

f) Se niegue el acceso, rectificación, cancelación u oposición de datos personales;

g) No se dé respuesta al ejercicio de derechos ARCO en los plazos establecidos por la Ley;

h) Se entreguen los datos personales en una modalidad o formato no solicitados o incomprensibles;

i) Se inconforme el titular por los costos de reproducción, envío o tiempos de entrega;

j) Se obstaculice el ejercicio de los derechos ARCO a pesar de ser procedente;

k) No se dé trámite a una solicitud para el ejercicio de derechos ARCO;

l) En los demás casos que dispongan las leyes.

Aspectos Procesales del Recurso de Revisión:

- Una vez admitido el recurso de revisión, el organismo garante podrá buscar una conciliación entre el titular y el responsable conforme al procedimiento previsto en la Ley.
- En caso de no alcanzarse una conciliación, el organismo garante:

  Tiene 40 días hábiles para resolver

  Ampliación—20 días hábiles más (por una sola ocasión)

  Tiene 5 días hábiles para prevenir al titular. La prevención ocurre cuando el escrito del recurso de revisión no cumple con los requisitos señalados y el organismo garante no cuenta con elementos para subsanarlos.

  Titular—5 días hábiles para subsanar omisión

  Tiene que aplicar la suplencia de la queja a favor del titular.

Las resoluciones de los organismos garantes en el recurso de revisión pueden:

A) Sobreseer el recurso de revisión por improcedente.

B) Confirmar la respuesta del responsable.

C) Revocar o modificar la respuesta del responsable.

D) Ordenar la entrega de los datos personales.

E) Establecer los plazos y términos para su cumplimiento.

F) Dar vista al órgano interno de control, contraloría o instancia equivalente en caso de que se adviertan presuntas responsabilidades administrativas.

G) Ser impugnadas por los titulares ante el Poder Judicial de la Federación en el orden federal.

En el caso de los organismos garantes estatales, ser impugnadas ante el Poder Judicial de la entidad federativa que corresponda, o bien, ante el INAI.

Las resoluciones emitidas por los organismos garantes son inatacables y definitivas para el responsable

2) Recurso de inconformidad:

- Procede contra una resolución emitida por un organismo garante estatal de un recurso de revisión.
- Se hace valer por el titular ante el organismo garante que emitió la resolución, o bien, ante el INAI. ¿Plazo? 15 días hábiles.
- Si se presenta el recurso de inconformidad ante el organismo garante se debe remitir al INAI junto con las constancias del procedimiento;
- Procede en los siguientes supuestos:

  a) Se clasifiquen indebidamente los datos personales;

  b) Se declare su inexistencia;

  c) Se declare la negativa de datos personales

Cabe mencionar, que cuando la Ley General alude al organismo garante (estatal) es solamente para la presentación del recurso de inconformidad, lo cual de ninguna manera significa que se haga valer ante dicho organismo. La competencia exclusiva para sustanciarlo y emitir resolución es del INAI

Aspectos procesales del recurso de inconformidad:

El INAI:

- Tiene 30 días hábiles para resolver

  Ampliación—30 días hábiles más (por una sola ocasión)

- Tiene 5 días hábiles para prevenir al titular

  Titular—15 días hábiles para subsanar omisión

- Tiene que aplicar la suplencia de la queja a favor del titular
- Tiene que poner a disposición de las partes las actuaciones tras concluirse la etapa probatoria

  Titular y organismo garante—5 días hábiles para alegatos

Las resoluciones del INAI dictadas en un recurso de inconformidad pueden:

A) Sobreseer el recurso de inconformidad por improcedente.

B) Confirmar la resolución del organismo garante.

C) Revocar o modificar la resolución del organismo garante, quién emitirá una nueva resolución con los parámetros indicados.

D) Ordenar la entrega de los datos personales, en caso de omisión del responsable.

E) Establecer los plazos y términos para su cumplimiento así como los procedimientos para su ejecución.

F) Dar vista al organo interno de control o instancia competente en caso de que se adviertan presuntas responsabilidades administrativas.

G) Ser impugnadas por los titulares ante el Poder Judicial de la Federación.

Aspectos importantes:

En caso de que la resolución del INAI modifique o revoque la resolución del organismo garante estatal, éste debe emitir un nuevo fallo atendiendo a los lineamientos que se fijaron al resolver el recurso de inconformidad, dentro del plazo de quince días hábiles, de conformidad con el artículo 127 de la Ley General.

Corresponde al organismo garante estatal realizar el seguimiento y vigilancia del cumplimiento de la nueva resolución que emita, en términos del artículo 128 de la Ley General.

Las resoluciones que emite el INAI son vinculantes, definitivas e inatacables para los responsables y organismos garantes estatales.

Los Lineamientos Generales han incorporado ciertos principios en materia procesal, los cuales son fundamentales para garantizarles a los ciudadanos un debido proceso.

Artículo 123. Principios que deberán observarse en la sustanciación de los recursos de revisión y de inconformidad:

- Legalidad
- Certeza jurídica
- Independencia
- Imparcialidad
- Eficacia
- Objetividad
- Profesionalismo
- Transparencia

Principios que garantizan una equidad procesal adecuada.

Medidas de Supervisión Previstas por la Ley

1) Facultad de verificación:

El INAI y organismos garantes tienen funciones de vigilancia y verificación del cumplimiento de la Ley o leyes estatales en la materia, según corresponda. Para cumplir con esta responsabilidad, pueden hacer uso de la facultad de verificación.

- La verificación puede iniciarse:

  De oficio—INAI u organismo garante cuenta con indicios que hagan presumir la existencia de violaciones a las leyes de datos personales.

  Denuncia—titular considera que el responsable ha cometido actos contrarios a las Ley o las leyes estatales en la materia, según corresponda, que los afectan.

  Cualquier persona tiene conocimiento de presuntos incumplimientos a la Ley.

Previo a la verificación respectiva el Instituto o los organismos garantes estatales, según corresponda, podrán desarrollar investigaciones previas, con el fin de contar con elementos para fundar y motivar el acuerdo de inicio respetivo

El procedimiento de verificación.

- Tiene que iniciar con una orden escrita que funde y motive su procedencia.
- Tiene una duración máxima de 50 días hábiles.
- Puede requerirle al responsable información vinculada con las presuntas violaciones a la Ley o las leyes estatales en la materia, según corresponda, y/o visitarlo en donde se encuentren sus bases de datos.
- Puede hacer uso de medidas cautelares en caso de daño inminente o irreparable en materia de protección de datos personales.
- Concluye con la resolución que emita el INAI o el organismo garante, la cual establecerá las medidas que deberá adoptar el responsable.

2) Auditorías voluntarias:

Se tratan de procedimientos de verificación iniciados voluntariamente por los sujetos obligados.

Las auditorías voluntarias tienen por objeto verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos de implementación para el cumplimiento de las disposiciones previstas en la Ley General o las leyes estatales en la materia, según corresponda.

El informe de auditoría debe dictaminar sobre la adecuación de las mismas y los controles implementados por el responsable, identificar deficiencias, así como proponer acciones correctivas complementarias, o bien, recomendaciones que en su caso correspondan.

Lo anterior, sin dejar de señalar que este tipo de mecanismos inician a instancia del responsable y no es propiamente un procedimiento de verificación a que se refiere en la Ley General.

En relación con el procedimiento de verificación, los Lineamientos Generales han establecido, entre otras cuestiones, lo siguiente:

En el ejercicio de las facultades de investigación y verificación:

- El personal del INAI tiene fe pública (Artículo 182).

- No tiene lugar el ejercicio de dichas facultades cuando proceda el recurso de revisión o el recurso de inconformidad.

Lo que se busca es verificar adecuadamente el cumplimiento de la ley.

Los Lineamientos Generales también han desarrollado, con un mayor nivel de detalle, la fase de investigación previa. Ésta la inicia el INAI con el objetivo de contar con mayores elementos que lo lleven a determinar si, efectivamente, existe algún incumplimiento de la Ley. De acuerdo con el artículo 189 de los referidos Lineamientos, la investigación previa puede iniciar:

- de oficio
- a petición de parte

Vigilancia permanente sobre quienes tratan los datos personales

De acuerdo con los Lineamientos Generales, al concluir la investigación previa, podría suceder lo siguiente:

Artículo 198. El INAI podría emitir un acuerdo de:

- Determinación: no hay elementos suficientes para acreditar un incumplimiento de la Ley o Lineamientos

- Inicio del procedimiento de verificación: existen elementos suficientes para acreditar un incumplimiento de la Ley o los Lineamientos

Se busca averiguar antes de sancionar.

En el ejercicio de la facultad de verificación, el INAI y los organismos garantes pueden establecer medidas cautelares. Los Lineamientos Generales señalan cuáles podrían ser dichas medidas:

Artículo 210

- Cese inmediato del tratamiento.
- Realización de acciones cuya omisión hayan causado o puedan causar un daño.
- Bloqueo de datos.
- Cualquier otra medida, de acción u omisión dirigida a proteger el derecho a la protección de datos personales.

Medidas que buscan salvaguardar la privacidad y los datos personales.

Medidas de Apremio

Para asegurar el cumplimiento de sus resoluciones, el INAI y los organismos garantes pueden imponer las siguientes medidas de apremio:

- Amonestación Pública;
- Multa—Equivalente a la cantidad de 150 hasta 1,500 veces el valor diario de la Unidad de Medida y Actualización. ¿Reincidencia? Multa hasta por el doble.

Auxiliares en el cumplimiento no espontáneo de las resoluciones dictadas por los organismos garantes.

Las medidas de apremio:

- Deben aplicarse e implementarse en un plazo máximo de 15 días hábiles contados a partir de que el infractor sea notificado.
- Deben considerar la condición económica del infractor, entre otros factores.
- Pueden ser impugnadas ante el Poder Judicial de la Federación o el Poder Judicial correspondiente en las Entidades Federativas.

Se trata de medidas indispensables en el cumplimiento de la Ley.

Para la aplicación de las medidas de apremio, los Lineamientos Generales han precisado—para el caso del INAI—la forma como habrán de imponerse:

> Artículo 235. El Pleno del INAI determinará e impondrá las medidas de apremio.
>
> Artículo 234. La Secretaría Técnica del Pleno, a través de la Dirección General de Cumplimientos y Responsabilidades, calificará las medidas a ser impuestas.
>
> Artículo 236. La Secretaría Técnica del Pleno, a través de la Dirección General de Cumplimientos y Responsabilidades, notificará, gestionará y ejecutará las medidas de apremio.

Se busca que las resoluciones de los organismos garantes sean de cumplimiento forzoso para todos los sujetos obligados por la Ley.

Los Lineamientos Generales también señalan algunos criterios que habrán de seguirse para determinar las medidas de apremio:

> Artículo 237. Criterios para determinar medidas de apremio:
>
> - Daño causado.
> - Indicios de intencionalidad.
> - Duración del incumplimiento.
> - Afectación al ejercicio de atribuciones del INAI.
> - Condición económica del infractor.
> - Reincidencia.

No son medidas únicas, sino diferenciadas en función del caso concreto.

Sanciones

La Ley prevé diversas sanciones que en sentido estricto se trata de responsabilidades administrativas y sus sanciones correspondientes. Ante su incumplimiento, algunas reglas que deben tomarse en cuenta son las siguientes:

- Las sanciones de carácter económico no pueden cubrirse con recursos públicos.
- Ni el INAI ni los órganos garantes imponen sanciones. Los órganos internos de control, contraloría o instancias equivalentes son las instancias competentes para conocer las presuntas responsabilidades administrativas derivadas de la Ley General y las leyes estatales en la materia e imponer las sanciones que correspondan.
- INAI y órganos garantes pueden dar vista a las autoridades competentes (p. ej. Órgano Interno de Control) para que impongan dichas sanciones. Los organismos garantes deben remitir a los órganos internos de control, contraloría o instancia equivalente la denuncia correspondiente junto con un expediente.
- Las infracciones a la Ley también pueden dar lugar a sanciones del orden civil, penal o de cualquier otro tipo.

Las sanciones son garantías de no repetición de las violaciones a la Ley.