

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

Curso de Capacitación

Otoño 2017

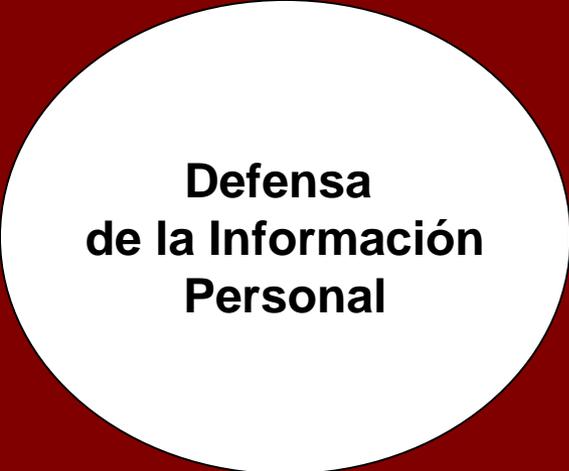


Panorama General

Contenido

- El Derecho a la Protección de Datos Personales en México
- Marco Jurídico Nacional e Internacional del Derecho a la Protección de Datos Personales
- Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados
- Principios, Deberes y Responsabilidades de los Sujetos Obligados por la Ley
- Derechos ARCO, Medios de Impugnación y Facultad de Verificación
- Taller de Casos Prácticos

El Derecho a la Protección de Datos Personales en México



**Defensa
de la Información
Personal**

Protección de Datos Personales

- Surge con la Sociedad de la Información en el mundo industrializado durante los años 70.
- Busca proteger la privacidad, dignidad y autonomía de las personas.
- Facilita el tratamiento de la información personal que hacen las organizaciones públicas y privadas.

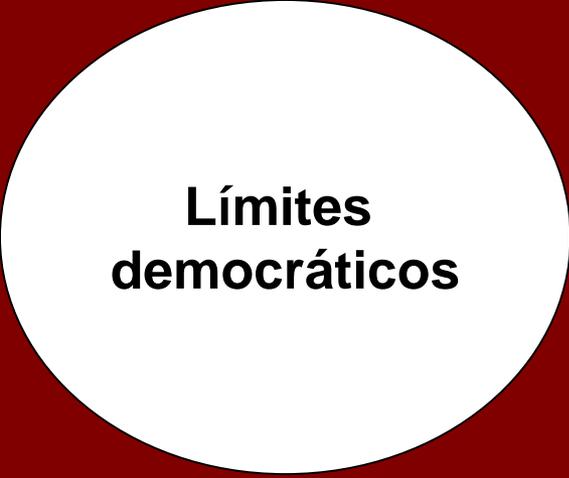
Política pública adoptada frente al creciente uso de las tecnologías de la información

**Poder a los
ciudadanos**

Derecho a la Protección de Datos Personales

- Ha venido surgiendo en diversos países (incluido México) como un derecho autónomo e independiente del derecho a la privacidad.
- Le confiere a las personas control sobre su información personal.
- Faculta al individuo a decidir quién, cómo, cuándo y hasta que punto utilizará su información personal.

Protege la dimensión informativa de nuestra vida privada



**Límites
democráticos**

Derecho a la Protección de Datos Personales (2)

- No es derecho absoluto.
- Sólo admite aquellas restricciones *prescritas en ley* que resulten razonables en una sociedad democrática: seguridad nacional, seguridad pública, preservación de la salud, prevención del delito y la protección de los derechos y libertades de los demás.

Su ejercicio se limita sólo por excepción

**Compleja
articulación**

Derecho a la Privacidad

Es el derecho que todo individuo tiene a separar aspectos de su vida privada del escrutinio público.

privacidad: “la entiendes cuando la pierdes”

**Doble
vertiente**

Componentes

- 1) Derecho a aislarte (Warren & Brandeis, 1890):
Implica poder escudarnos física y psicológicamente de los demás.
- 2) Derecho a controlar la información de uno mismo incluso después de divulgarse (Westin, 1967):
Implica poder participar activamente en sociedad.

Aspectos distintos pero intrínsecamente vinculados

**Protección de la
libertad y autonomía
personales**

Distinción

Derecho a la Privacidad

Protege al individuo de intromisiones arbitrarias o ilegales en su vida privada.

Derecho a la Protección de Datos Personales

Le confiere al individuo la facultad de participar en el tratamiento que otros hacen de sus datos personales.

**Protección de la
libertad y autonomía
personales**

Distinción (2)

Derecho a la Privacidad

Protege diversas áreas relacionadas con la vida privada del individuo:

- Domicilio
- Comunicaciones
- Familia
- Cuerpo
- Información personal

Derecho a la Protección de Datos Personales

Protege el manejo justo de los datos personales:

- Acceso
- Rectificación
- Cancelación
- Oposición
- Medidas de Seguridad

Derechos íntimamente relacionados

**Escrutinio público
del gobierno**

Derecho de Acceso a la Información Pública

Derecho que todo individuo tiene a acceder a la información que obra en los archivos públicos.

*Garantiza la participación democrática de los
ciudadanos*

**Fundamentalmente
democráticos**

Diferencia

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 no se encuentre clasificada como reservada o confidencial.

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, rectificarlos, cancelarlos y oponerse a que sean tratados.

**Fundamentalmente
democráticos**

Diferencia (2)

Derecho a la Protección de
Datos Personales

Suele limitar el ejercicio del
derecho de acceso a la
Información pública.

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.

Derechos distintos pero relacionados

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

**Protección
expresa en la
constitución**

Fundamento Constitucional

Artículo 16 Constitucional:

Se reforma en 2009 para darle status constitucional al *Derecho a la protección de los datos personales*. También se reconocen los derechos de acceso, rectificación y cancelación de los datos personales, así como el derecho a manifestar su oposición (Derechos ARCO)

*Protección de la privacidad desde el punto de vista
informativo*

Criterios de regulación

Fundamento Constitucional (2)

Artículo 16 Constitucional:

“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 será determinado por la ley

Pluralidad Legislativa

Fundamentos Legales

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley Federal de Protección de Datos Personales en Posesión de Particulares.
- Leyes estatales de protección de datos personales.

Mismo derecho pero regulado por leyes distintas

Universales y Regionales

Instrumentos Internacionales de Protección de Datos Personales

- 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).

Décadas distintas

Instrumentos Internacionales de Protección de Datos Personales (2)

- 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).

Actualización reciente

Instrumentos Internacionales de Protección de Datos Personales (3)

- 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: 2018.
- Red Iberoamericana de Protección de Datos Personales—Estándares de protección de datos personales para los Estados iberoamericanos (2017).

Jurídicamente no vinculantes para México

Ampliación normativa

Reforma Constitucional en Derechos Humanos

- Publicada en el Diario Oficial de la Federación el 10.06.2011.
- Incorporó a la Constitución mexicana los derechos humanos reconocidos en los tratados internacionales suscritos por México.
- Introdujo dos herramientas hermenéuticas:

Interpretación conforme

Principio pro persona

Nuevo paradigma de protección de derechos humanos

Mandato constitucional

Reforma Constitucional en Derechos Humanos (2)

- *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.

Expansión de derechos y libertades fundamentales

Fuentes internacionales

Implicaciones de la Reforma Constitucional en Derechos Humanos

- Derecho a la privacidad incorporado al texto de la Constitución:
 - Art. 11 Convención Americana de Derechos Humanos
 - Art. 17 Pacto Internacional de Derechos Civiles y Políticos
- Jurisprudencia de la Corte Interamericana de Derechos Humanos:
 - SCJN: jurídicamente vinculante para México
(Contradicción de tesis 293/2011)

Aliado en la protección de los datos personales

Restricciones legítimas

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:

derecho a la privacidad

derecho a la no discriminación

derecho de asociación

Tratamientos que respeten la dignidad humana

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

**Autoridad
federal y local**

Competencia en Materia de
Datos Personales

Federación

Sector público

Sector privado

Entidades

Federativas

Sector público

Jurisdicción dual

**Facultades
concurrentes**

Distribución de Competencias en el Sector Público

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

**Facultades
para
Autoridades
Federales**

**Facultades
para
Entidades
Federativas**

Una ley marco con estándares mínimos

**Universo
amplio**

Sujetos Obligados

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

Fideicomisos

Fondos

**Órganos
Autónomos**

Municipios

Partidos Políticos

**Federación:
Ejecutivo
Legislativo
Judicial**

**Entidades Federativas:
Ejecutivo
Legislativo
Judicial**

Personas físicas, morales y sindicatos quedan excluidos

Información personal

Conceptos Clave

Datos personales

Cualquier información concerniente a una persona física identificada o identificable.

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.

Refieren aspectos de la vida privada

Procesamiento de datos

Conceptos Clave (2)

Tratamiento

Operación manual o automatizada aplicada a los datos personales, p. ej. obtención, uso, registro, organización, conservación, difusión, transferencia.

Transferencia

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

Actividades propias en la sociedad de la información

Derechos y obligaciones distintos

Figuras Clave

Titular

Persona física a quien corresponden los datos personales

Responsable

Los sujetos obligados por la LGPDPPSO.

Encargado

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

Partes en las relaciones de tratamiento de datos

Protección multi-instancial

Rol de las Autoridades

Responsables

Son instancias públicas, no personas físicas.
Tienen el poder de decisión respecto al tratamiento de datos personales: uso, finalidades, tipo de datos, Reciben solicitudes para ejercicio de derechos ARCO.

Órganos garantes

INAI e Institutos locales en las entidades federativas.
Tienen autonomía constitucional—Arts. 6, 116-VIII.
Resuelven recursos de revisión x ejercicio der ARCO.

INAI

Interpreta la LGPDPSO en el ámbito administrativo.
Facultad de atracción de recursos de revisión.
Resuelve recursos de inconformidad vs resoluciones de órganos garantes.

Funciones distintas pero complementarias

Primer contacto

Responsables

Deben contar con:

Comité de
Transparencia

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

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.

Asesora a las áreas adscritas sobre datos personales

Obligados en garantizar el ejercicio de derechos ARCO

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

Responsabilidades

Principios de Protección de Datos Personales

Principio

Deber

Principio de licitud
(Art. 17)

Identificar en la normatividad las facultades que los autorizan a tratar datos personales.

Principio de finalidad
(Art. 18)

Determinar el uso concreto que se le va a dar a los datos personales ¿cambios? requiere consentimiento.

Principio de consentimiento
(Arts. 20, 21, 22)

Recolectar información personal sólo con el conocimiento y consentimiento del Titular (salvo excepciones).

Responsabilidades

Principios de Protección de Datos Personales (2)

Principio	Deber
Principio de lealtad (Art. 19)	No actuar de manera engañosa o fraudulenta—sin dolo, error o mala fe.
Principio de calidad (Arts. 23 y 24)	Asegurar que los datos personales se mantengan exactos, completos y actualizados.
Principio de proporcionalidad (Art. 25)	Recabar y utilizar sólo aquellos datos que resulten estrictamente necesarios para el fin propuesto.

Responsabilidades

Principios de Protección de Datos Personales (3)

Principio

Deber

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

Informar a los Titulares todo lo relacionado con el tratamiento de sus datos personales mediante un “Aviso de Privacidad”.

Principio de responsabilidad
(Arts. 29 y 30)

Implementar mecanismos que acrediten el cumplimiento de los principios, deberes y obligaciones previstos en la LGPDPSO.

Principios que garantizan un manejo justo de la información

**Enterar a los
ciudadanos**

Aviso de Privacidad

- Documento que informa a los titulares todos lo referente al tratamiento de sus datos personales.
- Puede ser difundido a través de medios electrónicos y físicos.
- Dos tipos de Aviso de Privacidad:
 - Simplificado
 - Integral

Comunicación esencial

Aviso de Privacidad (2)

Debe contener la siguiente información:

Simplificado

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.

Sitio para consultar el Aviso de Privacidad Integral.

Funciones distintas pero complementarias

Comunicación detallada

Aviso de Privacidad (3)

Debe contener la información del Simplificado y:

Integral

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.

Respeto absoluto a la autonomía de los individuos

Salvaguardias de la información

Medidas de Seguridad

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 los datos.

Tipos de Medidas de Seguridad:

- Administrativas
- Físicas
- Técnicas

Salvaguardias de la información

Medidas de Seguridad (2)

Administrativas

- Políticas y procedimientos para:
- a) la gestión, soporte y revisión de la seguridad de la información;
 - b) la identificación, clasificación y borrado de la información.

Físicas

- Políticas y procedimientos para:
- a) Prevenir el acceso no autorizado a la organización, instalaciones físicas, áreas críticas, recursos e info;
 - b) Prevenir daño o interferencia a instalaciones físicas áreas críticas de la organización, recursos e info;
 - 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.

Salvaguardias de la Información

Medidas de Seguridad (3)

Técnicas

Políticas y procedimientos para:

- a) asegurar que el acceso a las bases de datos sea por usuarios identificados y autorizados;
- b) generar incentivos para que los usuarios cumplan con sus funciones;
- c) revisar la configuración de seguridad del software y hardware;
- d) gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales

Salvaguardias de la Información

Medidas de Seguridad (4)

Otras

- 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 la seguridad ya ocurridas;
- B) Implementar un Sistema de Gestión de la seguridad de los datos personales;
- C) Elaborar un Documento de Seguridad que describa los elementos indispensables que permitirán asegurar un cuidado adecuado de los datos personales.

Riesgos importantes

Vulneración a la Seguridad de los Datos Personales (*Data Breach*)

- 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.
- Podría afectar los derechos patrimoniales o morales de los titulares

Supuestos:

- 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.

Fugas que comprometen la privacidad de los individuos

Obligaciones puntuales

Obligaciones por la Vulneración a la Seguridad de los Datos Personales

- Responsable deberá informar sin dilación alguna al titular de los datos personales y al organismo garante en cuanto se confirme que ha ocurrido una vulneración.
- Deber informar:
 - A) La naturaleza del incidente.
 - B) Los datos personales comprometidos.
 - C) Las recomendaciones que el titular puede adoptar para protegerse.
 - D) La acciones correctivas realizadas de forma inmediata
 - E) Los medios donde podrá obtener más información al respecto.

Registro

Obligaciones por la Vulneración a la Seguridad de los Datos Personales (2)

- Responsable deberá llevar una bitácora en la que describa las vulneraciones de seguridad ocurridas en su organización.
- Deberá registrar:
 - A) Fecha en que ocurrió la vulneración;
 - B) Motivo;
 - C) Acciones correctivas implementadas, de forma inmediata y definitiva.

No ocultar sino informar

**Protección
garantizada**

Obligaciones de Confidencialidad

- Responsable deberá 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 dicho tratamiento.
- Ejemplos:
 - A) Suscripción de cláusulas de confidencialidad con quienes intervengan en el tratamiento
 - B) Sanciones por la revelación no autorizada de datos personales

Responsabilidad en el manejo de la información personal

Figura auxiliar

“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
- No tiene poder de decisión sobre el alcance y contenido del tratamiento de los datos personales
- Debe limitar sus actuaciones a lo que diga el Responsable

Un tercero con responsabilidad

Deberes puntales

Obligaciones en el Caso de “Encargados”

- Responsable deberá formalizar su relación con el Encargado a través de un contrato o cualquier otro instrumento jurídico 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.

Deberes puntuales

Obligaciones en el Caso de “Encargados” (2)

- Responsable deberá autorizar expresamente los casos en los que el Encargado podría subcontratar los servicios de tratamiento de datos personales.
- Responsable 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.
- Responsable no estará obligado a informar a los titulares sobre aquellas comunicaciones de datos personales que les haga a los Encargados.

Garantizar la protección de los datos personales

Flujo de datos

“Transferencia”

Es toda comunicación de datos personales dentro o fuera del territorio mexicano realizada a persona distinta del Titular, del Responsable o del Encargado.

Intercambio de información

Salidas Autorizadas

Obligaciones en el Caso de “Transferencias”

- Responsable deberá requerir el consentimiento del Titular salvo excepciones.
- Responsable deberá formalizar la transferencia mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico.
Excepciones:
 - a) transferencia nacional—autorizada por ley .
 - b) transferencia internacional—prevista en tratados o solicitud de autoridad extranjera.
- Responsable deberá comunicarle al receptor de los datos personales su Aviso de Privacidad.

Información puntual al titular de los datos

Herramientas útiles

Mecanismos Preventivos

- Instrumentos previstos en la LGPDPPSO que los Responsables podrán usar 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

Previsión como mecanismo de protección

Protección Anticipada

Evaluación de Impacto en la Protección de Datos Personales

Documento mediante el cual el 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.

Evitar invasiones innecesarias a la privacidad

Plazos precisos

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

- Responsable debe realizar y presentar ante el organismo garante una Evaluación de Impacto 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.
 - Órgano garante—30 días hábiles para emitir recomendaciones no vinculantes.

Participación conjunta

Protección Ampliada

Esquemas de Mejores Prácticas

- Responsable puede adoptar—en lo individual o con el acuerdo de otros Responsables, Encargados u organizaciones—esquemas de mejores prácticas encaminados a cumplir con las obligaciones que la Ley le impone.
- 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;
 - F) Demostrar ante el órgano garante el cumplimiento de esa normatividad.

Optimizar la seguridad de los datos personales

Figura Regulada

Obligaciones Vinculadas con los Esquemas de Mejores Prácticas

- Responsable deberá obtener la validación o reconocimiento de sus Esquemas de Mejores Prácticas por los organismos garantes.

Necesita:

Cumplir con los parámetros que éstos emitan.

Notificar ante los organismos garantes dichos esquemas para su validación e inscripción en el registro.

- Organismo garante deberá emitir las Reglas de Operación de los registros.

Acompañamiento de los órganos garantes

Derechos ARCO, Medios de Impugnación y Facultad de Verificación

Pluralidad

Derechos incluidos en el Derecho a la Protección de Datos Personales (derechos ARCO)

Cualquier individuo tiene derecho a:

- **A**cceder a sus datos personales
- **R**ectificar sus datos personales
- **C**ancelar sus datos personales
- **O**ponerse al tratamiento de sus datos personales
- La portabilidad de sus datos personales

Ejercicio fácil

Derechos ARCO

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

Reglas claras

Derechos ARCO (2)

En su solicitud, el Titular deberá 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 der. 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.

Si falta alguno de estos requisitos, Responsable debe subsanarlos. Si no puede, previene; Titular, tiene 5 días para subsanar la omisión.

Tiempos precisos

Derechos ARCO (3)

Plazos:

- Para presentar solicitud cualquier momento
- Para responder solicitud 20 días hábiles
Ampliación—10 días hábiles
- Para hacer efectivos los derechos ARCO por el Responsable 15 días hábiles

**No son
absolutos**

Derechos ARCO (4)

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.

Derecho a inconformarse

Recurso de Revisión

- Se hace valer por el Titular ante la Unidad de Transparencia del Responsable o 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 los solicitado;
 - f) Se niegue el acceso, rectificación, cancelación u oposición de datos personales;

Derecho a inconformarse

Recurso de Revisión (2)

Procede en los siguientes supuestos (cont.):

- g) No se de 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 der. ARCO a pesar de ser procedente;
- k) No se de trámite a una solicitud para el ejercicio de der. ARCO;
- f) En los demás casos que dispongan las leyes.

**Procedimiento
claro**

Recurso de Revisión (3)

Aspectos Procesales

- Una vez admitido, organismo garante debe 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
 - Tiene 5 días hábiles para prevenir al Titular
 - Titular—5 días hábiles para subsanar omisión
 - Tiene que aplicar la suplencia de la queja

Posibilidades diversas

Recurso de Revisión (4)

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 en caso de responsabilidades.
- G) Ser impugnadas por los Titulares ante el Poder Judicial de la Federación.

Segunda Instancia

Recurso de Inconformidad

- Procede contra una resolución emitida por un organismo garante estatal en 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;
- Organismo garante debe remitir el Recurso 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

Audiencia a ambas Partes

Recurso de Inconformidad (2)

Aspectos Procesales

EL INAI:

- Tiene 30 días hábiles para resolver
Ampliación—30 días hábiles más
- Tiene 5 días hábiles para prevenir al Titular
Titular—15 días hábiles para subsanar omisión
- Tiene que aplicar la suplencia de la queja
- Tiene que poner a disposición de las partes las actuaciones tras concluirse la etapa probatoria
Titular y organismo garante—5 días hábiles para alegatos

Distintas Posibilidades

Recurso de Inconformidad (3)

Resoluciones del INAI 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 Órgano Interno de Control o instancia competente en caso de responsabilidades.
- G) Ser impugnadas por los Titulares ante el Poder Judicial de la Federación.

Supervisión Necesaria

Facultad de Verificación

- INAI y organismos garantes tienen funciones de vigilancia y verificación del cumplimiento de la Ley General y leyes derivadas de ésta.
- 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 que los afectan.
Cualquier persona tiene conocimiento de presuntos incumplimientos a la Ley.

Estricto apego a la legalidad

Facultad de Verificación (2)

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 y visitarlo en donde estén 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.
- Puede iniciarse voluntariamente—Auditorias

Cumplimiento eficaz

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

Cumplimiento eficaz

Medidas de Apremio (2)

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

Indispensables en el cumplimiento de la Ley

Censuras válidas

Sanciones

- La LGPDPPSO prevé diversas sanciones ante su incumplimiento.
- Las sanciones de carácter económico no pueden cubrirse con recursos públicos.
- Ni el INAI ni los órganos garantes imponen sanciones.
- INAI y órganos garantes pueden dar vista a las autoridades competentes (p. ej. Órgano Interno de Control) para que impongan dichas sanciones.
- Las infracciones a la LGPDPPSO también pueden dar lugar a sanciones del orden civil, penal o de cualquier otro tipo.

Garantías de no repetición

¡Gracias!