



GOBIERNO DE
MÉXICO

EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA



TECNOLÓGICO
NACIONAL DE MÉXICO



Instituto **Tecnológico**
de Aguascalientes

INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

AUDITORÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

UNIDAD 2:

EL MARCO JURÍDICO DE LA AUDITORÍA INFORMÁTICA

TEMA 2:

TABLA COMPARATIVA LAS REGULACIONES ESTABLECIDAS EN MÉXICO Y OTROS PAÍSES

Lic. Juan Carlos
Sánchez Gaytán

Participante:
Flores Zavala Jesús Uriel
Semestre: 08

Semestre: enero-junio de 2025

Aguascalientes, Ags. 19 de marzo de 2025



Regulaciones establecidas en México, la Unión Europea y Suiza para la protección de los datos en medios electrónicos.

México: Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP)

En la era digital, la información es uno de los activos más valiosos que poseemos. Desde nuestras interacciones en redes sociales hasta nuestras compras en línea, generamos constantemente datos que pueden ser utilizados para diversos fines. En este contexto, la protección de datos personales se ha convertido en una prioridad global. México no es la excepción y ha desarrollado un marco normativo robusto para garantizar que nuestros datos estén protegidos. [1]

La LFPDPPP, publicada en el Diario Oficial de la Federación el 5 de julio de 2010, tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

El tratamiento de datos personales implica la obtención, uso, divulgación o almacenamiento de datos personales. El uso de los datos personales abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia, comunicación o disposición de datos personales.

La autodeterminación informativa implica el derecho de las personas para decidir, de manera libre e informada, sobre el uso de la información que les pertenece.

Principios y derechos de protección de datos personales

Tanto la LFPDPPP como la LGPDPPSO contemplan que los responsables del tratamiento de datos personales deberán observar los siguientes principios:

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

Dichos principios se traducen en obligaciones concretas para los responsables del tratamiento.

Derechos

El artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, reconoce el derecho que tienen los ciudadanos para acceder, rectificar y



cancelar sus datos personales, así como oponerse a su uso. A estos derechos se les conoce como derechos ARCO, y se encuentran reconocidos tanto en la LFPDPPP como en la LGPDPPSO.

Autoridad de protección de datos en México

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Naturaleza jurídica: El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales también conocido como INAI, es el organismo constitucional autónomo encargado de que se cumplan y respeten dos derechos fundamentales: el de acceso a la información pública y el de protección de datos personales.

Funciones: En relación con el derecho a la protección de datos personales, el INAI es el organismo encargado de garantizar el uso adecuado de los datos personales, así como el ejercicio y tutela de los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) que toda persona tiene con respecto a su información. [2]

¿Cuáles son las sanciones por infringir el LFPDPPP?

El apercibimiento para que el responsable de datos personales lleve a cabo los actos solicitados por el titular, en los términos previstos por esta Ley, tratándose del incumplimiento con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales.

Multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal, en los casos de actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales.

Multa de 200 a 320,000 días de salario mínimo vigente en el Distrito Federal, en los casos de Incumplir el deber de confidencialidad, así como crear bases de datos en contravención a lo dispuesto en la Ley. [3]

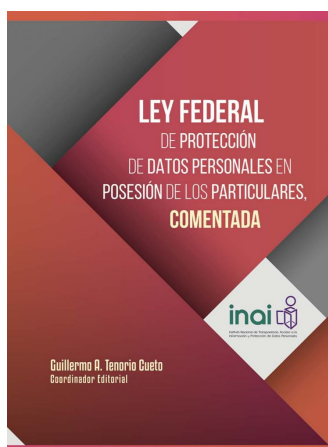


Figura 1 Documento oficial del INAI sobre la ley en particulares



Reglamento General de Protección de Datos (Unión Europea)

RGPD son las siglas en inglés del Reglamento General de Protección de Datos. Se trata de una ley de protección de datos con disposiciones que obligan a las empresas y organizaciones a proteger los datos y la privacidad de los ciudadanos de la UE en las transacciones que se realizan en los estados miembro. También regula el modo en que las empresas exportan los datos personales fuera de la UE. Muchos lo consideran el estándar de protección de datos más fuerte del mundo, ya que mejora la forma en que las personas pueden acceder a su información y los límites que las organizaciones deben cumplir al tratar los datos personales.

El RGPD exige a las empresas y organizaciones que realizan un tratamiento de datos a gran escala y un seguimiento de los interesados que cuenten con un responsable de la protección de datos (DPO). El DPO se convierte en una figura responsable de la gobernanza de los datos de la empresa y del cumplimiento.

¿Cuál es el propósito del RGPD?

El RGPD existe debido a la preocupación pública por la privacidad. Sustituyó a la Directiva de Protección de Datos de la UE de 1995, promulgada mucho antes de que Internet se convirtiera en un moderno centro de negocios en línea. Por lo tanto, era necesario para reemplazar la anticuada directiva que no abordaba la forma en que las empresas recogían, transferían y almacenaban los datos.

En la actualidad, el RGPD protege a la población de la UE y sus datos para garantizar que las organizaciones que recopilan y almacenan datos lo hacen de forma responsable. En el reglamento se ordena el mantenimiento seguro de los datos personales y se requiere que las organizaciones los protejan contra el procesamiento no autorizado o ilegal, daños, destrucción y pérdida accidental. Esto incluye muchas actividades relacionadas con el ransomware y el malware.
[4]

¿Qué derechos tienen los sujetos de datos en virtud del RGPD?

El RGPD define al sujeto de datos como "una persona física identificada o identificable." Los sujetos de datos tienen los siguientes derechos:

- Derecho a ser informado: los sujetos de datos deben recibir información fácil de entender sobre cómo se recopilan y tratan sus datos personales
- Derecho a la portabilidad de los datos: los sujetos de datos pueden transferir sus datos de un controlador de datos a otro
- Derecho de acceso: los sujetos de datos tienen derecho a obtener una copia de los datos personales recopilados
- Derecho de rectificación: los sujetos de datos pueden corregir los datos inexactos que haya sobre ellos
- Derecho de supresión: los sujetos de datos pueden solicitar la supresión de sus datos (también llamado derecho al olvido)



- Derecho a limitar el procesamiento: en determinadas circunstancias, los sujetos de datos pueden limitar la forma en que se procesan sus datos personales
- Derecho a oponerse: los sujetos de datos tienen derecho a oponerse al procesamiento de sus datos personales y, en determinadas circunstancias, el controlador de datos o el procesador de datos estarán obligados a cumplir con la oposición del sujeto de datos
- Derecho a oponerse al procesamiento automatizado: los sujetos de datos pueden oponerse a una decisión que les afecte jurídicamente y que esté basada únicamente en un procesamiento de datos automatizado

¿Cuáles son las sanciones por infringir el RGPD?

El RGPD describe las multas que se impondrán a las empresas que infrinjan sus políticas.

El RGPD establece dos niveles de multas, cada uno de los cuales corresponde a una categoría de infracción diferente:

- Primer nivel: una infracción tiene como consecuencia una multa máxima de 10 millones de euros o del 2 % de los ingresos anuales de la empresa en todo el mundo, el importe que sea superior.
- Segundo nivel: una infracción tiene como consecuencia una multa máxima de 20 millones de euros o del 4 % de los ingresos anuales de la empresa en todo el mundo, el importe que sea superior.

Además de estas multas, los sujetos de datos pueden solicitar una indemnización por daños y perjuicios cuando una empresa infrinja el RGPD. [5]



Figura 2 Recursos de bocetos de insignias de cumplimiento de GDPR

Ley Federal de Protección de Datos (Suiza)

La nueva Ley Federal de Protección de Datos (nFADP) es una normativa integral de protección de datos que protege la personalidad y los derechos fundamentales de los ciudadanos suizos al procesar sus datos personales.



El gobierno suizo introdujo la primera Ley Federal de Protección de Datos (FADP) en 1992 para abordar las crecientes preocupaciones sobre la privacidad frente a las tecnologías emergentes.

Después de que la Unión Europea introdujera el Reglamento General de Protección de Datos (GDPR), el gobierno suizo se vio obligado a considerar revisar su FADP para alinearla con los últimos estándares de privacidad.

Luego, el Consejo Federal de Suiza comenzó a trabajar en una versión revisada del FADP para abordar los cambios en el panorama tecnológico. El nFADP revisado fue aprobado por ambas cámaras del parlamento y entró en vigor el 1 de septiembre de 2023. El nFADP fue diseñado para abordar las lagunas del primer FADP y alinearse con los estándares del Reglamento General de Protección de Datos de la UE.

¿Cuáles son los derechos de los interesados en virtud del nFADP?

La nueva Ley Federal de Protección de Datos de Suiza (nFADP) otorga algunos derechos a los interesados para proteger sus datos personales compartidos con empresas.

Derecho de información

Según nFADP, las personas tienen derecho a solicitar información al controlador sobre el procesamiento de sus datos personales. Se les debe proporcionar la información necesaria, como los datos de contacto del controlador, el tipo de datos personales procesados, por qué se procesan, durante cuánto tiempo se almacenarán, quiénes tienen acceso a los datos y más.

Derecho a la portabilidad de los datos

Las personas tienen derecho a solicitar al controlador que entregue sus datos personales recopilados en un formato portátil que les permita transferir los datos a otro controlador. Los responsables del tratamiento deben gestionar las solicitudes de portabilidad de datos de los consumidores de forma gratuita si no requiere un esfuerzo excesivo.

Derechos legales

El nFADP de Suiza extiende algunos derechos legales a los interesados con respecto al procesamiento de sus datos personales:

- Los interesados tienen la derecho a solicitar la corrección de datos personales incorrectos compartidos con el responsable del tratamiento. Sin embargo, el responsable del tratamiento podrá denegar las solicitudes de corrección si:
 - existe alguna ley que restringe la corrección de los datos
 - los datos se utilizan con fines de archivo de interés público



- Los interesados pueden solicitar para detener el procesamiento de datos actividades, evitar la divulgación de datos personales específicos a terceros, y eliminar o destruir los datos personales si viola las disposiciones de protección de datos.
- Si no está claro si los datos personales son exactos o no, el interesado puede solicitar que los datos se etiqueten como cuestionado.
- Los interesados también pueden solicitar que cualquier corrección, eliminación, prohibición, disputa o sentencia se comparta con terceros o se publique. [6]

La gestión del consentimiento merece la pena

La FADP es extraterritorial, así que también se aplica a organizaciones ubicadas fuera de Suiza, siempre que traten datos de ciudadanos suizos.

La ley pretende garantizar un flujo de datos continuo y seguro, en formato físico o electrónico con la UE y el EEE. La ley también requiere acuerdos de adecuación con terceros países o el consentimiento de los sujetos de datos para las transferencias internacionales de datos.

La FADP protege los derechos de privacidad de datos de la ciudadanía suiza frente a las violaciones de la misma ya sea por un acceso excesivo o no autorizado a sus datos personales.

Gestión del consentimiento y cumplimiento de la FADP

En muchos casos, el tratamiento de datos personales está permitido sin necesidad de una base jurídica. Se requiere del consentimiento del sujeto de datos para tratar datos personales sensibles usados para hacer perfiles de alto riesgo por parte de instituciones gubernamentales o personas privadas; que se van a enviar a terceros países con los que no existen acuerdos de adecuación.

La nueva FADP

La FADP no es el RGPD en Suiza. Algunas diferencias regulatorias:

- Multas de hasta 250.000 francos suizos a responsables individuales o de hasta 50.000 a empresas
- Designar un Delegado de Protección de Datos es recomendable, pero no obligatorio
- Se requiere de menos información en los avisos o políticas de privacidad
- El adecuamiento de las transferencias de datos es determinado por el Consejo Federal. Las cláusulas contractuales estándar u otros acuerdos empresariales vinculantes también se pueden aplicar [7]



Tabla comparativa de las distintas leyes

Aspecto	México (LFPDPPP y Reforma 2021)	Unión Europea (GDPR)	Suiza (FADP revisada 2023)
Base legal	Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) y su Reglamento.	Reglamento General de Protección de Datos (GDPR), vigente desde 2018.	Ley Federal de Protección de Datos (FADP), revisada en septiembre de 2023 para fortalecer su marco legal.
Ámbito de aplicación	Aplica a entidades privadas y particulares que procesen datos en México.	Aplica a organizaciones dentro de la UE y a aquellas fuera que ofrezcan bienes/servicios a ciudadanos de la UE.	Aplica a empresas en Suiza y a entidades extranjeras que procesen datos de personas en territorio suizo.
Consentimiento	Requerido, salvo excepciones legales. Debe ser expreso, informado y por escrito/electrónico.	Debe ser libre, específico, informado y explícito (ej.: casilla no pre-marcada).	Similar al GDPR: consentimiento explícito para datos sensibles, con bases legales alternativas claras.
Derechos de los titulares	Acceso, rectificación, cancelación (ARCO) y oposición.	Incluye ARCO + portabilidad, limitación del tratamiento, derecho al olvido y oposición al perfilado.	Acceso, rectificación, supresión, oposición, portabilidad y derecho a conocer el origen de los datos.
Transferencias internacionales	Permitidas si el aviso de privacidad informa al titular y se obtiene su consentimiento.	Solo a países con nivel adecuado de protección o mediante cláusulas estándar (ej.: SCCs).	Requieren garantías como cláusulas contractuales (SCCs) o decisiones de adecuación.
Sanciones máximas	Hasta 4% del ingreso anual de la empresa (para infracciones graves).	Hasta €20 millones o 4% del volumen de negocios global anual (lo que sea mayor).	Hasta CHF 250,000 para personas físicas o de hasta 50.000 a empresas
Autoridad supervisora	Instituto Nacional de Transparencia, Acceso a la	Autoridades nacionales de cada país (ej.:	Prefecto Federal de Protección de Datos y Transparencia



	Información y Protección de Datos (INAI).	AEPD en España) y el Comité Europeo de Protección de Datos (EDPB).	(FDPIC), con mayores facultades de investigación desde 2023.
Cookies y rastreo digital	Regulado por la LFPDPPP: aviso de privacidad en sitios web y consentimiento para cookies no esenciales.	Requiere consentimiento explícito para cookies no esenciales (Directiva ePrivacy).	Actualizado en 2023: Consentimiento explícito para cookies no técnicas, alineándose con estándares de la UE.



Referencias

- [1] “La Protección de Datos Personales en México: Normatividad y su importancia”, *Colegio Jurista*. [En línea]. Disponible en: <https://www.colegiojurista.com/blog/art/la-proteccion-de-datos-personales-en-mexico-normatividad-y-su-importancia/>. [Consultado: 16-mar-2025].
- [2] “Normativa y legislación en PDP – Marco Internacional de Competencias de Protección de Datos Personales para Estudiantes”, *INAI*. [En línea]. Disponible en: https://micrositios.inai.org.mx/marcocompetencias/?page_id=370. [Consultado: 16-mar-2025].
- [3] “Conoce las sanciones por incumplir con LFPDPPP”, *Legafirm Consulting*, 20-sep-2021. [En línea]. Disponible en: <https://legafirm.com.mx/conoce-las-sanciones-por-incumplir-con-lfpdppp/>. [Consultado: 16-mar-2025].
- [4] “Reglamento general de protección de datos (GDPR, General Data Protection Regulation)”, *Veritas*. [En línea]. Disponible en: <https://www.veritas.com/es/mx/information-center/gdpr>. [Consultado: 16-mar-2025].
- [5] ¿Qué es el Reglamento general de protección de datos (RGPD)? *Cloudflare*. [En línea]. Disponible en: <https://www.cloudflare.com/es-es/learning/privacy/what-is-the-gdpr/>. [Consultado: 16-mar-2025].
- [6] “Nueva Ley Federal de Protección de Datos de Suiza (nFADP): una guía completa”, *FacilWP*, 25-abr-2024. [En línea]. Disponible en: <https://facil-wp.com/nueva-ley-federal-de-proteccion-de-datos-de-suiza-nfadp-una-guia-completa/>. [Consultado: 16-mar-2025].
- [7] “Ley de Protección de Datos de Suiza - Resumen de la FADP”, *Usercentrics*, 08-sep-2023. [En línea]. Disponible en: <https://usercentrics.com/es/fadp/>. [Consultado: 16-mar-2025].