etiqampus
e-Learning en Integridad

Guía Comparada Protección de Datos Personales: caso México

Compliance Internacional

NIVEL INTERMEDIO

Fecha	Marzo 2025
Tpo. de lectura	26 min.

El avance tecnológico y la transformación digital han puesto la protección de datos personales en el centro del debate regulatorio a nivel global. En Latinoamérica, el desarrollo y fortalecimiento de normativas en esta materia reflejan la creciente necesidad de garantizar la privacidad y seguridad de la información en un entorno empresarial cada vez más interconectado.

La evolución de estas regulaciones y su aplicación práctica imponen nuevos desafíos a las organizaciones, que deben adaptar sus procesos y modelos de negocios para cumplir con estándares más altos y responder a las exigencias de las autoridades regulatorias y fiscalizadoras.

En este contexto, especialista de destacadas firmas legales de 18 países miembros de Compliance Latam, han elaborado esta guía que, además de dar una visión clara y actualizada sobre los marcos normativos y últimas tendencias en protección de datos personales, entrega herramientas clave para que las empresas comprendan y gestionen los riesgos asociados al tratamiento de datos, fomenten una cultura de cumplimiento y refuercen la confianza con sus clientes y socios comerciales.

A continuación te presentamos la sección dedicada a México, escrita por Renata Buerón, Asociada, Privacidad, Protección de Datos y Tecnologías de Información, del estudio Basham.

FUENTE: el texto de esta portadilla se elaboró a partir de la introducción de la "Guía Comparada Protección de Datos Personales" publicada por la plataforma "Compliance Latam".

Guía Comparada Protección de Datos Personales

Marzo 2025



www.compliancelatam.legal



BASHAM 1912

Autor:

Renata Buerón, Asociada, Privacidad, Protección de Datos y Tecnologías de Información.

1. ¿Cuál es el marco regulatorio de la protección de datos personales en tu jurisdicción?

México reconoce en su Constitución los derechos humanos, incluidos los derechos políticos y las libertades civiles. Además, México es parte de tratados internacionales de derechos humanos, como la Carta de Derechos Humanos de la ONU, la Convención Americana sobre Derechos Humanos, entre otros. Es importante mencionar que, en México, los derechos humanos incluidos en los tratados internacionales se encuentran al mismo nivel que la constitución, es decir, en la cúspide del sistema jurídico. La protección de datos personales está reconocida como un derecho humano autónomo por la Constitución mexicana (art. 16, párrafo II). Además, México se adhirió al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108) y su protocolo adicional relativo a las Autoridades de Control y los Flujos Transfronterizos de Datos, en vigor para México a partir del 1 de octubre de 2018. La Constitución mexicana establece garantías y recursos con respecto a los derechos humanos. El recurso más importante para la protección de los derechos humanos en México es el amparo.

En el sector público, la ley que rige la protección de datos personales en México es la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 26 de enero de 2017, así como las leyes locales que abordan el tema dentro de cada estado de la República Mexicana.

En el sector privado, la ley que rige la protección de datos personales en México es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), publicada en el Diario Oficial de la Federación el 5 de julio de 2010. La LFPDPPP regula el tratamiento legítimo de datos personales por parte de los responsables, así como el derecho de cada individuo a determinar si sus datos personales pueden ser tratados. Los principios generalmente aceptados de protección de datos también se incorporan a la LFPDPPP, es decir, los principios de legalidad, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

La legislación secundaria que complementa la LFPDPPP, incluye al Reglamento de la LFPDPPP, y los Lineamientos del Aviso de Privacidad, publicados en el Diario Oficial de la Federación el 21 de diciembre de 2011 y el 17 de enero de 2013, respectivamente.

2. ¿Existe en tu país regulación sobre programas de prevención de infracciones o de cumplimiento en materia de protección de datos personales? ¿Son obligatorios? ¿En qué casos?

La LFPDPPP, y su reglamento (RLFPDPPP), determina diversas obligaciones con respecto al tratamiento de datos personales, y el artículo 48 del RLFPDPPP establece los medios para cumplir con el principio de responsabilidad, entre ellos desarrollar un programa de privacidad.

3. ¿Qué contenido mínimo deben tener los programas de cumplimiento en protección de datos personales en tu país?

No se establece específicamente qué debe incluir ese programa, sin embargo del contenido de dicho artículo, los programas de privacidad por lo general deben: ser obligatorios y exigibles al interior de la organización del responsable; poner en práctica un programa de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales; establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad; destinar recursos para la instrumentación de los programas y políticas de privacidad; instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos; revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran; establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales; disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento; establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la LFPDPPP y el RLFPDPPP, y establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.

4. ¿Qué beneficios trae contar al interior de la organización con un programa de cumplimiento en protección de datos personales?

El principal beneficio es minimizar riesgos en materia de seguridad de la información personal, lo que conlleva

a menores posibilidades de sufrir vulneraciones y, por tanto, inconformidades y demandas por parte de los afectados.

También se minimiza la posibilidad de ser sancionados por la autoridad de datos y por incumplir las leyes en la materia. Además, hay aspectos claves como la reputación y confianza por los consumidores/titulares de datos personales, junto a la protección de la marca.

5. ¿Existen procesos de certificación de los programas de cumplimiento en protección de datos en tu país? ¿Quién realiza la certificación?

N/A

6. ¿En tu jurisdicción es obligatorio contar con un delegado de protección de datos personales? ¿En qué casos?

Sí, el responsable del tratamiento debe nombrar a una persona o departamento específico de protección de datos. Esta persona o departamento será el encargado de promover la protección de los datos personales dentro de la organización, de verificar el cumplimiento de la ley y el reglamento, de responder a las solicitudes de los interesados cuando ejerzan sus derechos, entre otras obligaciones.

Asimismo, se debe contar con el delegado en todos los casos que una persona física o moral trate datos personales, no hay un criterio que delimite.

7. ¿Existen sanciones asociadas al incumplimiento de la normativa sobre protección de datos personales? ¿De qué tipo? ¿A cuánto ascienden las multas?

Las infracciones a la LFPDPPP o a su reglamento pueden ser sancionadas de la siguiente manera:

• Con una advertencia que instruya al responsable del tratamiento de los datos para que lleve a cabo las acciones solicitadas por el titular (en relación con el ejercicio de sus derechos)

• Con una multa que oscila entre las 100 y las 320.000 unidades denominadas UMA. Actualmente, el valor de una unidad llamada UMA es de 108.57 pesos mexicanos (aprox. USD 5.4). Por lo tanto, las multas oscilan entre aproximadamente USD 550 y USD 1' 500,000. Las multas pueden duplicarse si se trata de datos personales sensibles.

• Para las infracciones recurrentes, pueden imponerse multas adicionales y se calcularán sobre la misma base que en el párrafo anterior.

• Cuando se trata de infracciones cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces, los montos establecidos.

Además, se puede imponer una pena de prisión a cualquier persona que infrinja ilegalmente las medidas de seguridad o facilite una violación de una base de datos bajo su custodia o que se beneficie ilegalmente del tratamiento de datos personales, aprovechando engañosamente cualquier error del titular.

Sanción	Conducta
Apercibimiento	No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada.
100 a 160,000 veces el valor de la UMA $108.57 ($11,000 a $17,500)	• Actuar con negligencia o dolo en la tramitación de solicitudes de acceso, rectificación, cancelación u oposición de datos personales. • Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable. • Dar tratamiento a los datos personales en contravención a los principios establecidos en la LFPDPPP. • Omitir en el aviso de privacidad o todos los elementos a que se refiere el artículo 16 de esta ley. • Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de estos que legalmente procedan cuando resulten afectados los derechos de los titulares. • No cumplir con el apercibimiento de la autoridad.
	• Incumplir el deber de confidencialidad. • Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin

200 a 320,000 veces el valor de la UMA ($22,000 a $35,000,000.00)	obtener nuevamente el consentimiento del titular. • Transferir datos a terceros sin comunicar a estos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos. • Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable. • Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos previstos en la LFPDPPP. • Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que este sea exigible. • Obstruir los actos de verificación de la autoridad. • Recabar datos en forma engañosa y fraudulenta. • Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el instituto o los titulares. • Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos ARCO. • Crear bases de datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.

8. ¿Qué tipo de conducta sanciona la normativa en protección de datos personales de tu país?

En caso de que persistan las infracciones, se impondrá una multa adicional que irá de 100 a 320,000 veces el valor de la UMA; y tratándose de faltas cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces, los importes establecidos.

9. ¿Tu jurisdicción tiene un organismo técnico que dicte directrices y fiscalice el cumplimiento de las normas de protección de datos personales?

La autoridad encargada de la observancia de la protección de datos es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). El INAI es un organismo constitucional y autónomo responsable de promover y difundir el derecho al acceso a la información pública, así como el derecho a la protección de datos dentro de organismos gubernamentales y partes privadas. Este organismo se compromete a trabajar con otras autoridades federales, estatales y municipales para promover la protección de datos en diferentes industrias y sectores, como los sectores financieros, educativo y de salud.

La Autoridad Mexicana de Protección de Datos (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, INAI), será disuelta tras una reciente reforma constitucional, aprobada el pasado mes de diciembre de 2024.

El INAI tiene entre sus funciones velar por la transparencia de las acciones que realizan las entidades del sector público y salvaguardar el derecho humano a la protección de datos personales en posesión tanto de entidades del sector público como de particulares.

El Gobierno mexicano determinará qué entidad de la Administración Pública Federal asumirá la responsabilidad de velar por la protección de los datos personales en posesión de particulares.

Tras la publicación del proyecto de ley en el Diario Oficial de la Federación (20 de diciembre de 2024), el Congreso mexicano tiene 90 días (marzo de 2025) para reformar la legislación mexicana de protección de datos, la Ley Orgánica de la Administración Pública Federal (LOAPF) y las leyes secundarias correspondientes para designar a la nueva autoridad de protección de datos encargada de gestionar los procedimientos relacionados con la protección de derechos, las verificaciones y la imposición de sanciones. Aún no se ha determinado la dependencia o ministerio específico encargado de salvaguardar los datos personales en posesión de entidades privadas.

Todas las acciones realizadas por el INAI con anterioridad a la promulgación de la legislación secundaria mantendrán plena eficacia jurídica. La disolución de los entes autónomos no se producirá hasta que dicha legislación secundaria entre en vigor.

10. ¿Cuáles son los primeros pasos que toman las organizaciones en tu país para comenzar a aplicar la normativa en protección de datos personales en general y un programa de cumplimiento en particular?

Se lleva a cabo una auditoria en la materia.

11. ¿Cuál es el ámbito de aplicación territorial de la normativa de protección de datos de tu país? ¿La normativa puede aplicarse extraterritorialmente?

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su reglamento, son de aplicación extraterritorial en ciertos casos.

Antes de revisar los supuestos de aplicación extraterritorial, es importante conocer algunos conceptos clave que facilitan su identificación:

• **Responsable:** Persona física o moral del sector privado que decide sobre el tratamiento de datos personales.

• **Encargado:** Persona física o moral que trata datos personales en nombre y por cuenta del responsable.

• **Tratamiento:** Cualquier acción relacionada con datos personales, incluyendo su obtención, uso, divulgación o almacenamiento, ya sea por medios físicos o electrónicos. El uso comprende el acceso, manejo, aprovechamiento, transferencia o disposición de los datos personales.

• **Establecimiento:** Para personas físicas, se refiere al lugar donde se desarrollan sus actividades económicas o su domicilio. Para personas morales, es el lugar donde se encuentra su administración principal en México o cualquier instalación estable que permita el ejercicio real y efectivo de su actividad.

La LFPDPPP y RLFPDPPP resultan aplicables extraterritorialmente en los siguientes escenarios:

1. El responsable no está establecido en México, pero la legislación mexicana le resulta aplicable debido a la celebración de un contrato o en términos del derecho internacional.

2. El responsable no está establecido en México, pero utiliza medios situados en territorio mexicano, salvo que dichos medios se utilicen únicamente con fines de tránsito sin implicar tratamiento de datos.

Consideraciones sobre la aplicación extraterritorial

Es decir, la LFPDPPP y su reglamento serán aplicables incluso si el tratamiento central de datos no se lleva a cabo en México, pero cuando menos se recolectan en México. Por ello, si bien ni el responsable, ni el encargado realizan tratamiento de datos en territorio mexicano, la legislación mexicana resultaría aplicable en caso de que cuenten con medios localizados en nuestro país.

En la práctica es complejo que la autoridad de datos inicie y cumplimente una investigación por el incumplimiento de la LFPDPPP y su reglamento, por parte de una empresa o particular que no tenga representación en México.