USAID
DEL PUEBLO DE LOS ESTADOS UNIDOS DE AMÉRICA

MANUAL DE PROTECCIÓN DE DATOS PERSONALES

PARA ORGANIZACIONES DE LA SOCIEDAD CIVIL

AUTORES

Equipo Legal Amazon México
&
Carmina Mogollón González

COORDINACIÓN

Patricia Villa Berger

REVISIÓN LEGAL

Alan García, Débora Vera y Natalia Alvarado

REVISIÓN EDITORIAL

Maru Cortazar

CORRECTOR DE ESTILO

Raúl Estrada

Fundación Appleseed México agradece el apoyo brindado por Greenberg Traurig, S.C. y Dell México, por su valiosa colaboración en la elaboración de este manual.

La elaboración de este manual ha sido posible gracias al generoso apoyo del Pueblo de los Estados Unidos de América a través de la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID). El contenido del mismo se desarrolló bajo la coordinación de la Fundación Appleseed México, A.C. y no necesariamente refleja el punto de vista de USAID o del Gobierno de los Estados Unidos.

Esta obra es para fines informativos únicamente y la misma no cubre, ni pretende cubrir, todo lo que se requiere para el cumplimiento legal del tema particular que desarrolla. Nada en este manual tiene la intención de crear una relación cliente-abogado, por lo que no se deberá interpretar su contenido como asesoría legal o reemplazo de la asistencia legal requerida para casos individuales; consecuentemente, sus lectores deberán consultar a sus propios asesores legales para tal efecto.

Asimismo, se hace del conocimiento del lector que ninguna autoridad ha aprobado o desaprobado el contenido de la información descrita en este manual. La Agencia de los Estados Unidos para el Desarrollo Internacional, el Gobierno de los Estados Unidos, la Fundación Appleseed México, A.C., sus respectivas subsidiarias, afiliadas, asesores, consejeros o representantes, los autores de este material, y los colaboradores, no responderán de daño o perjuicio alguno derivado de o relacionado con, el uso de este manual o su contenido, o que de manera alguna se relacione con la información aquí comprendida.

En caso de requerir asesoría específica en la elaboración de estatutos sociales o cualesquiera de los trámites enunciados en esta obra, Fundación Appleseed México, A.C. y la Red ProBono México® podrán proporcionarles la asistencia correspondiente a las organizaciones de la sociedad civil conforme a los requerimientos y procedimientos internos de Fundación Appleseed México, A.C.

ÍNDICE

PROGRAMA PARA LA SOCIEDAD CIVIL DE USAID

El Programa para la Sociedad Civil de la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID) busca mejorar la capacidad institucional y sostenibilidad de las Organizaciones de la Sociedad Civil (OSC) mexicanas para implementar efectivamente sus agendas en la prevención del crimen y la violencia, la promoción y defensa de los Derechos Humanos, y la reforma al sistema de justicia. A fin de complementar los esfuerzos del Gobierno de México y para lograr los objetivos delineados en la Estrategia de Cooperación para el Desarrollo del País de USAID, el Programa para la Sociedad Civil busca involucrar a los actores clave para mejorar el entorno legal para las OSC en México y reducir las barreras que enfrentan para su registro legal y el cumplimiento de sus obligaciones, así como impulsar el desarrollo de las capacidades institucionales de organizaciones en el país.

El Programa para la Sociedad Civil de USAID busca promover un entorno más propicio y desarrollar las capacidades institucionales y humanas de las OSC para que estén mejor posicionadas para contribuir a generar impactos positivos en su entorno; monitorear y evaluar sus programas; y brindar mejores servicios a sus beneficiarios. También enfatiza la necesidad de desarrollar las capacidades de las OSC para construir alianzas estratégicas al interior del sector, así como con el sector privado y el gobierno para poder obtener resultados sostenibles en el largo plazo.

El Programa para la Sociedad Civil de USAID es implementado por Social Impact, Inc. en alianza con Fundación Appleseed México, A.C.

ABREVIACIONES

CPEUM o Constitución – Constitución Política de los Estados Unidos Mexicanos

GDPR – Reglamento General de Protección de Datos de la Unión Europea

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

LFPDPPP – Ley Federal de Protección de Datos Personales en Posesión de los Particulares

OSC – Organización u organizaciones de la sociedad civil

Reglamento – Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

NUEVE ACCIONES PARA EMPEZAR

ACCIÓN	PARA SABER MÁS...
1 Entender que las OSC, independientemente de que persigan fines sociales o asistenciales, están obligadas a cumplir con las obligaciones de materia de protección de datos personales.	-Sujetos de la LFPDPPP y otras definiciones (sección 3.3) -¿Cuándo una OSC se convierte en sujeto responsable? (sección 4.1) -¿Cómo saber si una OSC trata con datos personales? (sección 4.2) -¿Qué sucede cuando una OSC recibe fondos gubernamentales? (sección 4.6)
2 Saber qué son los datos personales.	-¿Qué es un dato personal? (sección 3.1) -Tipos de datos personales (sección 3.2) -Marco normativo (capítulo 2).
3 Aprender cómo tratar datos personales.	-Principios de la protección de datos personales (sección 3.4). -Obtención del consentimiento para tratamiento de datos personales (sección 4.3). -Casos más comunes (sección 4.4). -Transferencias y remisiones de datos personales (sección 4.5). -Confidencialidad (sección 6.1). -Medidas de seguridad (sección 6.2). -Mejores prácticas (capítulo 10).
4 Implementar el aviso de privacidad en la OSC.	-El aviso de privacidad (capítulo 5). -Casos más comunes (sección 4.4).
5 Implementar medidas de seguridad adecuadas y razonables para proteger los datos personales que la OSC trata.	-Medidas de seguridad (sección 6.2). -Mejores prácticas (capítulo 10).
6 Nombrar a la persona o departamento de datos personales.	-Persona o departamento de datos personales (sección 6.3).
7 Conocer las posibles vulneraciones a bases de datos personales y cómo proceder en caso que suceda.	-¿Qué hacer frente a una vulneración de bases de datos? (sección 6.4)
8 Aprender sobre los derechos de los titulares de datos personales para que la OSC los garantice adecuadamente.	-Derechos de los titulares de datos personales (capítulo 7). -Principios de la protección de datos personales (sección 3.4).
9 Conocer las facultades del INAI como autoridad en materia de datos personales.	-Autoridad (sección 3.5). -Marco normativo (capítulo 2). -Procedimiento de verificación (capítulo 8). -Sanciones (capítulo 9).

1. INTRODUCCIÓN

El presente manual tiene como propósito dar a conocer el panorama general de la normativa aplicable en materia de protección de datos personales en México, así como elementos prácticos para el sector de la sociedad civil organizada pueda cumplir con dicha normatividad.

La protección de datos personales en México tiene tal importancia que ha sido incorporada como derecho fundamental en el artículo 16 de la Constitución desde el 1° de junio de 2009. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) fue posteriormente publicada el 5 de julio de 2010, mientras que su Reglamento fue publicado el 21 de diciembre de 2011. Como consecuencia de esta reforma constitucional y de la publicación de la legislación secundaria, el otrora Instituto Federal de Acceso a la Información Pública se convirtió en la autoridad encargada de la protección de datos personales en posesión de particulares.

La LFPDPPP define los datos personales como ***"cualquier información relacionada a una persona física identificada o identificable"***, es decir, datos tales como nombre, domicilio, teléfono de contacto, correo electrónico personal son datos personales que permiten identificar a una persona física. Sin embargo, existen otro tipo de datos personales que afectan la esfera más íntima de las personas, o cuya utilización indebida pueda dar origen a discriminación o conllevar un riesgo grave para los individuos. Estos datos sensibles están relacionados con el origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual. Adicionalmente, existen datos financieros o patrimoniales, tales como la información fiscal, historial crediticio, cuentas bancarias, números de tarjetas de crédito o débito, información de ingresos, egresos.

Las OSC, dependiendo de sus actividades, pueden tratar con algunos o con todos estos tipos de datos en su día a día, al igual que cualquier otra persona física o moral. En consecuencia e independientemente de que persigan fines sociales o asistenciales, están obligadas a cumplir con la (LFPDPPP) y su reglamentación secundaria.

El objetivo de este manual es guiar a las OSC en dicho cumplimiento y de esa forma garantizar el derecho de todo individuo a su privacidad y a la autodeterminación informativa. En el tratamiento de datos personales, los individuos asumen que existe una expectativa razonable de privacidad, la cual es entendida como la confianza que una persona deposita en otra -en este caso en las OSC-, respecto a que sus datos personales serán tratados conforme a lo acordado entre las partes y en cumplimiento de la legislación.

Este manual ofrece una herramienta que ayude a fortalecer el sector y que promueva el cumplimiento legal por parte de las OSC, todo lo cual redunda en promover el Estado de Derecho en México.

2. MARCO NORMATIVO

La protección de datos personales tiene su fundamento en la Constitución Política de los Estados Unidos Mexicanos ("Constitución" o "CPEUM"), específicamente en sus artículos 6 y 16. El artículo 16 de la Constitución establece que toda persona tiene derecho a la protección de sus datos personales y al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición a su tratamiento. Por su parte, el párrafo II del apartado A. del artículo 6° constitucional, establece el derecho a la protección de la información que se refiere a la vida privada de las personas cuando ésta se encuentra en posesión del gobierno federal o de los gobiernos estatales. El derecho a la protección de los datos personales de los individuos es considerado como un derecho fundamental.

La protección de los datos personales es un derecho fundamental

Además, existen también tratados internacionales de derechos humanos que reconocen la privacidad como un derecho, tales como:

1. Declaración Universal de los Derechos Humanos (1948).
2. Declaración Americana de Derechos y Obligaciones del Hombre (1965).
3. Convención Americana sobre Derechos Humanos (1969).
4. Pacto Internacional de Derechos Civiles y Políticos (1966).
5. Convenio 108+ (Convention for the protection of individuals with regard to the processing of personal data, 1981).

Hay que recordar que la Constitución y los tratados internacionales de protección de derechos humanos están al mismo nivel y forman conjuntamente un bloque de protección, de acuerdo con el artículo 1° constitucional, conocido como "bloque de constitucionalidad".[1]

Hay que precisar que a partir del 1 de octubre de 2018, México es parte del Convenio 108+ y de su protocolo adicional, cuya importancia estriba en que son los primeros instrumentos internacionales en materia de datos personales que obligan a México. El objetivo principal de estos instrumentos es regular y salvaguardar el derecho fundamental a la protección de datos personales. Esto implica que todos los Estados Partes están obligados a transponer en sus leyes nacionales los principios establecidos para asegurarse que en tales países se respete el derecho fundamental que tiene todo individuo a la protección de sus datos personales.

[1] Derechos fundamentales. Cuando de manera suficiente se encuentran previstos en la Constitución Política de los Estados Unidos Mexicanos, se torna innecesario en interpretación conforme acudir y aplicar la norma contenida en tratado o convención internacional, en tanto el orden jurídico en su fuente interna es suficiente para establecer el sentido protector del derecho fundamental respectivo. Décima Época. Núm. de Registro: 2003548. Instancia: Tribunales Colegiados de Circuito. Jurisprudencia. Fuente: Semanario Judicial de la Federación y su Gaceta. Libro XX, Mayo de 2013, Tomo 2. Materia(s): Común. Tesis:I.3o.P. J/1 (10a.) Página: 1221.
Control de convencionalidad y constitucionalidad de normas generales aplicadas en el acto reclamado en un amparo indirecto. Es viable aunque aquéllas no hayan sido reclamadas de manera destacada o sea improcedente el juicio en su contra. Décima Época. Registro: 2001873. Instancia: Tribunales Colegiados de Circuito. Tesis Aislada. Fuente: Semanario Judicial de la Federación y su Gaceta, Libro XIII, Octubre de 2012, Tomo 4. Materia(s): Común. Tesis: XXVII.1o.(VIII Región) 8 K (10a.), Página: 2413.

Existen varias leyes, reglamentos y lineamientos que regulan la forma particular en la que se protegerá y garantizará este derecho, que se enlistan a continuación:

1. Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)[2];
2. Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Reglamento)[3];
3. Lineamientos del Aviso de Privacidad[4]; y
4. Recomendaciones en Materia de Seguridad de Datos Personales[5].

Además, existen criterios y manuales adicionales emitidos por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) como autoridad responsable de promover y vigilar la debida observancia del derecho a la protección de datos personales en la sociedad mexicana.

Es importante distinguir que el tratamiento de datos personales en posesión de autoridades está regulado en una ley independiente denominada Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la cual no aplica a las OSC por disposición expresa.[6] Las OSC deben tener en cuenta que aun y cuando reciban recursos gubernamentales (estatales y/o federales), la ley que les es aplicable respecto al tratamiento de datos personales es la LFPDPPP. Este manual se centra en el cumplimiento de las obligaciones y deberes establecidos en la LFPDPPP que es aplicable a los particulares, tales como las OSC.

En mayo de 2018, entró en vigor en la Unión Europea el Reglamento General de Protección de Datos (GDPR), relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos. Este reglamento funciona como un conjunto único de normas aplicable en toda la Unión Europea y refuerza los derechos de los individuos a la protección de su información personal y responsabiliza considerablemente a los responsables y encargados de su tratamiento.[7] La aplicación territorial del Reglamento se establece en el artículo 3 del mismo y, como regla general, solamente aplicaría a una OSC establecida en México en la medida en que la misma activa e intencionalmente se dirija a individuos localizados en la Unión Europea: por ejemplo en una campaña de recolección de fondos, o bien para monitorear el comportamiento de individuos localizados en Europa. En caso de tener dudas respecto a si es o no aplicable el GDPR a una OSC se recomienda solicitar asesoría dentro de su organización o en caso de ser necesario, pedir el apoyo de un abogado experto en la materia.

---

[2] Ley Federal de Protección de Datos Personales en Posesión de los Particulares. (5 de julio de 2010). Visitado el 24 de abril de 2019, disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf
[3] Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. (21 de diciembre de 2011). Visitado el 24 de abril de 2019, disponible en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf.
[4] Lineamientos del Aviso de Privacidad. (17 de enero de 2013). Visitado el 24 de abril de 2019, disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5284966&fecha=17/01/2013.
[5] Recomendaciones en Materia de Seguridad de Datos Personales. (30 de octubre de 2013). Visitado el 24 de abril de 2019, disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013.
[6] Artículo 1° de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados: "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." En términos de esta ley, un "sujeto obligado" es, 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.
[7] Ver sección 3.3 (Sujetos de la LFPDPPP y otras definiciones) para conocer quiénes son los responsables y encargados de datos personales.

EN RESUMEN...

✓ La protección de datos personales es un derecho fundamental reconocido en la Constitución (artículos 6 y 16) y en el derecho internacional.

✓ Las OSC, independientemente de que persigan fines sociales o asistenciales, están obligadas a cumplir con las obligaciones de materia de protección de datos personales.

✓ La normatividad mínima a conocer es:

1. Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).
2. Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Reglamento).
3. Lineamientos del Aviso de Privacidad.
4. Recomendaciones en Materia de Seguridad de Datos Personales

✓ Las actividades de las OSC respecto del tratamiento de datos personales se rigen únicamente por la LFPDPPP, sin importar que reciban recursos públicos.

3. LOS DATOS PERSONALES

3.1. ¿QUÉ ES UN DATO PERSONAL?

La LFPDPPP define "dato personal" como ***"cualquier información relacionada a una persona física identificada o identificable"***[8]. De manera general, una persona física puede entenderse como todo miembro de la especie humana con la posibilidad de adquirir derechos y contraer obligaciones y su información como individuo se encuentra protegida por la LFPDPPP. En términos de esta ley, las personas físicas protegidas por la misma se definen como "titular", que es considerada "la persona física a quien corresponden los datos personales"[9].

En lo que respecta a las empresas, organizaciones, asociaciones, etc. (conocidas en el ámbito jurídico como "personas morales"), su información corporativa y comercial por regla general no es considerada como datos personales sujeta a la protección de la LFPDPPP; sin embargo, tal información se protege en otros ordenamientos, tales como la Ley de Propiedad Industrial, la Ley Federal del Derecho de Autor, la Ley Federal del Trabajo, entre otras[10].

En el apartado siguiente se describirán los tipos de datos personales que la LFPDPPP protege, y que por ende también deben proteger las OSC que traten este tipo de datos.

3.2. TIPO DE DATOS PERSONALES

Según su naturaleza y régimen de protección, los datos personales se pueden clasificar en tres[11]:

1. Datos personales en general: cualquier información relacionada a una persona física identificada o identificable (ej. nombre, domicilio, teléfono de contacto, correo electrónico personal, actividades, experiencia laboral y profesional, etc.).

2. Datos personales sensibles: aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, orientación sexual.

3. Datos financieros y patrimoniales: aquellos datos personales relacionados con bienes (muebles e inmuebles) de un individuo, la información fiscal, historial crediticio, cuentas bancarias, números de tarjetas de crédito o débito, información de ingresos, egresos, etc.

---

[8]Artículos 3, fracción V de la LFPDPPP.
[9]Artículos 3, fracción XVII de la LFPDPPP.
[10]Las OSC deben tener en cuenta que aun y cuando la información de personas morales no es considerada por regla general como "datos personales" sí está sujeta a protección bajo otras leyes, como son la Ley de Propiedad Industrial, Ley Federal del Derecho de Autor, Código de Comercio, etc. Asimismo, la Suprema Corte de Justicia resolvió en una tesis aislada que la información de personas morales puede, en ciertos casos, equipararse a datos personales (ver tesis aislada con número de registro 2005522 disponible a través de https://sjf.scjn.gob.mx/sjfsist/Paginas/DetalleGeneralV2.aspx?ID=2005522&Clase=DetalleTesisBL).
[11]La LFPDPPP no contempla una definición para datos financieros o patrimoniales, sin embargo, el propio nombre de los mismos indica a qué se refieren y la autoridad en materia de protección de datos personales en México ha adoptado criterios para considerar a este tipo de información distinta a los datos generales o de identificación y a los datos personales sensibles.

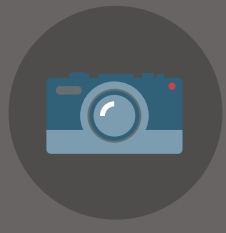
LOS DATOS PERSONALES PUEDEN SER:

1.
GENERALES: nombre, domicilio, teléfono de contacto, correo electrónico personal, actividades, experiencia laboral y profesional, etc.

2.
SENSIBLES: origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, orientación sexual.

3.
FINANCIEROS Y PATRIMONIALES: información fiscal, historial crediticio, cuentas bancarias, números de tarjetas de crédito o débito, información de ingresos, egresos, etc.

Con base en estas definiciones, las fotografías también son datos personales. Es importante tener en cuenta que en algunos casos las fotografías pueden ser considerados datos sensibles si su utilización puede dar pie a discriminación o algún peligro o riesgo para la persona, tales como problemas de seguridad o riesgos para la vida. En este sentido, los particulares que tengan en su posesión este tipo de datos deben evaluar el contexto específico en el que sus actividades se desenvuelven para valorar y decidir si la utilización de ciertos datos puede poner en riesgo la vida o seguridad de las personas o dar lugar a discriminación de la persona en cuestión. Para la utilización de datos personales sensibles, como podrían ser los retratos de personas o videos, en ciertas circunstancias, se requiere del consentimiento expreso y por escrito de sus titulares, o bien, de quienes los representen legalmente.



Las fotografías y los videos también son datos personales.

¿La OSC debe tratar con datos personales sensibles? Entonces se requiere del consentimiento expreso y por escrito de sus titulares o de sus representantes legales.

3.3. SUJETOS EN LA LFPDPPP Y OTRAS DEFINICIONES

TITULAR: Es la persona física a quien corresponden los datos personales. Por ejemplo, los empleados de las OSC, las personas físicas que llevan a cabo donaciones a las OSC y todos los individuos que se benefician de los programas de las OSC son considerados "titulares" en términos de la LFPDPPP, y sus datos personales deben ser protegidos conforme a los principios y deberes ahí establecidos.

RESPONSABLE: Se le denomina responsable, a la persona física o moral de carácter privado que decide sobre el tratamiento de datos personales. Las OSC que tratan datos personales de los titulares antes descritos se consideran responsables y por lo tanto están obligados a cumplir con la LFPDPPP y cuidar los datos personales que mantienen.

ENCARGADO: Se denomina a la persona física o moral que, sola o conjuntamente con otra, trate datos personales por cuenta del responsable. Los terceros que prestan servicios a las OSC que implican el tratamiento de datos personales (por ejemplo, servicios de administración de nómina, servicios de video o fotografía, servicios para campañas de recaudación de fondos), son considerados "encargados" en términos de la LFPDPPP.

TRATAMIENTO: La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales. En el caso de las OSC, el "tratamiento" de datos personales engloba todo el flujo de los datos personales dentro de la organización, desde que se recolectan y hasta que se eliminan de las bases de datos.

TRANSFERENCIAS: Es toda comunicación de datos personales realizada a terceros distintos del responsable o encargado del tratamiento. Toda transferencia, ya sea de carácter nacional o internacional, deberá contar con el consentimiento del titular de los datos personales, salvo las excepciones previstas en el artículo 10 de la LFPDPPP y que se explican más adelante en este manual.

3.4. PRINCIPIOS DE LA PROTECCIÓN DE DATOS PERSONALES

La LFPDPPP y su Reglamento establecen ocho principios rectores para la protección de los datos personales. Tomando en consideración que las OSC tratan datos personales en su día a día, es obligación de todos sus empleados involucrados en el tratamiento de datos personales el regir su actuación y proteger aquella información personal a la que tienen acceso, de conformidad con los mencionados principios.

A continuación, se realiza una descripción general de cada uno de los principios de protección de datos personales, tomando como base las disposiciones contenidas tanto en la LFPDPPP, como en su Reglamento:

1 LICITUD[12] A través del principio de licitud se obliga al responsable a que el tratamiento de los datos personales que recabe, lo realice con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional.

De conformidad con este principio, los empleados de toda OSC deberán tratar los datos personales que recaben atendiendo a las disposiciones legales aplicables.[13] Al respecto, es obligación de los empleados asistir a las capacitaciones y/o pláticas que se impartan al respecto, ya sea a través de la propia OSC o en otros foros.

2 CONSENTIMIENTO[14] De conformidad con este principio, se establece que el responsable deberá obtener el consentimiento para el tratamiento de los datos personales salvo ciertas excepciones de ley. Se debe obtener el consentimiento previo del titular de los datos para poder realizar el tratamiento de su información.

Por regla general el consentimiento tácito es suficiente. Éste se obtiene cuando habiendo puesto a disposición de los titulares el aviso de privacidad, no se manifieste su oposición.[15] Sin embargo, en el caso de datos financieros o patrimoniales, se requiere el consentimiento expreso de su titular, y en el caso de datos personales sensibles el consentimiento deberá ser expreso y por escrito, a través de firma autógrafa, firma electrónica o cualquier otro mecanismo de autenticación que al efecto se establezca.

No es necesario el consentimiento para el tratamiento de los datos personales cuando:

1. Esté previsto en una ley.
2. Los datos personales figuren en una fuente de acceso público.
3. Los datos personales se sometan a un procedimiento previo de disociación, de tal forma que no puedan asociarse, ni identificar a su titular.[16]
4. Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable.
5. Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes.
6. Sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos

[12] Artículos 7 de la LFPDPPP y 10 de su Reglamento.
[13] Ver capítulos 4, 5, 6, 7 y 8 del presente manual.
[14] Artículos 10 de la LFPDPPP y 11 de su Reglamento.
[15] Ver capítulo 5 del presente manual.
[16] Las medidas de disociación de datos personales se logran a través de medios tecnológicos para el caso de bases de datos electrónicas, pero para definir la manera más idónea de lograr la disociación de los datos personales es conveniente analizar caso por caso en cada OSC.

médicos o la gestión de servicios sanitarios y el titular no esté en condiciones de otorgar su consentimiento.

7. Se dicte resolución de autoridad competente.

Cuando se deban utilizar datos personales de menores de edad o de personas en estado de incapacidad, es necesario recabar el consentimiento de la persona que ejerce la patria potestad, el tutor o representante legal, según sea el caso, de conformidad con las reglas de representación del Código Civil aplicable. El aviso de privacidad se debe entregar a tales personas y en el mismo se debería aclarar que se están tratando datos personales de menores y cómo se cuidan.[17]

En caso de que el responsable desee tratar fotografías, deberá mencionarlo expresamente en el aviso de privacidad, así como cumplir con lo establecido en el artículo 87 de la Ley Federal del Derecho de Autor, el cual dispone que "el retrato de una persona sólo puede ser usado o publicado, con su consentimiento expreso, o bien con el de sus representantes o los titulares de los derechos correspondientes". Esto significa que el responsable deberá obtener una carta de consentimiento para uso de retratos/imagen que cumpla con lo establecido en la Ley Federal del Derecho de Autor, así como el aviso de privacidad.

En caso de duda respecto a si es o no necesario obtener el consentimiento para el tratamiento de datos personales, se debe consultar con el Departamento de Datos Personales o bien con la persona encargada del tema dentro de la OSC.

3 INFORMACIÓN [18] Atendiendo a lo dispuesto en la LFPDPPP y por el Reglamento de la LFPDPPP, el responsable deberá dar a conocer al titular, a través del aviso de privacidad, la información relativa a la existencia y características principales del tratamiento a que serán sometidos sus datos personales.

4 CALIDAD [19] Para cumplir con el principio de calidad, es obligación tratar los datos personales exactos, completos, pertinentes, correctos y actualizados atendiendo a las finalidades para las cuales fueron recabados. Cuando los datos son proporcionados por los titulares, se entiende que el responsable se encuentra en cumplimiento de este principio.

5 FINALIDAD [20] De conformidad con este principio, los datos personales solamente podrán ser recabados y tratados para cumplir con las finalidades establecidas en el aviso de privacidad correspondiente. Por lo anterior, para poder llevar a cabo el tratamiento de los datos personales para cualquier otra finalidad que no se encuentre establecida en el aviso de privacidad se deberá obtener el consentimiento de los titulares y el aviso de privacidad deberá ser modificado para informar sobre las nuevas finalidades.

Todas las personas que trabajan en una OSC, y que como parte de sus funciones tratan datos personales, deben conocer cuáles son las finalidades que dieron origen al tratamiento de datos personales y que las mismas son necesarias para la relación jurídica entre la OSC y el titular, así como aquéllas que no lo son.

---

[17] En lo que respecta a los menores de edad, también hay que contemplar las protecciones a la privacidad e intimidad que se establecen en la Ley General de los Derechos de Niñas, Niños y Adolescentes (ver artículos 76 a 81). Específicamente, los menores de edad están protegidos contra divulgaciones o difusiones ilícitas de su información o datos personales. De igual forma, es una violación a la intimidad de los menores de edad manejar su imagen, datos personales o referencias que permitan su identificación en medios de comunicación menoscabando su honra, reputación o que los ponga en riesgo. La violación a éstas y otras obligaciones pueden dar pie a acciones civiles de reparación del daño y procedimientos administrativos.
[18] Artículos 3, fracción I de la LFPDPPP y 23 de su Reglamento.
[19] Artículo 36 del Reglamento de la LFPDPPP.
[20] Artículos 12 de la LFPDPPP y 40 de su Reglamento.

Todas las personas que trabajan o colaboran en una OSC, que traten datos personales, deben conocer las finalidades que dan origen al tratamiento de datos personales.

6 LEALTAD [21] Todos los datos personales deberán tratarse privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad por lo que, bajo ningún supuesto, se deberán recabar datos personales a través de medios engañosos o fraudulentos.

En lo que se refiere a la expectativa razonable de privacidad[22], ésta se entiende como la confianza que deposita cualquier persona en otra, con respecto a que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron[23].

7 PROPORCIONALIDAD [24] De conformidad con el principio de proporcionalidad, tanto la OSC como sus empleados, deberán llevar a cabo el tratamiento solamente de aquellos datos personales que resulten necesarios, adecuados y relevantes en relación para las finalidades para las que se hayan obtenido.

Conforme a este principio, se debe seguir un criterio de minimización, en términos del cual los datos personales que se traten sean los mínimos necesarios de acuerdo con las finalidades para los que se requieran.

8 RESPONSABILIDAD [25] Toda OSC, como responsable, debe velar y responder por el tratamiento de los datos personales que mantiene bajo su posesión, y también por aquellos que hubiere comunicado a un tercero, ya sea que se éstos terceros se encuentren en México o en el extranjero.

¡Menos es más!
Las OSC sólo deben tratar los datos personales que sean necesarios, adecuados y relevantes para los fines que persiguen. Recabar datos personales innecesarios es un riesgo potencial (legal y de gestión) para cualquier organización.

[21] Artículos 7 de la LFPDPPP y 44 de su Reglamento.
[22] Dentro de los estándares para la protección de la privacidad de los individuos se ha desarrollado en países como Estados Unidos, Canadá y países europeos el denominado estándar a una "expectativa razonable de privacidad". Este estándar se compone de: (i) un elemento subjetivo conforme al cual toda persona debe tener una expectativa real de que determinados ámbitos de su vida no se harán públicos; esto es, se mantendrán privados a la intromisión de terceros (incluyendo del gobierno), y (ii) tal expectativa debe ser reconocida por la sociedad como algo razonable; siendo este segundo un elemento objetivo. Conforme a este estándar, aun y cuando un individuo se encuentre en un lugar público puede preservar como privados diversos ámbitos de su vida (por ejemplo, saber que no será grabado dentro de un vestidor en una tienda de ropa o que la conversación que tenga desde una caseta telefónica no será escuchada por terceros). En México dicho estándar se encuentra reconocido en la LFPDPPP, pero todavía está pendiente de que sea interpretado y desarrollado por la autoridad reguladores y nuestros tribunales.
[23] Artículo 7 de la LFPDPPP.
[24] Artículo 45 del Reglamento de la LFPDPPP.
[25] Artículos 6 y 14 de la LFPDPPP, 47 y 48 de su Reglamento.

3.5. AUTORIDAD

La LFPDPPP es el principal cuerpo normativo y tiene por objeto la protección de los datos personales y la finalidad de regular que su tratamiento sea controlado e informado, a efecto de garantizar la privacidad y el derecho a que toda persona pueda decidir qué hacer con su información. La autoridad responsable de que los datos personales sean tratados de conformidad con la LFPDPPP es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

EN RESUMEN...

✓ Un dato personal es cualquier información relacionada a una persona física identificada o identificable.

✓ Según su naturaleza y régimen de protección, los datos personales se pueden clasificar en tres:

1. Generales
2. Sensibles
3. Financieros y patrimoniales

✓ La LFPDPPP establece 8 principios rectores para la protección de datos, los cuales deben regir las actividades de las OSC en esta materia: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad, responsabilidad. Las actividades de las OSC respecto del tratamiento de datos personales se rigen únicamente por la LFPDPPP, sin importar que reciban recursos públicos.

✓ Siempre se debe obtener el consentimiento del titular o representante legal para el tratamiento de datos personales.

✓ Las OSC deben dar a conocer a los titulares de los datos personales, a través del aviso de privacidad, la información relativa a la existencia y características principales del tratamiento a que serán sometidos sus datos personales.

✓ Las OSC sólo pueden recabar y usar datos para las finalidades que especifique en su aviso de privacidad. Si habrá nuevas actividades y proyectos que no estén contemplados en el aviso de privacidad, éste se tiene que modificar con antelación.

✓ Hay que recabar y usar sólo los datos que sean estrictamente necesarios para las actividades de la OSC.

4. LAS OSC Y LOS DATOS PERSONALES

4.1. ¿CUÁNDO UNA OSC SE CONVIERTE EN SUJETO RESPONSABLE?

Toda OSC que trate datos personales está sujeta al cumplimiento de obligaciones en materia de protección de datos personales. Como se explicó antes, la definición de "tratamiento" establecida en la LFPDPPP es muy amplia y abarca todo el ciclo de los datos personales dentro de una OSC, empezando desde el momento en que se obtengan, y abarcando su uso, divulgación, aprovechamiento o almacenamiento por cualquier medio. Quien decida sobre este tratamiento será considerado como responsable, y por ende, sujeto al cumplimiento de los principios y deberes de la LFPDPPP.

En este sentido, las OSC que traten cualquier tipo de dato personal son responsables para efectos de la LFPDPPP.

Las OSC deben contar con planes de capacitación recurrente para sus empleados y colaboradores sobre las obligaciones de la LFPDPPP, así como sobre las medidas y procedimientos internos que establezcan para cumplir con la ley, de manera que exista un entendimiento común institucional sobre qué implicaciones prácticas derivan de la LFPDPPP en el desarrollo de las actividades de la OSC.

4.2. ¿CÓMO SABER SI UNA OSC TRATA DATOS PERSONALES?

Para determinar si una OSC trata datos personales es conveniente responder la siguiente pregunta:

¿La OSC solicita datos personales a personas físicas para establecer con ellas algún tipo de relación?

En caso de contestar afirmativamente, la OSC efectivamente trata datos personales y, por tanto, se encuentra obligada a cumplir con la LFPDPPP. La solicitud de datos personales se puede dar a través de diversas acciones, tales como padrones de beneficiarios, listas de asistencia a actividades o eventos, encuestas, cuestionarios, expedientes personales de donantes, beneficiarios o empleados, procesos de contratación de empleados o voluntarios, entre otros.

4.3. OBTENCIÓN DEL CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS PERSONALES

Con excepción de los supuestos previstos en la LFPDPPP, todo tratamiento de datos personales se encuentra sujeto al consentimiento de su titular[26]. Los responsables tendrán, en todo momento, la carga de la prueba de haber obtenido el consentimiento para llevar a cabo el tratamiento de datos personales. Es importante que las OSC, como cualquier otro sujeto regulado por la LFPDPPP, cuente con un aviso de privacidad que sea puesto a disposición de las personas de quienes se tratarán datos personales y que éstas acepten el mismo.

Al poner a disposición de los individuos un aviso de privacidad y al no manifestar éstos su negativa, otorgan su consentimiento tácito. El consenti-

[26] Artículos 8 y 10 de la LFPDPPP.

miento tácito es, por regla general, suficiente para obtener autorización para el tratamiento de datos personales. Tratándose de datos patrimoniales o financieros, el consentimiento deberá ser expreso. Para el caso de datos sensibles se deberá obtener el consentimiento expreso[27] y por escrito de su titular. En el entorno digital se considera que el consentimiento se obtuvo por escrito cuando se utiliza firma electrónica o cualquier otro mecanismo o procedimiento que permita identificar claramente a los individuos y recabar su consentimiento, como puede ser el marcado de casillas electrónicas.

El mecanismo idóneo para obtener el consentimiento expreso y por escrito es el aviso de privacidad; sin embargo, se pueden utilizar otros medios como pueden ser cartas de autorización independientes. En cualquier caso, es importante que las OSC conserven durante todo el tiempo en que mantengan datos personales y posteriormente durante los plazos de prescripción correspondientes[28], los avisos de privacidad, u otros documentos/medios físicos o electrónicos, a través de los cuales se acredite que se obtuvo el consentimiento.

No se requiere consentimiento cuando el tratamiento de los datos personales tenga el propósito de cumplir obligaciones derivadas directamente de la relación jurídica que las OSC tengan con los individuos. Es decir, que sean necesarias para el cumplimiento y mantenimiento de la relación legal. Tampoco se requiere el consentimiento cuando tal situación esté prevista en una ley, los datos personales se sometan a un procedimiento previo de disociación, y otros supuestos previstos en la LFPDPPP. Lo anterior, no exime a las OSC de su obligación de informar, a través de su aviso de privacidad, sobre las finalidades para las cuales serán tratados sus datos personales.

Para finalidades secundarias, como son fines de mercadotecnia, publicidad y prospección comercial, los titulares de los datos personales deben tener la opción de manifestar su negativa para el tratamiento de sus datos personales para estos propósitos previo al tratamiento de su información personal. El momento ideal es cuando se pone a disposición el aviso de privacidad y puede ser por escrito (si se obtienen los datos de manera personal) o con casillas de verificación (si los datos personales se obtienen a través de medios tecnológicos). También podrán revocar su consentimiento posteriormente mediante el procedimiento de ejercicio de derechos ARCO que se explica más adelante.

De conformidad con el principio de proporcionalidad (mencionado en la sección 2 anterior), cada responsable debe tratar únicamente aquellos datos personales de los titulares que sean estrictamente necesarios para regular la relación que guardan con éstos.

Es importante tomar en cuenta que en términos de la fracción I del artículo 10 de la LFPDPPP, en la medida en que las OSC deban recabar datos personales para cumplir con la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (prevención de lavado de dinero) podrán prescindir del con-

[27] El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos. Ver artículo 8 de la LFPDPPP.
[28] A reserva de que la OSC revise cada caso en concreto con su departamento legal o asesor jurídico, se recomienda tomar como plazo de prescripción legal el establecido en el artículo 1159 del Código Civil Federal, es decir 10 años. Para mayor referencia, el artículo mencionado dispone lo siguiente: "Fuera de los casos de excepción, se necesita el lapso de diez años, contado desde que una obligación pudo exigirse, para que se extinga el derecho de pedir su cumplimiento."

sentimiento de los titulares para tratar tales datos personales. Esto, en virtud de que dicha ley obliga a las OSC a recabar ciertos datos personales relacionados con donativos susceptibles de identificación o aviso; pero en el entendido que deberán seguir cumpliendo a cabalidad con todos los otros principios y deberes de la protección de datos personales explicados en el presente manual.

Las OSC deben contar con una estrategia para comunicar adecuadamente esta situación a los donantes: de una parte, la necesidad de contar con la información que la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (prevención de lavado de dinero) señala, pero que la OSC tratará esos datos con las mismas protecciones y bajo los mismos principios que otros datos personales.

4.4. CASOS MÁS COMUNES

4.4.1. Datos personales de beneficiarios o usuarios

Las OSC generalmente tratan datos personales de sus beneficiarios o usuarios. Con respecto a los beneficiarios, el tipo de tratamiento dependerá del propósito de la OSC y los datos personales que éstas obtienen. A manera de ejemplo, existirán casos en que las OSC, además de los datos personales generales o de identificación, traten datos personales sensibles que tendrán como objeto identificar a personas que, conforme a su objeto, requieren recibir apoyos o a las que se les presta un servicio. Lo más recomendable es que las OSC cuenten con avisos de privacidad específicos para cada categoría de titulares de datos personales, conforme a sus actividades y necesidades.

Toda OSC debe cuidar que no se traten más datos personales que los esencialmente necesarios para cumplir el propósito de la misma y que, el consentimiento obtenido para dicho tratamiento sea el requerido conforme a los señalado en el apartado que antecede (implícito, expreso o expreso por escrito).

4.4.2. Datos personales de candidatos o empleados

Para el debido tratamiento de los datos personales de candidatos a un puesto de trabajo es necesario que, al primer contacto que se tenga con éstos, se les proporcione el aviso de privacidad y se obtenga el consentimiento para el tratamiento de su información personal.

Es recomendable que en las solicitudes de empleo solamente sean requeridos datos personales esenciales y justificados para conocer por parte del entrevistador o la persona que estará encargada de evaluar las capacidades y aptitudes del candidato para el desempeño de un puesto vacante, lo cual suele incluir su trayectoria laboral y experiencia académica.

Una vez que una persona es contratada por una OSC se deberá obtener toda la información necesaria para la celebración y el cumplimiento de la relación laboral, incluyendo aquella requerida para la preparación de su contrato laboral, el pago de su salario, evaluar su desempeño, entre otra.

Por otra parte, una vez que ha finalizado el proceso de contratación o la relación laboral, se deben destruir todos los datos personales respecto de los cuales ya no exista una razón legítima para mantenerlos.

Todos los empleadores, al ser sujetos de cum-

plimiento de la LFPDPPP, deben cumplir con las obligaciones que se establecen en ella. Las OSC, al ser empleadores, también deben cumplir con este aspecto de la LFPDPPP en su relación con sus candidatos a empleo, empleados y otro tipo de colaboradores.

4.4.3. Datos personales de donantes

Los donantes son parte esencial de una OSC, ya que ellos forman uno de los pilares más importantes para su funcionamiento y solvencia. Por lo anterior, es necesario que las personas encargadas en tratar su información personal, que generalmente incluye datos personales financieros (como es datos de tarjetas de crédito) estén conscientes que estos datos deben ser cuidados y valorados a efecto de no realizar actos que vayan en contra de la voluntad de contribuir a una OSC como donantes.

Existen casos en los que el personal que trabaja en OSC distintas, solicita a amigos o conocidos que trabajan en otra OSC, que le compartan los datos de contacto de sus donantes para informarles de su proyecto. A pesar de que esta práctica tiene un fin loable, es contraria los principios establecidos por la LFPDPPP, ya que como regla general, cualquier transferencia de datos personales debe ser consentida por su titular, a través de una cláusula de aceptación incluida en el aviso de privacidad proporcionado a las donantes personas físicas. Para mayor referencia, se pueden consultar los principios que rigen el tratamiento de datos personales.

4.4.4. Datos personales de otros tipos de titulares (individuos)

Como se explicó anteriormente, las OSC por lo general tratan datos personales de beneficiarios o usuarios, candidatos a empleo o empleados y de donantes, pero podrían tratar datos personales de otro tipo de titulares (individuos). En todo caso, el tratamiento de datos personales debe encontrarse justificado y cualquier relación que el responsable (en este caso, la OSC) establezca con personas físicas de quienes recabe datos personales debe regularse por un aviso de privacidad, el cual variaría tanto en los datos personales que se obtengan como en las finalidades y las transferencias realizadas. No es lo mismo tratar información de un empleado o candidato, que aquellos que corresponden a un donante o beneficiario -ya que las finalidades del tratamiento varían de caso a caso- y, por tanto, los datos personales requeridos también son diferentes.

Por lo anterior, es necesario plantearse las siguientes preguntas que orientan para saber qué información se puede/debe recabar en cada relación que establezca un responsable:

- ¿Cuál es el objeto de la relación con la persona?

- ¿Qué datos personales son necesarios para cumplir el objeto de la relación?

- Además de las finalidades esenciales para cumplir el objeto de la relación, ¿existen finalidades adicionales? En caso afirmativo, ¿qué datos personales se requieren y cuál es el objeto?

- ¿Habrán transferencias de los datos personales que se obtendrán? ¿Para qué objeto?

Habiendo contestado estas preguntas, el responsable tendrá elementos para poder elaborar el aviso de privacidad respectivo y crear los procesos internos dentro de la OSC para que el tratamiento de dicha información se realice en cumplimiento de los principios establecidos en la LFPDPPP.

4.5. TRANSFERENCIAS Y REMISIONES DE DATOS PERSONALES

La LFPDPPP y su Reglamento prevén dos supuestos que se refieren a la compartición de datos personales con terceros y, a pesar de ser parecidos, cada uno de ellos tiene diferentes implicaciones tanto en las obligaciones que tiene el responsable frente al titular de los datos como las que éste adquiere frente a la ley; se trata de las transferencias y las remisiones.

4.5.1. Transferencias[29]

La transferencia de datos personales tiene lugar cuando una OSC comparte datos personales fuera de su organización con un tercero que no los tratará por cuenta y en representación de la OSC. Para ilustrar lo anterior, un ejemplo práctico es aquel en que una OSC comparte datos personales de sus donantes con otra asociación u organización para que ésta pueda informar al donante de la labor que realiza.[30]
De conformidad con la LFPDPPP y su Reglamento, por regla general toda transferencia debe ser consentida por el titular de los datos, es decir, la OSC requiere contar con el consentimiento del titular previo a realizarla. El consentimiento se debe obtener a través de una cláusula incluida en el propio aviso de privacidad. En caso contrario se estaría violando el deber de confidencialidad al que están sujetos todos aquellos particulares que tratan datos personales.

En los siguientes casos no es necesario contar con el consentimiento de los individuos para transferir datos personales a terceros:

1. Que exista una disposición legal que obligue a las OSC a transferir los datos personales.

2. Que la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios.

3. Que la transferencia sea realizada a sociedades controladoras, subsidiarias o afiliadas de la OSC, bajo control común o con cualquier otra sociedad del mismo grupo que opere bajo los mismos procesos o políticas internas. Por ejemplo, organizaciones internacionales con presencia en diferentes lugares u organizaciones que tengan diferentes sedes u oficinas y que operen bajo los mismos procesos y políticas internas.

En la sociedad civil organizada, es común que se conformen colectivos o agrupaciones que frecuentemente son de carácter informal, es decir, no se establece una relación jurídica corporativa u orgánica entre las OSC que los conforman. Dado que en estos casos no hay un control común ni las mismas políticas internas sobre el tratamiento de datos personales porque cada organización conserva autonomía e independencia, los datos personales no se deben transferir sin que exista consentimiento de los titulares.

4. Que la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés de los individuos con un tercero.

---

[29]Artículos 67 a 76 del Reglamento de la LFPDPPP.
[30]Cuando una OSC comparte datos personales con un prestador de servicios no es considerado una "transferencia", sino una "remisión" de datos tal como se explica en la siguiente sección. Ver también artículos 2, fracción IX y 53 del Reglamento de la LFPDPPP.

5. Que la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia.

6. Que la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

7. Que la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre la OSC y los individuos.

En caso de que la OSC vaya a recibir datos personales por transferencia de otro particular, hay que firmar un acuerdo en el que el responsable que transferirá los datos cumpla con todos los requisitos de ley para la transferencia y se haga responsable por cualquier reclamación o sanción administrativa que ocurra por su incumplimiento de la normativa o del acuerdo que firmó en relación con los datos transferidos.

Antes de llevar a cabo cualquier transferencia de datos personales con base en estas excepciones es conveniente que la OSC confirme con su encargado de datos personales, y si es necesario con un abogado especialista en el tema, si efectivamente se actualiza el supuesto correspondiente. Eso ayudará a las OSC a cumplir con sus obligaciones señaladas en la LFPDPPP.

4.5.2. Remisiones

Las remisiones de datos personales tienen lugar cuando la OSC los comparte con una persona física o moral ajena a la OSC, a fin de que dicho tercero preste un servicio al responsable de los datos y que pueda cumplir con el objeto de la relación con el titular de los mismos. A estos terceros se les denomina "encargados" en la LFPDPPP y únicamente puede tratar los datos de conformidad con las instrucciones de la OSC, y por su cuenta y representación.

Un ejemplo de una remisión es aquel en que una OSC contrata a un prestador de servicios de nómina para que éste se encargue de la gestión de los pagos de los empleados mes a mes, en dicha relación es necesario que la OSC comparta los datos personales de sus empleados con la empresa de gestión de nómina para efecto de que, los empleados, mes a mes puedan recibir su sueldo.

Otro ejemplo puede ser en caso de que la OSC requiera enviarles un paquete a sus donadores con folletos de la OSC así como con información del uso que se le ha dado a sus donaciones; para tal efecto, la OSC contrata a una empresa de mensajería o, en caso de hacer esto de manera electrónica, a una empresa de gestión y administración de comunicaciones a través de correo electrónico, a las cuales les comparte los datos personales de los donantes para que éstos reciban la información.

De conformidad con la LFPDPPP y su Reglamento, las remisiones de los datos personales no deben ser informadas ni tampoco contar con el consentimiento de los titulares. En el entendido que la OSC seguirá siendo responsable ante los titulares (donantes, empleados, beneficiarios) del tratamiento que los encargados les den a sus datos personales, por lo que las OSC se deben asegurar el debido tratamiento que éstos les den a los datos personales. Toda relación entre las OSC y los encargados debe quedar documentada en contratos que permitan acreditar la existencia de la relación entre las partes y su alcance y contenido.

4.6. ¿QUÉ SUCEDE CUANDO UNA OSC RECIBE FONDOS GUBERNAMENTALES?

Es importante distinguir que el tratamiento de datos personales en posesión de autoridades está regulado en una ley independiente denominada Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la cual no aplica a las OSC por disposición expresa[31]. Las OSC deben tener en cuenta que aun y cuando reciban recursos gubernamentales (estatales y/o federales) la ley que les es aplicable respecto al tratamiento de datos personales sigue siendo la LFPDPPP. Este manual se centra en el cumplimiento de las obligaciones y deberes establecidos en la LFPDPPP que es aplicable a los particulares, tales como las OSC.

[31] Supra. nota 6.

EN RESUMEN...

✓ Toda OSC que trate datos personales (ya sea de empleados, donantes, beneficiarios, usuarios, clientes, voluntarios, colaboradores, candidatos a empleo, etc.) está sujeta al cumplimiento de la LFPDPPP.

✓ Es indispensable que las OSC incorporen capacitación en protección de datos personales para todos los empleados y colaboradores de la OSC.

✓ Las OSC tienen que documentar que han obtenido el consentimiento de los titulares para recabar y usar sus datos personales. Esto se hace a través del aviso de privacidad.

✓ Las OSC deben contemplar al menos los siguientes casos para la elaboración de su(s) aviso(s) de privacidad:

1. Beneficiarios o usuarios.
2. Candidatos o empleados.
3. Donantes (personas físicas).
4. Otras personas físicas con las que exista una relación y se requiera de sus datos personales.

✓ Las OSC pueden transferir datos personales a terceros, siempre que los titulares lo consientan o se trate de un caso de excepción. Las transferencias deben estar contempladas en el aviso de privacidad.

✓ Los colectivos o agrupaciones de OSC de carácter informal (es decir, que no hay una relación jurídica corporativa u orgánica entre las OSC que los conforman) no entran en la excepción al consentimiento para las transferencias, por lo que hay que evitar compartir datos personales entre organizaciones bajo estos esquemas de colaboración si no se cuenta con el consentimiento de los titulares.

✓ La OSC pueden remitir datos personales a terceros para que éstos presten un servicio a la OSC para que ésta pueda cumplir con la relación que tiene con los titulares. Estos terceros son encargados y tratan los datos personales conforme a las instrucciones de la OSC. Toda relación entre las OSC y los encargados debe quedar documentada en contratos que permitan acreditar la existencia de la relación entre las partes y su alcance y contenido.

5. EL AVISO DE PRIVACIDAD

Una de las principales obligaciones que deben cumplir los responsables del tratamiento de datos personales es contar con un aviso de privacidad, el cual, de conformidad con la LFPDPPP es un documento físico, electrónico o en cualquier otro formato (e.j. sonoro), a través del cual se informe a los titulares sobre la existencia, finalidades y características principales del tratamiento al que serán sometidos los datos personales que se recaben. Las omisiones en el aviso de privacidad pueden ser sancionadas con multas, según se explica en el capítulo 9 del presente Manual.

Es importante señalar que todo responsable de datos personales debe, por regla general, entregar a los titulares de datos personales un aviso de privacidad previo a recabar sus datos personales. Todos los particulares que tratan datos personales, incluyendo las OSC, deben cumplir con el principio de información y esto se logra principalmente con la puesta a disposición de los titulares del aviso de privacidad.

¿POR DÓNDE EMPEZAR?

¡Visita el generador de avisos de privacidad del INAI!
Esta herramienta permite crear avisos de privacidad de manera rápida, sencilla y gratuita: https://generador-avisos-privacidad.inai.org.mx/

5.1. ¿PARA QUÉ SIRVE?

El aviso de privacidad tiene como propósito principal informar a los titulares sobre el alcance, términos y condiciones del tratamiento de sus datos personales y sobre los derechos con los que cuentan en relación con el tratamiento de su información personal, a fin de que el titular pueda decidir si desea entregarle sus datos al responsable y, en su caso, saber con qué derechos cuenta en relación con sus datos personales. En otras palabras, el aviso de privacidad proporciona a los particulares información para tomar decisiones informadas en relación a sus datos personales y saber que cuentan con cierto control y con la facultad de disponer de su información.

5.2. ¿QUÉ ELEMENTOS DEBE CONTENER?

El aviso de privacidad integral[32] deberá contener, al menos, la información abajo listada, en el entendido que los responsables podrían también informar a los particulares otros temas, tales como la descripción de medidas de seguridad que tienen implementadas, con qué subcontratistas comparten los datos personales, a través de qué medios obtienen los datos personales, entre otros:

1. La identidad y domicilio del responsable que trata los datos personales.
2. Los datos personales que serán sometidos a tratamiento.
3. El señalamiento expreso de los datos personales sensibles que se tratarán.
4. Las finalidades del tratamiento.
5. Los mecanismos para que el titular pueda manifestar su negativa para el tratamiento de sus datos personales para aquellas finalidades que no son necesarias, ni hayan dado origen a la relación jurídica con el responsable.
6. Las transferencias de datos personales que, en su caso, se efectúen; el tercero receptor de los datos personales, y las finalidades de las mismas.
7. La cláusula que indique si el titular acepta o no la transferencia, cuando así se requiera.
8. Los medios y el procedimiento para ejercer los derechos ARCO.[33]
9. Los mecanismos y procedimientos para que, en su caso, el titular pueda revocar su consentimiento al tratamiento de sus datos personales.
10. Las opciones y medios que el responsable ofrece al titular para limitar el uso o divulgación de los datos personales.
11. La información sobre el uso de mecanismos en medios remotos o locales de comunicación electrónica, óptica u otra tecnología, que permitan recabar datos personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos, en su caso.
12. Los procedimientos y medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

¿CÓMO SABER SI EL AVISO DE PRIVACIDAD DE UNA OSC ES SENCILLO Y COMPRENSIBLE?

1. Está redactado con información necesaria, expresado en lenguaje claro.
2. No tiene frases inexactas, ambiguas o vagas.
3. Su lenguaje toma en cuenta los perfiles de los titulares de los datos personales.
4. No induce a los titulares a elegir una opción en específico.
5. Las casillas de verificación para otorgar consentimiento (si las hay), no aparecen previamente marcadas.
6. No remite a textos o documentos que no estén disponibles para el titular.

[32] Ver artículo 15 de la LFPDPPP Lineamiento Vigésimo de los Lineamientos del Aviso de Privacidad. Las modalidades del aviso de privacidad se explican en la sección 5.6. del presente manual.
[33] Ver capítulo 7 del presente manual.

Cuando se deban utilizar datos de menores de edad o de personas en estado de incapacidad, es necesario recabar el consentimiento de la persona que ejerce la patria potestad, el tutor o representante legal, según sea el caso, de conformidad con las reglas de representación del Código Civil aplicable. El aviso de privacidad se debe entregar a tales personas y en el mismo se debe aclarar que se están tratando datos personales de menores y cómo se cuidan.

En caso de que el responsable desee tratar fotografías, deberá mencionarlo expresamente en el aviso de privacidad, así como cumplir con lo establecido en el artículo 87 de la Ley Federal del Derecho de Autor, el cual dispone que "el retrato de una persona sólo puede ser usado o publicado, con su consentimiento expreso, o bien con el de sus representantes o los titulares de los derechos correspondientes". Esto significa que el responsable deberá obtener una carta de consentimiento para uso de retratos que cumpla con lo establecido en la Ley Federal del Derecho de Autor, así como el aviso de privacidad.

5.3. TIPOS DE AVISOS DE PRIVACIDAD

El aviso de privacidad puede ser:

1. Físico (e.j. escrito en papel)
2. Electrónico (e.j. colocado en la página, sitio web o correos electrónicos)
3. Sonoro (e.j. grabación telefónica)

5.4. ¿DÓNDE SE DEBE PUBLICAR?

El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología, de la siguiente manera:

Cuando los datos personales sean obtenidos personalmente del titular, el aviso de privacidad deberá ser facilitado en el momento en que se tiene el primer contacto con él o ella y previo a que se recabe su información, salvo que se hubiera facilitado el aviso de privacidad en un momento previo. Por ejemplo, en el primer contacto que se tenga con un candidato a un empleo y previo a recabar sus datos personales, se le deberá proporcionar el aviso de privacidad.

Cuando los datos personales sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología; como podría ser cuando un donante proporciona sus datos a una OSC a través de su página de internet o vía telefónica, el aviso de privacidad debe estar disponible en línea o en una grabación telefónica a la que deben tener acceso los donantes, previo a entregar sus datos personales.

Es recomendable que el aviso de privacidad se elabore de la mano con un especialista en la materia para que éste refleje lo que efectivamente hará la OSC con los datos personales que recabe, así como cumplir cabalmente con las obligaciones derivadas de la LFPDPPP. Adicionalmente, el plan de capacitación para empleados y colaboradores de la OSC deberá enfocarse también en conocer el contenido del aviso de privacidad de la organización, así como revisarlo periódicamente para asegurarse que sigue estando vigente material y normativamente.

EL ABC DEL AVISO DE PRIVACIDAD

El INAI cuenta con una guía para redactar el aviso de privacidad, así como ejemplos y modelos, que pueden ser de utilidad para las OSC. Visita: http://abcavisosprivacidad.ifai.org.mx/#seccion5

5.5. MODALIDADES DEL AVISO DE PRIVACIDAD

El aviso de privacidad puede tener varias modalidades[34] dependiendo de las circunstancias específicas en las que se recaben los datos personales y los medios utilizados para la obtención de los mismos. Cada modalidad tiene diferentes elementos informativos, como a continuación se sintetiza:

MODALIDAD	ELEMENTOS INFORMATIVOS
Integral	1. La identidad y domicilio del responsable que trata los datos personales. 2. Los datos personales que serán sometidos a tratamiento. 3. El señalamiento expreso de los datos personales sensibles que se tratarán. 4. Las finalidades del tratamiento, distinguiendo entre finalidades que son necesarias y dieron origen a la relación jurídica entre la OSC y el individuo, de las que no lo son (haciendo referencia explícita en caso de que los datos se usen para finalidades de mercadotecnia y publicidad) y señalando el mecanismo para que el titular pueda manifestar su negativa para que sus datos personales sean tratados para finalidades no estrictamente relacionadas con la relación legal. 5. Los mecanismos para que el titular pueda manifestar su negativa para el tratamiento de sus datos personales para aquellas finalidades que no son necesarias, ni hayan dado origen a la relación jurídica con el responsable. 6. Las transferencias de datos personales que, en su caso, se efectúen; el tercero receptor de los datos personales, y las finalidades de las mismas.

[34] Ver capítulos IV y V de los Lineamientos del Aviso de Privacidad (publicados el 17 de enero de 2013). Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5284966&fecha=17/01/2013

7. La cláusula que indique si el titular acepta o no la transferencia, cuando así se requiera.

8. Los medios y el procedimiento para ejercer los derechos ARCO.

9. Los mecanismos y procedimientos para que, en su caso, el titular pueda revocar su consentimiento al tratamiento de sus datos personales.

10. Las opciones y medios que el responsable ofrece al titular para limitar el uso o divulgación de los datos personales.

11. La información sobre el uso de mecanismos en medios remotos o locales de comunicación electrónica, óptica u otra tecnología, que permitan recabar datos personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos, en su caso.

12. Los procedimientos y medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

Simplificado

1. La identidad y domicilio del responsable que los recaba.

2. Las finalidades del tratamiento de datos, distinguiendo entre finalidades que son necesarias y dieron origen a la relación jurídica entre la OSC y el individuo, de las que no lo son (haciendo referencia explícita en caso de que los datos se usen para finalidades de mercadotecnia y publicidad) y señalando el mecanismo para que el titular pueda manifestar su negativa para que sus datos personales sean tratados para finalidades no estrictamente relacionadas con la relación legal.

3. Los mecanismos que el responsable ofrece para que el titular conozca el aviso de privacidad integral, así como ejercer la negativa para el uso de datos en finalidades secundarias (tales como mercadotecnia).

Esta modalidad de aviso de privacidad se suele usar cuando se quiere proporcionar a los individuos una versión más corta del aviso integral, que puedan leer de forma más rápida y eficiente; siempre, en el entendido que después deben poder conocer el aviso completo.

Corto	I	La identidad y domicilio del responsable;
	2	Las finalidades del tratamiento, distinguiendo entre finalidades que son necesarias y dieron origen a la relación jurídica entre la OSC y el individuo, de las que no lo son (haciendo referencia explícita en caso de que los datos se usen para finalidades de mercadotecnia y publicidad). Sin que se tenga que señalar el mecanismo para que el titular pueda manifestar su negativa para que sus datos personales sean tratados para finalidades no estrictamente relacionadas con la relación legal. Los mecanismos que el responsable ofrece para que el titular conozca el aviso de privacidad integral.
	3	Este aviso se debe usar únicamente para espacios reducidos y de manera excepcional.

Las OSC tienen la obligación de crear aviso(s) de privacidad integral(es), mientras que contar con una versión simplificada es recomendable para informar a los titulares de una manera más rápida y accesible.

MODALIDAD DE AVISO	NIVEL DE OBLIGATORIEDAD
Integral	Obligatorio
Simplificado	Recomendable
Corto	Excepcional

La utilización de cada modalidad depende del medio de obtención de los datos, como se resume a continuación:

OBTENCIÓN DE LOS DATOS	¿QUÉ SIGNIFICA?	¿CUÁNDO PONER A DISPOSICIÓN EL AVISO DE PRIVACIDAD?	¿QUÉ MODALIDAD DEL AVISO DE PRIVACIDAD CORRESPONDE?
Directa	El propio titular proporciona los datos personales por algún medio que permite su entrega directa al responsable, entre ellos, medios electrónicos, ópticos, sonoros, visuales o cualquier otra tecnología, como correo postal, internet o vía telefónica, entre otros.	El responsable deberá poner a su disposición el aviso de privacidad previo a la obtención de los mismos.	Integral o simplificado
Indirecta	El responsable obtiene los datos personales sin que el titular se los haya proporcionado de forma personal o directa, como por ejemplo a través de una fuente de acceso público o una transferencia.	1) Si los datos proceden de una transferencia o fuente de acceso público: el responsable receptor o que obtiene los datos personales deberá poner a disposición el aviso de privacidad al primer contacto con el titular. 2) Si el tratamiento no requiere contacto con el titular, el responsable deberá hacer de su conocimiento el aviso de privacidad previo al aprovechamiento de los datos personales para la finalidad respectiva.	Integral o simplificado

Personal	El titular proporciona los datos personales al responsable o a la persona física designada por el responsable, con la presencia física de ambos.	El responsable deberá poner a su disposición el aviso de privacidad previo a la obtención de los mismos.	Integral

Cuando el espacio utilizado para la obtención de los datos personales sea mínimo y limitado, de forma tal que los datos personales recabados o el espacio para la difusión o reproducción del aviso de privacidad también lo sean, se podrá utilizar la modalidad de aviso de privacidad corto. Algunos casos en los que esto puede ser necesario son rifas (por el espacio reducido de talonarios), o listas de asistencia o registro para cursos o eventos.

La puesta a disposición del aviso de privacidad simplificado o corto no exime a la OSC de su obligación de proveer los mecanismos para que el titular pueda conocer el contenido del aviso de privacidad integral.

EN RESUMEN...

✓ El aviso de privacidad es un documento físico, electrónico o en cualquier otro formato (e.j. sonoro), a través del cual se informa a los titulares sobre la existencia, finalidades y características principales del tratamiento al que serán sometidos los datos personales que se recaben.

✓ El aviso de privacidad proporciona a los particulares información que les permite tomar decisiones informadas con relación a sus datos personales y saber que cuentan con cierto control y con la facultad de disponer de su información.

✓ El aviso de privacidad puede tener tres modalidades: integral, simplificado o corto.

✓ Las OSC están obligadas a desarrollar el aviso de privacidad integral, aunque es altamente recomendable contar con una versión simplificada.

✓ La información que debe contener el aviso de privacidad integral es:

1. La identidad y domicilio del responsable.
2. Los datos personales que serán sometidos a tratamiento.
3. El señalamiento expreso de los datos personales sensibles que se tratarán.
4. Los mecanismos para que el titular pueda manifestar su negativa para finalidades que no son necesarias, ni que hayan dado origen a la relación jurídica con el responsable.
5. Las transferencias de datos personales, el tercero receptor y las finalidades de las mismas.
6. La cláusula que indique si el titular acepta o no la transferencia, cuando así se requiera.
7. Los medios y el procedimiento para ejercer los derechos ARCO.
8. Los mecanismos y procedimientos para revocar su consentimiento al tratamiento de sus datos personales.
9. Las opciones y medios que el responsable ofrece al titular para limitar el uso o divulgación de los datos personales.
10. La información sobre el uso de mecanismos en medios remotos o locales de comunicación electrónica, óptica u otra tecnología, que permitan recabar datos personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos.
11. Los procedimientos y medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

✓ Es recomendable que el aviso de privacidad se elabore de la mano con un especialista en la materia para que este refleje lo que efectivamente hará la OSC con los datos personales que recabe, así como cumplir cabalmente con las obligaciones derivadas de la LFPDPPP.

6. DEBERES DE LAS OSC COMO SUJETOS RESPONSABLES

6.1. CONFIDENCIALIDAD

La confidencialidad es la garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona. Cada individuo tiene derecho a proteger su información personal. Cuando decide compartir dicha información se debe asegurar al individuo que sus datos personales continuarán siendo confidenciales.

En este contexto, cada OSC, y todo tercero encargado, deben guardar estricta confidencialidad respecto de los datos personales que les proporcionan los individuos. Esta obligación subsiste aun después de finalizada la relación entre la OSC y los titulares. Conforme a lo anterior, solamente se pueden compartir los datos personales con prestadores de servicios con los que haya formalizado su relación jurídica en términos de lo señalado anteriormente en este manual y hacer transferencias de datos también conforme a lo aquí establecido.

6.2. MEDIDAS DE SEGURIDAD

En cumplimiento del denominado deber de seguridad o cuidado, tanto responsables como encargados tendrán la obligación de implementar medidas de seguridad físicas, administrativas y técnicas para proteger los datos personales que traten contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado, así como para guardar la confidencialidad de los mismos. Dichas medidas no podrán ser menores a aquellas que mantengan para el manejo de su información. En otras palabras, las medidas utilizadas por las OSC para cuidar los datos personales no deben ser menores a aquellas usadas para proteger su propia información (financiera, estratégica, comercial, etc).

A continuación, se describen algunos ejemplos de cada una de las medidas.

6.2.1. Medidas físicas

Las medidas de seguridad físicas son el conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología, destinadas para: (i) prevenir el acceso no autorizado, el daño o la interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información, (ii) proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones, (iii) proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad, y (iv) garantizar la eliminación segura de datos personales.

MEDIDAS DE SEGURIDAD FÍSICA PUEDE SER:

- **Cerraduras y/o claves de acceso donde se archivan datos personales**
- **Protección física de equipos móviles como celulares, tabletas o computadoras**
- **Trituradoras de papel para eliminar datos personales de forma segura**

Soportes físicos tales como archiveros, gavetas, anaqueles y bodegas en los cuales se procesan y almacenan dichos datos, cuyo acceso se logrará con llaves asignadas únicamente a las personas encargadas del tratamiento de datos personales. No se podrá dar acceso a terceros que no tengan una causa justificada en función de su puesto y de sus funciones para conocer la información almacenada en soportes físicos. De igual forma, en caso de tenerse una llave o clave de acceso a los mismos, esta deberá ser resguardada en un lugar seguro y no ser prestada o proporcionada a ningún tercero. La persona a quien se le otorgue una clave de acceso o llave para acceder a los soportes físicos en donde se encuentren respaldados datos personales, será responsable del debido cuidado de la misma.

6.2.2. Medidas organizacionales o administrativas

Las medidas de seguridad administrativas son: el conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel de la organización. La identificación y clasificación de los datos personales, así como la concienciación, formación y capacitación del personal de cada OSC en esta materia son medidas de seguridad administrativas.

Entre las medidas de seguridad administrativas para el cuidado de datos personales se encuentran las siguientes:

1. Inventario de datos personales y de los sistemas de tratamiento.

2. Registro de los medios de almacenamiento de los datos personales.

3. Determinación de funciones y obligaciones de los cargos dentro de cada OSC que tratan datos personales.

4. Programa de revisiones y auditorías, para evaluar y medir el cumplimiento de este manual.

5. Implementación de análisis de riesgos periódicos para identificar peligros y maneras de reducir tales riesgos.

6. Anualmente, llevar a cabo un ejercicio para identificar medidas de seguridad que han sido implementadas de manera efectiva, e identificación de medidas de seguridad faltantes.

7. Plan de trabajo para implementación de medidas de seguridad faltantes en términos del análisis antes señalado.

8. Capacitación del personal de cada OSC que efectúe el tratamiento de datos personales, conforme a lo señalado en este manual.

MEDIDAS DE SEGURIDAD ORGANIZACIONALES PUEDEN SER:

- **Inventarios de datos personales y sistemas de tratamiento**
- **Determinación clara de funciones y roles dentro de la OSC respecto del tratamiento de datos personales**
- **Revisiones de medidas de seguridad**
- **Auditorías de cumplimiento**
- **Análisis de riesgo periódicos**
- **Planes de trabajo**
- **Capacitación**

Para poder implementar correctamente todas estas medidas, es indispensable que los responsables capaciten a sus empleados y colaboradores frecuentemente para estar en posibilidades de cumplir con las obligaciones que marca la LFPDPPP. Llevar a cabo de forma periódica revisiones internas, y auditorías externas, sirve para verificar que lo establecido en este manual efectivamente se está implementando y cumpliendo dentro de la OSC y ayuda a que las OSC se mantengan vigentes y al día en el cumplimiento de sus obligaciones derivadas de la LFPDPPP; incluyendo con el principio de responsabilidad que se explica en este documento. La persona encargada de cumplimiento en temas de protección de datos personales dentro de cada OSC se debe cerciorar de que por lo menos cada 6 meses se implemente una revisión interna de cumplimiento de este manual.

6.2.3. Medidas técnicas

Las medidas de seguridad tecnológicas son el conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la seguridad para asegurar que: (i) el acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados, (ii) que los usuarios que accedan a la información lo hagan al llevar a cabo actividades que lo requieran con motivo de sus funciones, (iii) se implementen acciones para la adquisición, operación, desarrollo y mantenimiento de sistemas seguros, y (iv) se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales.

Soportes electrónicos desde donde se traten los datos personales y se guarde la base de datos, acceso a los datos o archivos únicamente a través de contraseñas asignadas a cada uno de los usuarios; protector de pantalla con solicitud de contraseña para desbloqueo; mecanismos contra código malicioso; establecimiento de contraseñas a la red inalámbrica; instalar actualizaciones de seguridad en los equipos de forma semestral, etc.

MEDIDAS DE SEGURIDAD TÉCNICAS PUEDEN SER:

- **Asignar contraseñas de acceso a todos los equipos electrónicos**
- **Protectores de pantalla con solicitud de contraseña para desbloquear**
- **Contraseñas para la red inalámbrica que use la OSC o sus colaboradores (sea en oficina o en casa)**
- **Contraseñas para acceder a bases de datos**
- **Encriptar comunicaciones electrónicas de la OSC**

En la implementación de las medidas de seguridad, las OSC pueden tomar en cuenta el siguiente material desarrollado y publicado por el INAI:

1. Recomendaciones en materia de seguridad de datos personales, disponible en **http://inicio.ifai.org.mx/MarcoNormativoDocumentos/RECOMENDACIONES%20EN%20MATERIA%20DE%20SEGURIDAD%20DE%20DATOS%20PERSONALES.pdf**

2. Tabla de equivalencia funcional entre estándares de seguridad y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, su reglamento y las Recomendaciones en materia de seguridad de datos personales, disponible en **http://inicio.inai.org.mx/DocumentosdeInteres/Tabla_de_Equivalencia_Funcional(Junio2015).pdf**

3. Manual en materia de seguridad de datos personales para MiPyMEs y organizaciones pequeñas mexicanas, disponible en **http://inicio.ifai.org.mx/nuevo/Manual%20seguridad%20MIPYMES.pdf**

4. Manual en materia de seguridad basada en un entorno Microsoft para MiPyMEs y organizaciones pequeñas mexicanas, disponible en **http://inicio.inai.org.mx/DocumentosdeInteres/Manual_Microsoft.pdf**

5. Guía para el tratamiento de datos biométricos, disponible en **http://inicio.inai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf**

6.3. PERSONA O DEPARTAMENTO DE DATOS PERSONALES

Todo responsable deberá designar a una persona o departamento de datos personales[35], quien dará trámite a las solicitudes de los titulares para el ejercicio de los derechos a que se refiere la LFPDPPP. Asimismo, la persona o el departamento encargado tendrá la obligación de fomentar la protección de datos personales al interior de la organización, en este caso, la OSC. Esta obligación puede recaer en un departamento ya establecido dentro de la OSC, como podría ser el departamento legal o de cumplimiento, o cualquier otra área con funciones afines a las actividades de protección de datos personales.

[35] También conocido como Oficial de Protección de Datos Personales, Departamento de Protección Datos Personales, Persona Designada para la Protección de Datos Personales, o Chief Privacy Officer.

En caso de tener dudas sobre la mejor persona o departamento para asumir estas responsabilidades, se recomienda consultar las "Recomendaciones para la Designación de la Persona o Departamento de Datos Personales" emitido por el INAI y que se encuentra disponible en: **http://inicio.ifai.org.mx/DocumentosdeInteres/RecomendacionesDesignar.pdf.**

6.4. ¿QUÉ HACER FRENTE A UNA VULNERACIÓN DE BASES DE DATOS?

Existe una vulneración a la seguridad de las bases de datos personales mantenidas por una OSC, cuando en cualquier fase de tratamiento tiene lugar alguno de los siguientes acontecimientos:

- Pérdida o destrucción no autorizada de datos personales.
- Robo, extravío o copia no autorizada.
- Uso, acceso o tratamiento no autorizado.
- Daño, alteración o modificación no autorizada.

Se aconseja revisar y conocer las "Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales" emitidas por el INAI y que se encuentran disponibles en http://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf

En estas recomendaciones se describen los procesos y controles sugeridos por el INAI para que los responsables, en este caso las OSC, respondan y mitiguen vulneraciones a la seguridad de la información personal que mantienen.

¿QUÉ ES UNA VULNERACIÓN DE BASES DE DATOS?

- **Pérdida o destrucción no autorizada de datos personales**
- **Robo, extravío o copia no autorizada**
- **Uso, acceso o tratamiento no autorizado**
- **Daño, alteración o modificación no autorizada**

En caso de que ocurra una vulneración de seguridad, se deberán consultar inmediatamente las recomendaciones del INAI antes señaladas y, en cualquier caso, seguir los siguientes pasos:

1. Detonar un proceso de revisión exhaustivo de la magnitud de la afectación, incluyendo: (i) causas, (ii) sistemas y datos afectados, (iii) tipo de vulneración, (iv) medidas de seguridad que fueron comprometidas, (v) nivel de afectación (identificar si se afectaron, o no, derechos morales o patrimoniales de los usuarios y de qué forma), (vi) actores involucrados en la vulneración determinando si éstos podrían ser parte de la organización o terceros ajenos a la misma, y (vii) otros factores.

En caso de que la vulneración ocurra en sistemas administrados por un tercero encargado, el prestador de servicios deberá estar obligado contractualmente a notificar inmediatamente a la OSC sobre cualquier

vulneración y cooperar durante todo el proceso de revisión y remediación correspondiente.

2. Evaluar si se debe notificar a los titulares sobre la vulneración. Las vulneraciones de seguridad de datos personales deben ser notificadas a los titulares cuando éstas afecten de manera significativa sus derechos patrimoniales o morales.

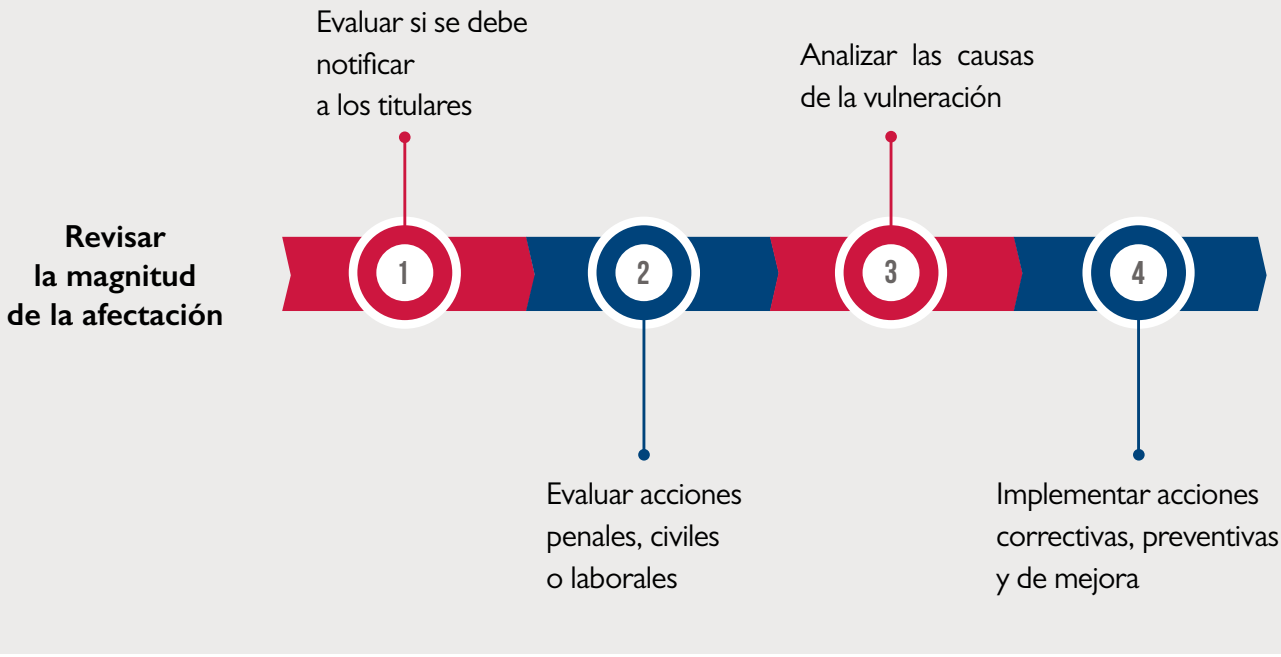
En caso de que la notificación a los titulares sea procedente, se deberá informar, por lo menos, lo siguiente:

- La naturaleza del incidente.
- Los datos personales comprometidos.
- Las recomendaciones a los usuarios acerca de las medidas que éstos pueden adoptar para proteger sus intereses.
- Las acciones correctivas realizadas de forma inmediata.
- Los medios donde pueden obtener más información.

3. Analizar las causas por las cuales se presentó la vulneración en cuestión e implementar un plan de remediación que incluya las acciones correctivas, preventivas y de mejora para actualizar las medidas de seguridad a efecto de evitar nuevas vulneraciones.

4. Evaluar potenciales acciones penales, civiles y/o laborales.

ANTE UNA VULNERACIÓN DE SEGURIDAD:



EN RESUMEN...

✓ La OSC debe guardar estricta confidencialidad respecto de los datos personales que le son proporcionados.

✓ La OSC debe implementar las medidas de seguridad siguientes:

1. Físicas.- Sirven para prevenir acceso no autorizado a equipo e información de la OSC, proteger equipo móvil, proveer mantenimiento a los equipos que contienen información y garantizar la eliminación segura de datos personales.

2. Organizacionales o administrativas.- Acciones y mecanismos para la gestión, soporte y revisión de la seguridad de la información, tales como inventarios, determinación de funciones, programas de revisiones y auditorías, análisis de riesgo periódicos, plan de trabajo, identificación de medidas de seguridad, capacitación.

3. Técnicas.- Actividades, controles y mecanismos para identificar y autorizar usuarios, así como proteger el acceso a datos o archivos. Pueden ser contraseñas para equipos y redes, protector de pantallas con clave de desbloqueo, actualizaciones de seguridad, etc.

✓ La OSC debe contar con una persona o departamento de datos personales para dar trámite a solicitudes de titulares y fomentar la protección de datos dentro de la OSC.

✓ La OSC debe revisar periódicamente los accesos y permisos de las personas que trabajen o colaboren en ella, y retirarlos en caso que la relación con éstas haya terminado o su rol haya cambiado.

✓ Pasos a seguir ante una vulneración de seguridad:

1. Detonar un proceso de revisión exhaustivo de la magnitud de la afectación.

2. Evaluar si se actualiza la obligación de notificar a los titulares (en caso que afecten derechos patrimoniales o morales).

3. Analizar las causas por las cuales se presentó la vulneración en cuestión, e implementar un plan de remediación.

4. Evaluar potenciales acciones penales y/o laborales.

7. DERECHOS DE LOS TITULARES DE DATOS PERSONALES

Todo titular de datos personales goza de ciertos derechos conocidos como "Derechos ARCO", los cuales puede ejercer ante cualquier responsable (cualquier OSC) que recabe sus datos personales. Se les llama Derechos ARCO por las iniciales de cada uno de los derechos con los que cuentan los titulares: Acceso, Rectificación, Cancelación y Oposición, y se explican a continuación. Estos derechos están reconocidos en el artículo 16 de la Constitución federal.

El procedimiento para el ejercicio de Derechos ARCO se explica más adelante y debe quedar establecido en el aviso de privacidad. Cada OSC debe tener claridad respecto a los pasos a seguir en caso de recibir una solicitud de ejercicio de derechos ARCO y quién dentro de la organización es responsable de darle trámite a la misma.

7.1 DERECHOS ARCO

1. Acceso. El titular tiene acceso a sus datos personales y a saber cuáles de ellos están siendo tratados y para qué fines.

2. Rectificación. El titular puede rectificar sus datos personales en caso de que sean incorrectos.

3. Cancelación. El titular puede cancelar el uso de sus datos en caso de que considere que no se están tratando conforme a lo que haya autorizado o a los principios o deberes que establece la LFPDPPP y su Reglamento. El fin último de la cancelación de los datos personales es que los mismos se eliminen de las bases de datos de los responsables, para lo cual primero pasan por una fase de bloqueo (que es el equivalente a un "archivo muerto" de la información personal) en donde se mantienen solamente en espera a que se agoten los plazos de prescripción legales o internos aplicables. Por ejemplo, la información de exempleados se debe conservar por el área de recursos humanos durante los plazos establecidos en la legislación fiscal, laboral[36] y de seguridad social.

4. Oposición. El titular puede oponerse al tratamiento de sus datos personales con causa justificada y legítima. Conforme a este derecho, los titulares pueden oponerse a que sus datos personales sean tratados para determinados fines. Por ejemplo, los beneficiarios de algún programa de ayuda de una OSC pueden oponerse a que sus nombres, fotografías u otra información sea utilizada en el informe de actividades de la OSC.

7.2 TRÁMITE DE SOLICITUDES DE EJERCICIO DE DERECHOS ARCO (PLAZOS, RESPUESTAS, INCONFORMIDADES)

Los titulares pueden en cualquier momento y de manera gratuita solicitar el acceso, rectificación, cancelación u oposición sobre el tratamiento de sus datos personales frente al responsable, una OSC por ejem-

[36] Los artículos 519 de la Ley Federal del Trabajo y 30 del Código Fiscal de la Federación establecen que los datos de identificación de un empleado, así como los documentos relacionados con su expediente laboral deben mantenerse durante toda la relación laboral y hasta 2 años posteriores a su terminación, sin embargo, es necesario revisar previamente con el departamento jurídico en caso de realizar el borrado de datos o depuración de documentos con información con ex empleados para corroborar que no existe alguna disposición legal o juicio en proceso, que obligue a conservarlos por un mayor tiempo.

plo, que se encuentre en posesión de los mismos.[37]

Los derechos ARCO pueden ejercerse únicamente por el titular y/o su representante legal, previa acreditación de su identidad o personalidad.[38]

La solicitud de derechos ARCO debe ser presentada a través de los medios de atención señalados previamente en el aviso de privacidad y contener, al menos, la siguiente información:

1. Nombre y domicilio del titular o cualquier otro medio para recibir la respuesta (la falta de este requisito es motivo para tener por no recibida la solicitud).

2. Los documentos que acrediten la identidad del titular o la personalidad de su representante.

3. Descripción precisa de los datos personales respecto de los cuales el titular busca ejercer alguno de los derechos.

4. De ser aplicable, otros elementos o documentos que faciliten la localización de los datos personales.

PLAZOS El responsable (la OSC) debe tramitar todas las solicitudes recibidas y para ello tiene un plazo máximo de 20 días hábiles a partir de su recepción. En caso de que la solicitud esté incompleta, el responsable puede solicitar al titular, dentro de los 5 días hábiles siguientes, que aporte información adicional para atender su petición.

En caso de que el titular no proporcione la información solicitada dentro de los 10 días hábiles siguientes a la recepción de dicho requerimiento, su solicitud de derechos ARCO se tendrá por no presentada. Si el titular atiende el requerimiento, el plazo para que el responsable dé respuesta a la solicitud empezará a correr al día siguiente de que el titular haya atendido el requerimiento.

RESPUESTA El responsable se encuentra obligado a emitir una respuesta a la solicitud del titular y referirse única y exclusivamente a los datos indicados en la misma. Para tal efecto, el responsable deberá proporcionar la misma a través de un formato de fácil acceso, legible y comprensible.

RESPUESTA FAVORABLE Si el responsable considera que la solicitud de derechos ARCO es procedente, entonces contará con 15 días hábiles posteriores a la mencionada contestación para hacer efectiva la determinación tomada.

NEGATIVA AL EJERCICIO DE LOS DERECHOS ARCO El responsable puede negar el ejercicio de los Derechos ARCO en los siguientes casos:

- Si el titular o su representante no se acreditaron debidamente.
- No se encontraron los datos personales en su base de datos.
- Se lesionan los derechos de terceros.
- Cuando la rectificación, cancelación u oposición haya sido realizada previamente.
- Exista impedimento legal o resolución de una autoridad que restrinja el ejercicio de estos derechos.

En el caso de una solicitud de cancelación (eliminación), la OSC se podría negar a llevar a cabo la misma cuando los datos personales:

- Se refieran a las partes de un contrato y sean necesarios para su desarrollo y cumplimiento. Por ejemplo, un empleado no puede solicitar que los datos

[37] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (2015). Guía Práctica para la Atención de las Solicitudes de Ejercicio de los Derechos ARCO. INAI. Disponible en: http://inicio.ifai.org.mx/Publicaciones/02GuiaAtencionSolicitudesARCO.pdf; Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios (INFOEM). ¿Qué es una solicitud de derechos ARCO? Visitado el 24 de abril de 2019, disponible en: https://infoem.org.mx/src/htm/queEsArco.html

[38] Artículo 89 de la LFPDPPP.

personales contenidos en su contrato laboral sean eliminados mientras la relación laboral esté vigente.
• Deban ser tratados por disposición legal.
• Se obstaculice una actuación judicial o administrativa vinculada a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas.
• Sean necesarios para proteger intereses jurídicamente tutelados del titular.
• Sean necesarios para realizar una acción en función del interés público.
• Sean necesarios para cumplir con una obligación legalmente adquirida por el titular.
• Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud.

Ahora bien, en términos del artículo 32 de la LFPDPPP, el responsable debe comunicar al titular la determinación adoptada en un máximo de 20 días, contados desde la fecha en que se recibió la solicitud de ejercicio de derechos ARCO, y que de ser procedente ésta se haga efectiva dentro de los 15 días siguientes a la fecha de comunicación de la respuesta. Estos plazos se pueden ampliar por un periodo igual, siempre que el caso específico lo amerite.

En caso de existir cualquier duda sobre si se actualiza alguna causal para negar el ejercicio del derecho ARCO, se debe que consultar a la persona o departamento de datos personales de la OSC, o bien, un especialista en esta materia.

INCONFORMIDAD En caso de que el titular no esté conforme con la respuesta, o bien, el responsable omita dar respuesta, el titular podrá presentar una solicitud de protección de derechos ante el INAI conforme a lo que se explica en la sección siguiente.

7.3. PROCEDIMIENTO DE PROTECCIÓN DE DERECHOS

En caso de que el responsable omita dar una respuesta a una solicitud de derechos ARCO o ésta sea en sentido negativo, el titular de los datos personales puede iniciar frente al INAI, dentro de los 15 días hábiles siguientes, un procedimiento de protección de derechos por cualquiera de las siguientes razones:

- No le entregaron los datos personales solicitados.
- El formato es incomprensible.
- El responsable se negó a corregir o cancelar la información o atender la solicitud de oposición.
- La respuesta sea incompleta o incomprensible.
- Esté inconforme con el costo o modalidad de reproducción.

Posteriormente, se notifica al responsable de los datos personales y éste cuenta con 15 días hábiles para la contestación y ofrecimiento de pruebas. Se programa audiencia en 15 días y se presentan alegatos dentro de los 5 días hábiles siguientes.

El INAI tiene un plazo máximo de 50 días hábiles para dictar una resolución, en la cual podrá: a) desechar la solicitud de protección de derechos o b) confirmar, revocar o modificar la respuesta de la organización.

En caso aplicable, el responsable debe dar cuenta por escrito del cumplimiento de lo ordenado por el INAI dentro de los siguientes 10 días hábiles.

EN RESUMEN...

✓ Los titulares pueden en cualquier momento y de manera gratuita solicitar el acceso, rectificación, cancelación u oposición (solicitud de derechos ARCO) sobre el tratamiento de sus datos personales frente a la OSC.

✓ Las OSC están obligadas a emitir una respuesta al titular que haya iniciado una solicitud de derechos ARCO, en un formato de fácil acceso, legible y comprensible.

✓ Las OSC tienen que cumplir puntualmente con los siguientes plazos:

1. 20 días hábiles para tramitar las solicitudes de derechos ARCO, a partir de su recepción.

2. 5 días hábiles, a partir de la recepción de la solicitud ARCO, para solicitar información adicional al titular.

3. 15 hábiles para cumplir con la respuesta favorable a la solicitud de derechos ARCO, posteriores a la contestación.

✓ Cualquier duda sobre alguna solicitud de derechos ARCO se debe consultar con la persona o departamento de datos personales, o bien, o un especialista en la materia.

8. PROCEDIMIENTOS DE VERIFICACIÓN

El INAI tiene la facultad de requerir a los responsables que traten datos personales, aquella documentación que se encuentre relacionada con el tratamiento que hace de los mismos, así como la realización de visitas al establecimiento en el que se encuentren las bases de datos en las que esta información se encuentra almacenada.

Este procedimiento puede iniciarse de oficio o a petición de parte; en otras palabras, el INAI puede: (i) iniciarlo cuando así lo considere conveniente y en contra de cualquier responsable, o (ii) con base en la denuncia que haya realizado cualquier persona de quien el responsable trate sus datos personales. El INAI inicia este tipo de procedimientos cuando presume de forma fundada y motivada la existencia de violaciones a la LFPDPPP.

La mejor forma de prepararse para un procedimiento de verificación es estar en cumplimiento del presente manual, y por consiguiente de la LFPDPPP. Esto es, cumplir con las obligaciones aquí descritas y tener debidamente documentado dicho cumplimiento.

Los procedimientos de verificación tienen una duración máxima de 180 días hábiles y la determinación que tome el INAI con respecto al mismo, deberá tomarse dentro de los 180 días hábiles siguientes. Al respecto, el INAI podrá ampliar este último plazo por una sola vez y por un periodo igual (i.e., 180 días hábiles).

Cuando se realiza una visita de verificación dentro de un procedimiento de verificación por parte del INAI, los servidores públicos se presentan en el domicilio del responsable con una orden por escrito en la que se precisa el lugar a visitar, el objeto y alcance de la visita y los artículos de LFPDPPP en los que se fundamenta la misma. Es importante que al momento de que se realiza una visita de verificación, los servidores públicos se identifiquen y se revise que la orden se encuentre firmada (de la cual debe exigirse una copia). La visita de verificación se realizará en presencia de dos testigos y se elaborará un acta en la que se dejará constancia de lo acontecido.

Una vez finalizado el procedimiento de verificación, el INAI dictará las medidas que deberá adoptar el responsable y, en su caso, iniciar un procedimiento de imposición de sanciones (o indicar el plazo en el que se iniciará el mismo). Las sanciones que podrían ser impuestas a los responsables se describen más adelante.

En caso de que el responsable no se encuentre de acuerdo con la determinación derivada del procedimiento de verificación, ésta se podrá impugnar a través de juicio de nulidad ante el Tribunal Federal de Justicia Administrativa.

EN RESUMEN...

✓ El INAI tiene la facultad de requerir a los responsables que traten datos personales, documentación relacionada con el tratamiento de los mismos y realizar visitas a los establecimientos en donde está almacenada la información (procedimiento de verificación).

✓ La mejor forma para prepararse ante un eventual procedimiento de verificación es:

1. Cumplir con las obligaciones sobre el aviso de privacidad, incluyendo documentar el consentimiento de los titulares.

2. Implementar medidas de seguridad físicas, organizacionales y técnicas para proteger los datos personales.

3. Nombrar la persona o al departamento de datos personales de la OSC.

4. Capacitar al personal y colaboradores de la OSC sobre las obligaciones de protección de datos personales.

5. Verificar que las actividades relacionadas con datos personales cumplen con la LFPDPPP y sus principios.

9. SANCIONES

La LFPDPPP contempla conductas que ameritan infracciones y que son delitos en materia de datos personales,[39] las cuales deben ser conocidas para prevenirlas oportunamente.

9.1. INFRACCIONES

El INAI podrá sancionar a cualquier responsable en caso de que éste realice cualquiera de las siguientes conductas:

1. No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada, en los términos previstos en la LFPDPPP.

2. Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales.

3. Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable.

4. Dar tratamiento a los datos personales en contravención a los principios establecidos en la LFPDPPP.

5. Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16 de la LFPDPPP.

6. Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares.

7. No cumplir con el apercibimiento que se le haga por parte del INAI.

8. Incumplir el deber de confidencialidad.

9. Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin observar lo dispuesto por la LFPDPPP.

10. Transferir datos a terceros sin comunicar a éstos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos.

11. Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable.

12. Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la LFPDPPP.

13. Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible.

14. Obstruir los actos de verificación del INAI.

15. Recabar datos en forma engañosa y fraudulenta.

16. Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el Instituto o los titulares.

17. Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos de acceso, rectificación, cancelación y oposición establecidos en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.

18. Crear bases de datos en contravención a lo dispuesto la LFPDPPP.

19. Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en la LFPDPPP.

[39] Artículos 63 a 69 LFPDPPP.

SUPUESTO	SANCIÓN	EQUIVALENCIA A PESOS MEXICANOS (PARA 2019)
Conducta 1	Apercibimiento	No Aplica
Conductas 2 a 7	Multa de 100 a 160,000 Unidades de Medidas y Actualización (UMA)[40]	$8,449 a $13'518,400
Conductas 8 a 18	Multa de 200 a 320,000 UMA	$16,898 a $27'036,800

En caso de reincidencia, el INAI podrá imponer una multa adicional que irá de 100 a 320,000 UMA y tratándose de infracciones cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse al doble.

9.2. DELITOS

La LFPDPPP también contempla delitos cuando existe un tratamiento indebido de datos personales, mientras el fin sea con ánimo de lucro o lucro indebido. Al respecto, se establecen las siguientes penas:

DELITO	PENA
Al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.	3 meses a tres años de prisión
Al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.	6 meses a 5 años de prisión

De igual forma, en caso de que se afecten datos personales sensibles, la pena correspondiente se duplicará.

[40] 1 UMA = $84.49. Fuente: Instituto Nacional de Estadística y Geografía (INEGI). Unidad de Medida y Actualización (UMA). Visitado el 24 de abril de 2019, disponible en: https://www.inegi.org.mx/temas/uma/

EN RESUMEN...

✓ La LFPDPPP contempla sanciones administrativas (multa y apercibimiento) por incumplir con la ley, así como pena de prisión por tratamiento indebido de datos personales.

10. MEJORES PRÁCTICAS

Existen diferentes formas en que un responsable del tratamiento pueda llegar a encontrarse en una situación de incumplimiento respecto de los datos personales que trata. Teniendo esto en cuenta, es importante que los miembros de la OSC proactivamente busquen y desarrollen mejores prácticas relacionadas con el tratamiento de datos personales y su seguridad para proteger los derechos de sus titulares. Algunos consejos o mejores prácticas se detallan a continuación.

10.1 SOBRE LOS DATOS PERSONALES

1.Tratar únicamente los datos que la OSC estrictamente requiere.

2. Procurar utilizar datos que sean de naturaleza pública o que hayan pasado un proceso estricto de disociación.

3. Evitar tratar datos personales sensibles por equivocación. Existe la posibilidad de recaudar datos por error del titular o del responsable del tratamiento. Por ende, es importante que los procedimientos de recolección de datos estén diseñados para evitar la recolección de datos de naturaleza sensible.

10.2 SOBRE LA ORGANIZACIÓN DE LOS DATOS PERSONALES

1. En cada base de datos, mantener un campo en el que se indique la modalidad de la recolección y el lugar donde se encuentra la prueba del consentimiento del titular.

2. Tener un inventario detallado y permanentemente actualizado de las bases de datos que contengan datos personales con al menos la siguiente información:

(i) fecha de creación de la base,

(ii) el estado, tipo y lugar de almacenamiento de las autorizaciones del tratamiento,

(iii) la forma de recolección de los datos,

(iv) la cantidad de entradas en la base,

(v) los tipos de datos tratados (si son públicos, privados, etc),

(vi) la localización física o lógica de la base,

(vii) las medidas de seguridad que la protegen,

(viii) el fin del tratamiento de la base de datos,

(ix) los encargados del tratamiento (si aplica) y el estado de los convenios vigentes sobre tratamiento de datos con dichos encargados,

(xi) los proveedores de los datos (si aplica),

(xii) nivel de seguridad y

(xiii) si la base de datos ha sido objeto de un proceso de disociación. Esto permite una visión de alto nivel del estado de protección de cada una de las bases y de sus contenidos así como del estado del cumplimiento.

3.Asegurarse de que los sistemas y procedimientos que implementará estén de acuerdo con su política de tratamiento de datos y su aviso de privacidad.

4. Cuando se procure una base de datos de un tercero, asegurarse de firmar un acuerdo en el que el responsable que transferirá los datos cumpla con todos los requisitos de ley para la transferencia y se haga responsable por cualquier reclamación o sanción administrativa que ocurra por su incumplimiento de la normativa o del acuerdo que firmó en relación con los datos transferidos.

10.3 PRECISIONES FINALES

1. Es sumamente importante mantener vigilancia constante y un gran nivel de diligencia respecto del tratamiento de datos personales. Los avisos de privacidad, las bases de datos personales y las políticas organizacionales se deben revisar recurrentemente.

2. La protección de los datos personales es un esfuerzo colectivo dentro de las organizaciones. Todos los miembros de la organización deben entender los procedimientos y políticas de la organización, así como poder identificar cuando un dato personal está siendo tratado de manera irregular o ilegal.

ANEXO - FORMATO DE AVISO DE PRIVACIDAD

El siguiente formato se ofrece como ejemplo para orientar a las OSC sobre la manera en que puede redactarse el aviso de privacidad.

HERRAMIENTAS ADICIONALES:	
• **Generador de avisos de privacidad del INAI.- Esta herramienta permite crear avisos de privacidad de manera rápida, sencilla y gratuita: https://generador-avisos-privacidad.inai.org.mx/**	• **El ABC del Aviso de Privacidad.- El INAI cuenta con una guía para redactar el aviso de privacidad, así como ejemplos y modelos, que pueden ser de utilidad para las OSC: http://abcavisosprivacidad.ifai.org.mx/#seccion5**

AVISO DE PRIVACIDAD DE [INSERTAR NOMBRE COMPLETO DE LA OSC]

A través del presente Aviso de Privacidad ("Aviso de Privacidad"), le comunicamos las condiciones y garantías a través de las cuales ***[INSERTAR NOMBRE COMPLETO DE LA OSC]*** domiciliada en ***[INSERTAR DOMICILIO, CÓDIGO POSTAL],*** en su calidad de Responsable del Tratamiento, tratará sus Datos Personales.

¿Qué tipo de datos personales recolectamos?
[INSERTAR TIPO DE DATOS PERSONALES QUE SE RECOLECTAN Y EL MODO COMO SE RECOLECTA **TENER EN CUENTA QUE SE DEBE SIEMPRE O PEDIR AUTORIZACIÓN O COMPARTIR EL AVISO DE PRIVACIDAD PREVIO A LA RECOLECCIÓN**] (los "Datos Personales").

¿Con qué objetivo trataremos sus Datos Personales?
Las finalidades para las cuales trataremos sus Datos Personales son las siguientes:
• ***[INCLUIR UNA DESCRIPCIÓN DE LAS FINALIDADES DEL TRATAMIENTO DE LOS DATOS, TALES COMO COMUNICAR INFORMACIÓN COMERCIAL QUE PUEDA SER DE SU INTERÉS, CUMPLIMIENTO DE NUESTRAS OBLIGACIONES FISCALES, ETC.]***

¿A través de qué canales puede ejercer sus derechos en relación con los Datos Personales?
Usted podrá ejercer sus derechos de acceso, rectificación, cancelación y oposición de conformidad con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) a través de los siguientes canales:

• ***[INCLUIR EL MEDIO A TRAVÉS SE PUEDE EJERCER LOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN U OPOSICIÓN], [INCLUIR SITIO WEB, CORREO ELECTRÓNICO A TRAVÉS DEL CUAL SE PUEDE CONSULTAR EL AVISO Y LA POLÍTICA, SOLICITAR INFORMACIÓN O EJERCER LOS DERECHOS DEL TITULAR].***

• ***[OPCIONAL: INCLUIR UN PROCEDIMIENTO PARA LA REALIZACIÓN DE LAS CONSULTAS, UN MÍNIMO DE INFORMACIÓN QUE SE DEBE COMPARTIR PARA ASEGURARSE QUE LA PERSONA ES QUIEN DICE SER, ETC].***

Asimismo, podrá limitar el uso o divulgación de sus datos de la siguiente forma:

- ***[INCLUIR LOS MEDIOS Y OPCIONES PARA LA LIMITACIÓN DEL USO O DIVULGACIÓN DE LOS DATOS].***

Con su confirmación expresa o tácita, usted está dando su aprobación para que el Encargado del Tratamiento realice las siguientes operaciones con sus datos:

Tipo de Operación	Destinatario de los Datos	Finalidad de la Operación

Tenga en cuenta que con su aceptación de la Política de Privacidad o su ausencia de oposición expresa al Aviso de Privacidad, se entenderá que ha otorgado su consentimiento para las operaciones antes descritas. ***[**SÓLO EN CASO DE QUE SE REALICE TRANSFERENCIA DE DATOS PERSONALES**]***

Los cambios que ocurran en nuestra Política de Privacidad o en el Aviso de Tratamiento podrán ser consultados a través del siguiente enlace: ***[INCLUIR ENLACE].*** También serán comunicadas a través de correo electrónico en caso de que usted haya compartido su correo electrónico con nosotros y no nos haya solicitado su eliminación o nos haya revocado la autorización para el tratamiento de estos.

“Manual de Protección de Datos personales para Organizaciones de la Sociedad Civil”
se editó en la Ciudad de México en agosto de 2019.