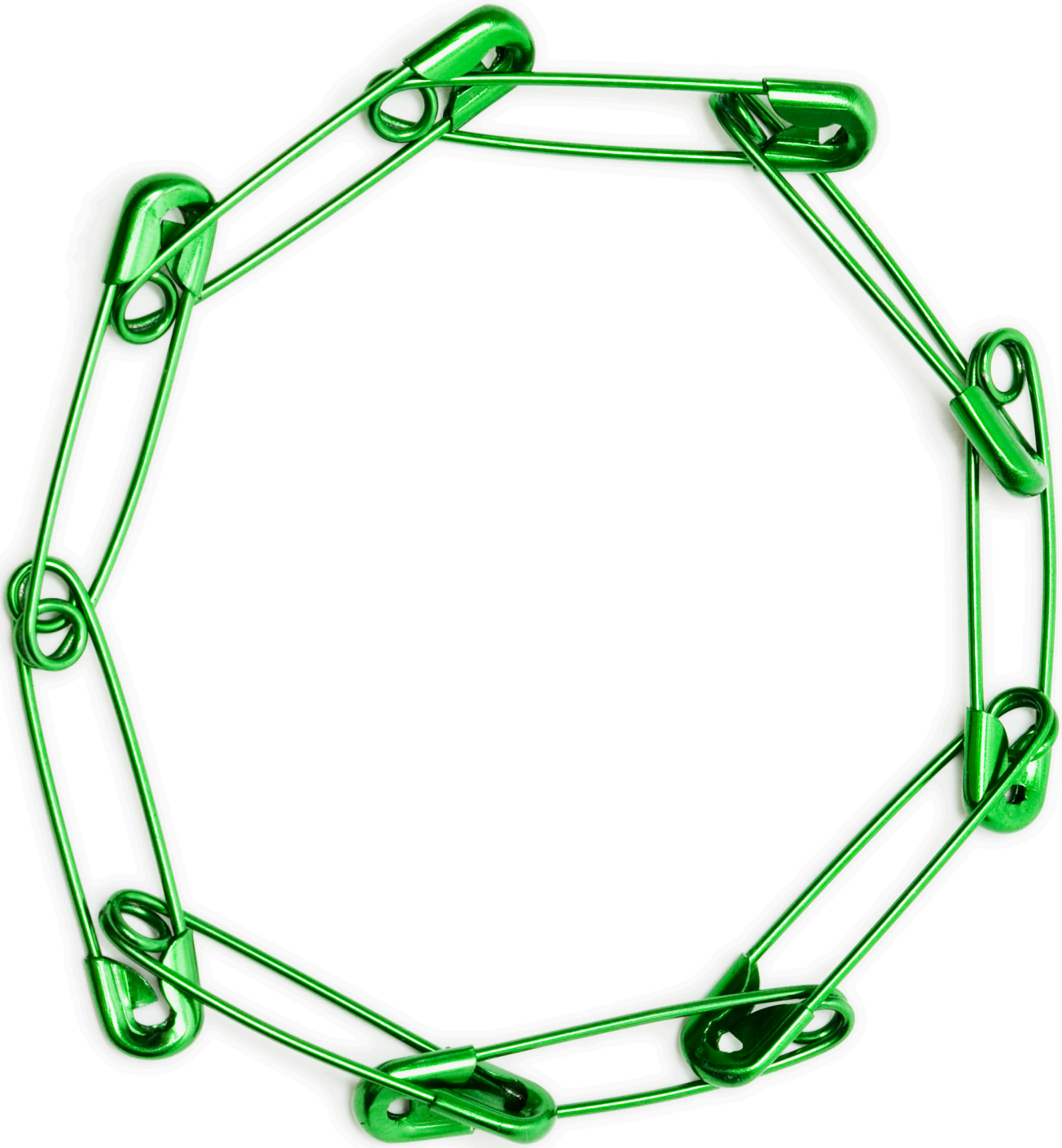
Deloitte.

Ley Federal de Protección de Datos Personales en Posesión de Particulares



Ley Federal de Protección de Datos Personales en Posesión de Particulares

Antecedentes

En un mundo con gran despliegue tecnológico y donde la economía gira en torno a la información, es de extrema importancia contar con una legislación que proteja los datos personales. En México es una necesidad clara y como prueba, desde 2001 se han presentado siete iniciativas que van desde las muy conservadoras hasta las muy liberales.

Las noticias recientes han presentado incidentes sobre el robo y tráfico de datos en México que nos ponen a pensar en la vulnerabilidad de los sistemas y el riesgo que representan para cualquier individuo u organización.

Los riesgos tecnológicos son un asunto de todos los días para los ejecutivos de las organizaciones. No es exagerado decir que las amenazas a la confidencialidad son un tema que cada día preocupa más, pues los riesgos se multiplican conforme avanza la tecnología.

Por esta razón, el 5 de julio de 2010 se publicó en el Diario Oficial de la Federación (DOF) la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDP), la cual tiene como objetivo proteger los datos personales en posesión de los particulares y regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de los individuos.

Bajo este contexto, la Ley mencionada anteriormente entró en vigor al día siguiente de su publicación en el DOF y las empresas contarán con un plazo de 18 meses para implementar políticas y procedimientos, así como los mecanismos necesarios en recursos humanos, legal, tecnología, procesos e infraestructura para cumplir con dicha Ley. El Ejecutivo Federal expedirá el reglamento respectivo en el año siguiente a su entrada en vigor. En ese mismo periodo los responsables designarán a la persona o el departamento de datos personales a que se refiere el Artículo 30 de la Ley y expedirán sus avisos de privacidad a los titulares de esa información.

Las sanciones por faltas a la LFPDP van desde sanciones económicas (altas) hasta la privación de la libertad.

El Instituto Federal de Acceso a la Información y Protección de Datos Personales (IFAI PDP) es el encargado de promover y difundir el ejercicio del derecho a la información, resolver sobre la negativa a las solicitudes de acceso a la información y proteger los datos personales en poder de dependencias y entidades.

Lo anterior nos lleva a cuestionarnos: ¿qué tanta capacidad tienen las compañías para hacerle frente a estos riesgos?, ¿existen controles robustos dentro de estas instituciones para la protección de datos en su confidencialidad, integridad y disponibilidad? Actualmente, ¿los procesos para el tratamiento de los datos de las empresas mexicanas cumplen con la LFPDP?

¿Qué es la LFPDP?

La Ley cuenta con 69 artículos agrupados en once capítulos y transitorios.

I. Disposiciones Generales	II. Los Principios de Protección de Datos Personales
III. Los Derechos de los Titulares de Datos Personales	IV. Ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición - ARCO
V. De la Transferencia de Datos	VI. Las Autoridades Sección I. Del Instituto Sección II. De las Autoridades Reguladoras
VII. Del Procedimiento de Protección de Derechos	VIII. Del Procedimiento de Verificación
IX. Del Procedimiento de Imposición de Sanciones	X. De las Infracciones y Sanciones
XI. De los Delitos en Materia del Tratamiento Indebido de Datos Personales	
Transitorios	

Ahora bien, es necesario partir en términos del artículo 1 de la LFPDP, donde se explica que el objeto de esta Ley es: "la protección de los datos personales en posesión de los particulares", a excepción de lo descrito en el artículo 2 (sociedades de información crediticia cuando se esté en los supuestos de la Ley de la materia y personas que recolectan y almacenan datos, siempre y cuando no sea con fines de divulgación ni de utilización comercial), siendo los sujetos de la Ley los particulares (personas físicas o morales de carácter privado). Por lo anterior, todos aquellos que no estén en los supuestos de excepción que tengan en posesión datos personales de particulares, serán los sujetos a cumplir con esta Ley.

Dato Personal	Cualquier información concerniente a una persona física identificada o identificable. Consentimiento: expreso verbalmente, escrito, medio electrónico, óptico u otra tecnología. Consentimiento tácito si el Titular no manifiesta oposición.
Dato Personal Sensible	Datos personales que afectan la esfera más íntima de su Titular o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave (por ejemplo: origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual). Consentimiento: expreso y por escrito, firma autógrafa, electrónica o cualquier mecanismo de autenticación.

La Ley prevé sanciones que van desde el apercibimiento (equivalente a una llamada de atención), hasta la imposición de multas desde 100 hasta 320 mil días de Salario Mínimo General Vigente, lo cual equivale a cerca de 18 millones de pesos. Además, en función de la gravedad del delito, podrían existir responsabilidades civiles y penales.

Los delitos en materia del tratamiento indebido están descritos en los siguientes artículos:

Artículo 67.- Se impondrán de tres meses a tres años de prisión 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.

Artículo 68.- Se sancionará con prisión de seis meses a cinco años 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.

Artículo 69.- Tratándose de datos personales sensibles, las penas a que se refiere este Capítulo se duplicarán.

Finalmente, la Ley destaca algunas fechas importantes que deberán tener presentes cada una de las compañías para su cumplimiento en los tiempos determinados y evitar sanciones. Partiendo de la fecha de la publicación de la Ley en el DOF y su entrada en vigor (5 de julio de 2010), las compañías cuentan con un periodo de gracia para su preparación.

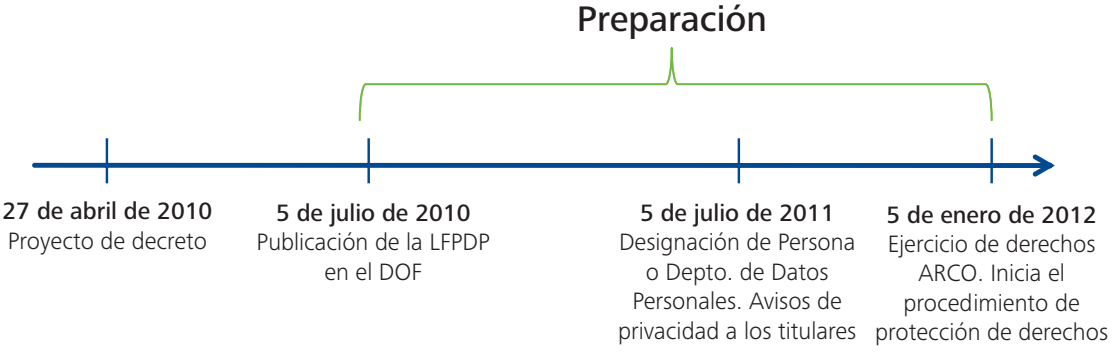
Nuestra visión de la LFPDP

La entrada en vigor de la Ley supone para las compañías la imposición de nuevas obligaciones tanto jurídicas como técnicas, físicas y organizacionales en materia de protección de datos personales.

Si bien hasta ahora se tenía una idea clara de lo que era necesario proteger desde el punto de vista técnico, los sistemas de información y la custodia de los datos en cualquiera de sus formatos implican la necesidad de analizar a profundidad el "ciclo de vida del dato", es decir, resulta primordial controlar cómo viaja la información entre los distintos departamentos de la organización, dónde y cuándo se duplica, dónde y cómo se almacena, a quién y cómo se envía, cuándo y cómo se destruye, etc.

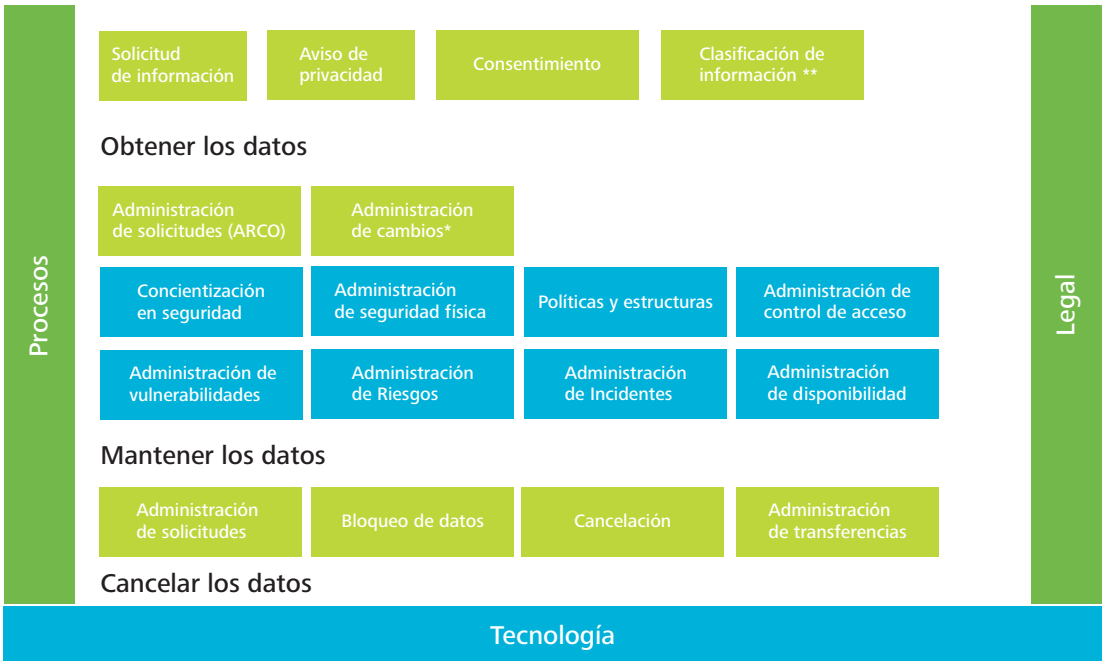
Esto implica la necesidad de llevar a cabo una revisión completa del tratamiento que se realiza de los datos personales en la organización prestando especial interés a temas tradicionalmente no tan trabajados como: la seguridad en el puesto de trabajo, la tipología y seguridad en archivos físicos, la utilización de fax, el escáner, las fotocopiadoras, las memorias USB, entre otros.

Por todo esto, consideramos que los factores claves de éxito para la adecuada implantación y gestión de las medidas jurídicas, técnicas, físicas y organizacionales exigidas por la Ley serían:



- **Respaldo y participación de la Dirección.**
  El proyecto debe ser de ámbito global y abarcar a toda la organización, lo que sólo puede lograrse con un fuerte respaldo de la Dirección.
- **Coordinación global.**
  Si bien en los planes de acción aparecerán medidas de índole jurídica, técnica, física y organizacional, son necesarias una coordinación y una visión únicas y globales que garanticen la adecuada complementariedad de las mismas.
- **"No empezar la casa por el tejado".**
  Es necesario analizar el flujo de la información dentro de la organización para poder identificar los distintos tratamientos que se hacen de los mismos, y los posibles puntos de archivo, duplicado, envío, recepción y destrucción de la información con el fin de poder adoptar las medidas jurídicas, técnicas, físicas y organizativas exigidas por la normativa vigente en materia de protección de datos.
- **Concientización del personal.**
  El cumplimiento de gran parte de los nuevos procedimientos estará basado fundamentalmente en la concientización y la participación de los empleados.

Basados en los principios que la LFPDP indica y partiendo del análisis de la presente Ley, podemos observar que existen tres macroprocesos inmersos para que una compañía pueda alinearse a dicha Ley, así como los actores principales para su implementación.



** La clasificación de la información se refiere a identificar datos sensibles según la Ley.

* Administración de cambios se refiere a transferencia y cambios en finalidad.

Procesos que se podrían basar en estándares como ISO27001, ISO20000, DRP (BS25999), COBIT.

Cada uno de los macroprocesos (obtener los datos, mantener los datos y cancelar los datos) cuenta con varios procesos para la gestión y tratamiento de los datos, los cuales están interrelacionados unos con otros en función de las necesidades de los Titulares, así como los requerimientos determinados por el IFAI PDP y la Secretaría de Economía mencionadas en la presente Ley.

Nuestra visión final para evaluar el cumplimiento de la LFPDP consiste en realizar un análisis de brechas de cada uno de los procesos involucrados de la compañía contra la Ley, apoyados en la aplicación de mejores prácticas y marcos de referencia reconocidos internacionalmente, tales como ISO27001, ISO20000, BS25999, COBIT, COSO, etc., y definir los procesos legales requeridos para su cumplimiento integral.

Como se mencionó anteriormente, esto no puede llevarse a cabo sin el compromiso y participación del recurso humano de la compañía, es decir, los diferentes actores involucrados para su implementación y gestión. El rol de cada uno de los actores es el siguiente:

Legal.- Es el punto de contacto con las autoridades y las áreas internas. Es importante su participación en el diseño, implementación y gestión de las actividades para el cumplimiento de los requerimientos.

Procesos de negocio.- Punto de contacto de los titulares para dar respuesta, entre otras, a las solicitudes ARCO (acceso, rectificación, cancelación y oposición). Participan en la obtención de la información (aviso de privacidad, consentimiento).

Tecnología.- Es necesaria para la implementación de medidas administrativas, técnicas y físicas para proteger la seguridad de los datos, basadas en un análisis de riesgos. Es relevante para la administración de disponibilidad, vulnerabilidades e incidentes.

Servicios para la alineación con la LFPDP

Deloitte en materia de protección de datos para el cumplimiento con la LFPDP ofrece una gran variedad de servicios profesionales adaptados a las necesidades del cliente, entre los que se encuentran:

Revisión o diagnósticos

- Revisión del grado de cumplimiento de los procesos de la compañía hacia la LFPDP, en el cual se realiza un diagnóstico de los procesos actuales de la compañía respecto a su alineación con la LFPDP (previo a su implementación). Con esto ayudamos a las empresas a identificar la brecha para la elaboración del plan de acción correspondiente para su implementación.
- Evaluación de los procesos implementados (post-implementación) por la compañía para determinar el grado de cumplimiento de la LFPDP.
- Revisiones periódicas para evaluar los procesos para el cumplimiento con la LFPDP.

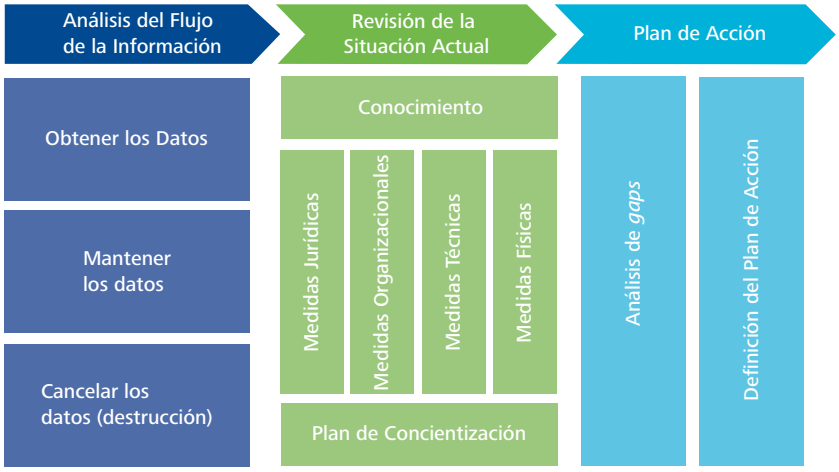
Asesoramiento

- Implementación de los planes para la adaptación a la LFPDP vigente.
- Concientización del personal respecto a la LFPDP.

Evaluación a terceros

- Diagnóstico del grado de cumplimiento de los procesos del tercero hacia la LFPDP, en caso de que el cliente requiera transferir algún proceso para el tratamiento de los datos.

El enfoque de solución que proponemos para asesorar a las compañías a su alineación con la LFPDP es el siguiente:



Contactos:

Región Centro
José González Saravia
Socio
Tel. +52 (55) 5080 6722
jgonzalezsaravia@deloittemx.com

Eduardo Cocina
Socio
Tel. +52 (55) 5080 6936
ecocina@deloittemx.com

Rocío Gutiérrez
Gerente
Tel. +52 (55) 5080 6686
rocgutierrez@deloittemx.com

Oscar Moreno
Gerente
Tel. +52 (55) 5080 6569
osmoreno@deloittemx.com

Región Norte
Salomón Rico
Socio
Tel. +52 (81) 8133 7351
srico@deloittemx.com

Región Bajío
Victor Salcedo
Socio
Tel. +52 (33) 3819 0555
vsalcedo@deloittemx.com

Región Frontera
Mario García
Socio
Tel. +52 (664) 622 7810
magarcia@deloittemx.com

www.deloitte.com/mx