FONDO DE INFORMACIÓN Y DOCUMENTACIÓN PARA LA INDUSTRIA INFOTEC

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO

METODOLOGÍA DE MEJORES PRÁCTICAS

(IMPLEMENTACIÓN DE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES EN MÉXICO)

PROYECTO INTEGRADOR

QUE PARA OBTENER EL GRADO DE:

MAESTRO EN DIRECCIÓN ESTRATÉGICA DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

PRESENTA:

JESÚS ERNESTO BRISEÑO MONTIEL

ASESORA:

DRA. WILMA ARELLANO TOLEDO

MÉXICO DF **2013**

Unidad de Posgrados INFOTEC

UT D SCHOOL OF MANAGEMENT
THE UNIVERSITY OF TEXAS AT DALLAS

DEDICATORIA

Los grandes momentos, los grandes triunfos y las grandes metas, invariablemente se forman de la continuidad de pequeños pasos.

Jesús Ernesto Briseño Montiel.

A mi amado hijo Jesús Ernesto

A Lupita y Jesús Ernesto, mis padres

AGRADECIMIENTOS

Estudiar una maestría es un gran reto que implica compromiso, dedicación y tiempo.

En este camino que emprendí tuve la fortuna de contar con muchas personas que de una u otra forma siempre me acompañaron y alentaron.

A mi hijo Jesús Ernesto, por creer en mi.

A Gemalis y Perla, por el apoyo y paciencia que siempre me brindaron.

A la Dra. Wilma Arellano Toledo por su dirección, entusiasmo y apoyo que hicieron posible este proyecto.

A todos mis maestros que influyeron con sus lecciones y experiencias en cambios positivos para mi vida personal y profesional.

A todos aquellos que en algún momento me animaron a seguir adelante.

ÍNDICE

INTRODUCCIÓN.

Hoy día, hablar de *datos personales* ya no es un concepto novedoso; el derecho a la protección de éstos es fundamental en muchos países desde hace tiempo, inclusive el Consejo de Europa promovió que cada 28 de enero se conmemore la firma del Convenio 108[1] para la protección de personas con respecto al tratamiento automatizado de datos de carácter personal. En México, la importancia se entiende al haber sido incorporado este derecho fundamental en nuestra Carta Magna en los Artículos 6 y 16.

La cotidiana familiaridad para la utilización de datos personales, también facilita riesgos para su uso sin consentimiento previo con fines desconocidos, es por eso que la protección de datos personales, es indispensable, para asegurar el control sobre la información e identidad personal.

Valorando lo anterior y después de la revisión de la situación actual en México de la aplicación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), su Reglamento (RLFPDPPP), el análisis de diferentes documentos y experiencias relacionadas con las prácticas efectivas, considero necesario desarrollar un proyecto de solución estratégica que comprende la metodología de mejores prácticas, que de manera ordenada y eficiente, facilite el apropiamiento y cumplimiento de la LFPDPPP con su Reglamento, considerando los aspectos jurídicos, tecnológicos, económicos y sociales en beneficio de las personas o clientes y las organizaciones.

La metodología utilizada para la elaboración del presente trabajo consistió en definir un marco teórico que sirviera de plataforma para el desarrollo de la metodología de mejores prácticas de implantación de la Ley, a través de estudiar lo que las empresas que ya cumplen con ella hicieron.

El esquema metodológico fundamental fue:

[1] García, P. (2013). *La importancia de la protección de datos personales.* Educa Transparencia. Santiago, Chile.

- Analizar y seleccionar los tópicos y elementos, críticos e indispensables, de los modelos de gestión.
- Analizar y seleccionar los tópicos y elementos, críticos e indispensables, para el cumplimiento de la LFPDPPP.
- Estructurar la metodología de mejores prácticas en 7 grandes estrategias de implantación.

El primer Capítulo se enfoca en el marco teórico conceptual del Derecho a la Protección de Datos Personales en Posesión de los Particulares entendiendo como surge, su sustento constitucional, las diferentes figuras jurídicas y sus principios, determinando lo que se entiende por cada uno de los conceptos utilizados a lo largo del presente documento, ya que sin ellos, sería difícil entender el contexto del punto de partida.

Así, el segundo Capítulo, profundiza y determina la situación actual de las empresas y los particulares en México en cuanto al apropiamiento, implementación y cumplimiento de la Ley y su Reglamento, además de la cronología de cumplimiento.

La determinación de las principales obligaciones a cumplir por los particulares (personas y empresas) con respecto de los datos personales y las sanciones en caso de incumplimiento, son los temas analizados en el tercer Capítulo.

El cuarto y último Capítulo, establece la propuesta de metodología, que surge como resultado de revisar diferentes esquemas de mejores prácticas usados por las empresas en México para cumplir con la Protección de Datos Personales en Posesión de los Particulares, privilegiando los derechos y seguridad de los usuarios, proporcionando una herramienta al sector privado de México, para la apropiación de dicha protección alineando principalmente las perspectivas jurídica y tecnológica, sin dejar de lado las económicas y sociales.

Finalmente, las conclusiones que pretenden servir de base a nuevas propuestas para realizar las acciones necesarias a través del uso de metodologías de mejores prácticas que permitan el cumplimiento ordenado y eficaz en materia de la LFPDPPP y su Reglamento.

CAPÍTULO I: MARCO TEÓRICO CONCEPTUAL.

El creciente uso y adopción de las tecnologías de la información y la comunicación (TIC) por las personas y por las instituciones ha generado una nueva forma de interactuar, intercambiar y gestionar la información, especialmente los datos personales.

En un mundo globalizado como el de hoy, las sociedades transitan cada vez más hacia una Sociedad de la Información y el Conocimiento (SIC) con las complejidades tecnológicas y jurídicas que esto conlleva, por lo que es vital, que se cuente con la protección de datos personales en ámbitos públicos y privados.

Los grandes avances y el incremento exponencial de las tecnologías de la información y comunicaciones han permitido que en muchas ocasiones, los datos personales no sean tratados para los fines que originalmente fueron recabados o que sean transmitidos sin la autorización del titular, violentando la privacidad y derechos.

Para entender la importancia del por qué ahora más que nunca, los datos personales deben estar protegidos en cualquier ámbito, se debe empezar por entender el concepto de derecho a la protección de datos personales; para ello a continuación, distinguiremos brevemente derecho a la intimidad, derecho a la privacidad y derecho a la protección de los datos personales.

Según la doctrina, cuando se habla de derecho a la intimidad, debemos pensar en [2]aquello que se considera más propio y oculto del ser humano, entendiéndose por propio y oculto la información que se mantiene para sí mismo. Este derecho, a consecuencia del desarrollo tecnológico y el creciente almacenamiento de información relativa a la persona, así como la inmersión cada vez mayor de la misma y de la propia sociedad, ha tenido que ir ampliando sus directrices, ya no sólo dentro de su contexto de los sentimientos, emociones, del hogar, de los papeles, la correspondencia, las

[2]García González Aristeo, (2011). *La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado,* Boletín Mexicano de Derecho Comparado, UNAM. México.

comunicaciones telefónicas, video vigilancia, etcétera, sino además, hoy es necesario su reconocimiento y más aún, el establecimiento de mecanismos de protección que puedan hacer frente a su uso y manejo.

El derecho a la intimidad es el derecho humano por el cual una persona tiene el poder de excluir a otras del conocimiento de su vida personal (los sentimientos, emociones, datos biográficos, personales e imagen), en ese sentido, el derecho a la privacidad, se refiere adicionalmente al derecho de determinar la cantidad y qué información de su vida personal puede ser legítimamente comunicada a otros (el derecho a controlar la información[3]).

El derecho a la privacidad está íntimamente relacionado con el principio de autodeterminación informativa que es un principio regulador en materia de la tutela de los datos personales y que a su vez, se encuentra dentro de los principios de libertad de la voluntad, lo que se traduce en la autonomía del consentimiento, es decir, la posibilidad de autorizar, bloquear, oponerse y ratificar los datos personales.

En México, se conocen como derechos ARCO y están consignados en la Constitución Política de los Estados Unidos Mexicanos (CPEUM), en el segundo párrafo del Artículo 16, así como en la LFPDPPP, Capítulo IV "Del ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición".

Por su importancia, a continuación se expone una breve explicación de cada uno de los derechos ARCO.

Acceso: se refiere a que el titular tiene derecho a obtener del responsable sus datos personales y ser informado de las condiciones y generalidades del tratamiento de los mismos.

[3]Piñar Mañas José Luis. (2008). *¿Existe la privacidad?*, Universidad San Pablo-CEU de Madrid. Madrid, España. P.8

Rectificación: el titular tiene derecho a solicitar al responsable que rectifique los datos personales que estén incompletos o inexactos.

Cancelación: Se refiere al cese en el tratamiento por parte del responsable a partir de un bloqueo de los mismos y su posterior supresión.

Oposición: El titular podrá oponerse al tratamiento de sus datos personales.

El derecho de protección de datos personales[4], implica el poder de disposición y control que faculta a su titular a decidir cuáles de sus datos proporciona a un tercero, así como el saber quién posee esos datos y para qué, pudiendo oponerse a esa posesión o uso.

Debemos entender que un dato personal es "cualquier información concerniente a una persona física identificada o identificable"[5].

Por ello los datos personales se encuentran tutelados como parte del derecho a la intimidad, que es un derecho conceptualmente más restrictivo que el derecho a la privacidad, el cual también se relaciona con los datos personales. Entendiendo estos derechos como esferas, la más íntima sería el derecho a la intimidad, le seguiría el derecho a la privacidad, luego tendríamos los datos personales públicos y finalmente todos estos estarían dentro del derecho a la protección de datos personales.

Con el propósito de clarificar estos conceptos, a continuación se presenta una gráfica utilizada por Jacqueline Peschard Mariscal, del Instituto de Acceso a la Información Pública (IFAI) en 2008.

[4]Peschard Mariscal Jacqueline. (2008). *El derecho a la protección de datos personales*, IFAI. México.
[5]Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Artículo 3, fracción V. Publicada el 5 de julio de 2010 en el *Diario Oficial de la Federación* y entró en vigor el 6 de julio de 2010.

Diferencia entre el derecho a la intimidad, derecho a la privacidad y derecho de protección de datos personales

Gráfica 1. Fuente: El derecho a la protección de datos personales, Jacqueline Peschard Mariscal, IFAI, 11 de noviembre de 2008.

Como anteriormente se cita, es indudable que en la actualidad, hablar de datos personales ya no es un concepto "nuevo" puesto que el derecho a la protección de éstos se considera como un derecho fundamental en muchos países desde hace mucho tiempo.

En Europa, en 1973 nace la "Datalag o Ley de Datos", en el 2000 surge el concepto de protección de datos personales y en el caso de Estados Unidos de América, aparece aunque con alcances distintos, como concepto de privacidad en 1974.

Asimismo, se encuentra en diversos instrumentos internacionales como la Directiva 95/46/CE sobre protección de personas físicas en lo que respecta al tratamiento de

datos personales y a la libre circulación de esos datos[6], el Convenio 108[7] del Consejo de Europa y otros a los que México está adherido, como en el caso de la Declaración Universal de los Derechos Humanos Artículo 12[8], el Convenio para la Protección de los Derechos y las Libertades Fundamentales en el Artículo 8[9], El Pacto Internacional de Derechos Civiles y Políticos en el Artículo 17[10], la Convención Americana sobre Derechos Humanos en el Artículo 11, apartado 2[11], entre otros.

Por considerar que contienen los elementos más importantes de los citados instrumentos legales, a continuación se transcriben algunas definiciones de los mismos.

Declaración Universal de los Derechos Humanos, Artículo 12:
"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Es importante comentar que antes de que se incorporara el derecho a la vida privada en la Declaración Universal de los Derechos Humanos, los tribunales americanos habían comenzado a reconocer el nuevo derecho a la privacidad y en Europa reconocían el derecho a la intimidad, a la privacidad y a partir del siglo pasado, derecho a la protección de datos personales, sin embargo desde un personal punto de vista, a partir de que se incorpora a la Declaración Universal de los Derechos Humanos, es cuando se propicia con mayor celeridad su incorporación en otros instrumentos internacionales.

[6]Parlamento Europeo y del Consejo. (1995). Directiva 95/46/CE, *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*. Luxemburgo.
[7]Consejo de Europa. (1981), *Convenio 108*, *para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*. Estrasburgo.
[8]"Organización de Naciones Unidas (ONU). (1948). *Declaración Universal de Derechos Humanos*". Artículo 12.París. http://www.un.org/spanish/aboutun/hrights.htm
[9]Unión Europea (1950).*Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales*. Artículo 8. Roma.
[10]Organización de Naciones Unidas (ONU). (1966). *Pacto Internacional de Derechos Civiles y Políticos. Resolución 2200 A (XXI)* de la Asamblea General.
[11]Convención Americana sobre Derechos Humanos (Pacto de San José). (1969).*suscrita en la conferencia especializada interamericana sobre derechos humanos (B-32)*. Artículo 11, apartado 2. San José, Costa Rica.

Convenio para la Protección de los Derechos y las Libertades Fundamentales, Artículo 8:

"Derecho al respeto a la vida privada y familiar.

1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

En este caso también destaca la importancia que se le da al derecho y libertad de los seres humanos para que se les respete en su vida privada, su familia, su domicilio o su correspondencia.

Directiva 95/46/CE sobre protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, Artículo 1:

"Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales".

Esta directiva tiene un enfoque más específico para los datos tratados por medios automatizados o las denominadas comunicaciones electrónicas, consagradas en la Directiva 2002/58/CE[12], así como a los datos contenidos en un archivo de papel y tiene como objetivo, proteger los derechos y las libertades de las personas en lo que respecta al tratamiento de datos personales, estableciendo ciertos principios como el de

[12]Parlamento Europeo y del Consejo. (2002). Directiva 2002/58/CE, *relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)*. Bruselas.

Calidad de datos, Legitimación del tratamiento, Derecho al acceso, Derecho de oposición y la notificación del tratamiento.

Convenio 108 del Consejo de Europa, Artículo 1:
"El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona ("protección de datos")".

Como en los otros casos comentados, aquí también se repite la importancia al respeto de los derechos y libertades fundamentales enfatizando la vida privada de las personas.

Es importante mencionar que estos derechos fueron reconocidos con mayor claridad en México tras la reforma del Artículo primero de la Constitución Política de los Estados Unidos Mexicanos (CPEUM). Esta reforma, realizada el 10 de junio de 2011 principalmente cambia la visión de lo que se concebía como "Garantías Individuales" a un concepto más moderno y de reconocimiento en el ámbito internacional, denominándolos "De los Derechos Humanos y sus Garantías", asimismo, en lugar de "otorgar" los derechos, ahora los "reconoce", considerando que se goza de los derechos y mecanismos de garantía reconocidos tanto por la Constitución como por los tratados internacionales, abriéndose con ello de forma clara y decisiva al derecho internacional de los derechos humanos.

Entre otros cambios, incorpora el principio de interpretación *pro personae* que es muy reconocido en el ámbito internacional de los derechos humanos y que se refiere a que cuando existan dos o más interpretaciones o normas jurídicas, se deberá elegir la que más proteja al titular de un derecho humano. Obliga al Estado Mexicano, en todos sus niveles de gobierno, a promover, respetar, proteger y garantizar los derechos humanos además de prevenir, investigar, sancionar y reparar las violaciones a dichos derechos humanos.

Es importante señalar que la CPEUM contempla con mucha claridad el derecho a la protección de datos personales y el derecho a la vida privada, sin embargo, el derecho a la vida privada a nivel federal, no está puntualmente definido como en algunos ámbitos locales, tal es el caso del Distrito Federal, que en su Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, El Honor y la Propia Imagen en el Distrito Federal[13] lo define en su Capítulo I, principalmente en los Artículos 9, 10, 11 y 12 que a continuación son transcritos:

"Artículo 9.- Es vida privada aquella que no está dedicada a una actividad pública y, que por ende, es intrascendente y sin impacto en la sociedad de manera directa; y en donde, en principio, los terceros no deben tener acceso alguno, toda vez que las actividades que en ella se desarrollan no son de su incumbencia ni les afecta."

"Artículo 10.- El derecho a la vida privada se materializa al momento que se protege del conocimiento ajeno a la familia, domicilio, papeles o posesiones y todas aquellas conductas que se llevan a efecto en lugares no abiertos al público, cuando no son de interés público o no se han difundido por el titular del derecho."

"Artículo 11.- Como parte de la vida privada se tendrá derecho a la intimidad que comprende conductas y situaciones que, por su contexto y que por desarrollarse en un ámbito estrictamente privado, no están destinados al conocimiento de terceros o a su divulgación, cuando no son de interés público o no se han difundido por el titular del derecho."

"Artículo 12.- Los hechos y datos sobre la vida privada ajena no deben constituir materia de información. No pierde la condición de íntimo ni de vida privada aquello que ilícitamente es difundido."

[13]Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, El Honor y la Propia Imagen en el Distrito Federal, Publicado el 19 de mayo de 2006 en la *Gaceta Oficial del Distrito Federal* y entró en vigor el 20 de mayo de 2006.

El antecedente directo de la LFPDPPP, es la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), publicada en el *Diario Oficial de la Federación* el 11 de junio de 2002, que tiene por objeto regular el derecho a la información en su dimensión del acceso a la información, sin embargo, refiere que los datos personales serán considerados como información confidencial y que requerirían del consentimiento de los individuos para su difusión, distribución o comercialización en los términos de la propia ley. Esta ley protege la información que se refiere a la vida privada y los datos personales, pero solo a la información en posesión del sector público.

Para entender en qué situación jurídica se encuentra actualmente México, a continuación se hace una breve referencia del marco jurídico actual que le da legitimidad y fuerza a la protección de datos personales, enfocándonos principalmente a los que se encuentran en posesión de los particulares.

1.1. Reforma al Artículo 6° de la Constitución Política de los Estados Unidos Mexicanos.[14]

Esta reforma es resultado de uno de los procesos políticos más esperanzadores de los últimos años en nuestro país:[15] otorga en definitiva, a toda persona, el poder de conocer, sin trabas ni condiciones artificiales, todos los documentos en los que consta la actividad de los gobiernos federal, estatal y municipal de México, estableciendo el acceso a la información pública como un derecho fundamental de los mexicanos. Se trata de una reforma amplia por su alcance y de grandes consecuencias para el futuro ya que introduce el derecho a la protección de datos y diferencia entre la vida privada y los datos personales

Esta reforma es sin duda alguna un gran avance en lo que respecta al derecho de acceso a la información y consecuentemente, de la transparencia en México.

[14] Constitución Política de los Estados Unidos Mexicanos. *Reforma al artículo 6º. Diario Oficial de la Federación* del 6 de marzo de 2007. México.
[15] Instituto Federal de Acceso a la Información Pública (IFAI). (2007). *Reforma al artículo 6º. Constitucional*. México.

El Decreto nos indica que adiciona un segundo párrafo al Artículo 6 con VII fracciones.

Por su relevancia, a continuación se describe dicho párrafo y sus fracciones:

"Artículo 6.-…
Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

I. …
II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.
III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.
IV. …

Por la importancia para este trabajo, a continuación se realiza un breve análisis de la fracción II.

La fracción II es una de las tres fracciones que contienen los principios fundamentales que conforman la base de este derecho, pero también incluye, la posibilidad de las excepciones. Por ejemplo, se establece la importante limitante para el derecho de acceso a la información, específicamente a la vida privada y a los datos personales, siendo claro, que de no existir la restricción, el principio de publicidad pondría en riesgo el derecho a la intimidad y la vida privada, que es otro derecho fundamental.

Como ya se ha comentado, es importante no confundir la vida privada con los datos personales, que aunque están íntimamente relacionados, en el caso de la vida privada,

se refiere a la intervención del Estado y otros particulares; en el caso de los datos personales se refiere a la expresión de la privacidad.

1.2. Reforma al Artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.[16]

Esta reforma es muy importante porque establece el derecho a la protección de datos personales y señala que su propósito es consolidar el derecho a la protección de datos en nuestro país, extendiendo su ámbito de aplicación a todos los niveles y sectores, con lo que complementa la protección de datos en posesión de los particulares.

Es importante señalar que en el contexto de esta reforma, el derecho de protección de datos personales se incluye con el reconocimiento independiente y autónomo.

Por su importancia se destaca lo siguiente de la reforma:

"Artículo 16.- …

"Toda persona tiene derecho a la protección de sus datos personales, así como al derecho de acceder a los mismos, y en su caso, obtener su rectificación, cancelación y manifestar su oposición en los términos que fijan las Leyes. La Ley puede establecer supuestos de excepción a los principios que rigen el tratamiento de datos, por razones de seguridad nacional, de orden, seguridad y salud pública o para proteger los derechos de terceros".

1.3. Reforma al Artículo 73 de la Constitución Política de los Estados Unidos Mexicanos.[17]

[16] Constitución Política de los Estados Unidos Mexicanos. *Reforma al artículo 16.Diario Oficial de la Federación* del 1º. de junio de 2009. México.
[17] Constitución Política de los Estados Unidos Mexicanos. *Reforma al artículo 73, fracción XXIX-O. Diario Oficial de la Federación* del 30 de abril de 2009. México.

La relevancia de esta reforma está en su finalidad de otorgarle la facultad exclusiva al Congreso de la Unión de legislar en materia de protección de datos personales en posesión de los particulares, es decir, faculta al Congreso para expedir una Ley de Protección de Datos en posesión de particulares.

Esta reforma se basa en la utilización de los datos para realizar diferentes transacciones comerciales, por lo que inciden en el ámbito federal, por ello se resalta lo que en realidad hace: obliga también a los particulares a proteger los datos personales que poseen.

1.4. Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y su Reglamento (RLFPDPPP).

Con excepción de la reforma del Artículo 6º. Constitucional (que se refiere a la LFTAIPG), derivado de las reformas constitucionales que se han comentado, el 5 de julio de 2010, se emite la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[18] y el 21 de diciembre de 2011 su Reglamento[19], mismos que a continuación se describen por ser la base jurídica de donde se desprende el fundamento para presente trabajo.

1.4.1. Objeto de la LFPDPPP.

El objeto de la ley se encuentra en el artículo primero que indica "…tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas", en otras palabras, la LFPDPPP pretende evitar el uso indebido o no autorizado de los datos personales, es decir, que los particulares solamente podrán usar nuestros datos para los fines que nos informaron y en cuyo caso otorgamos una autorización, lo que se

[18] Ibídem.
[19] Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación* del 21 de diciembre de 2011 y entró en vigor el 22 de diciembre de 2011.

conoce como principio de consentimiento, por lo que regula el tratamiento legítimo, controlado e informado de los datos personales que están en posesión de particulares, garantizando la privacidad y la autodeterminación Informativa de las personas.

1.4.2. ¿A quién es aplicable la LFPDPPP y su Reglamento (RLFPDPPP)?.

De conformidad con el Artículo 1 de la LFPDPPP, “es de orden público y de observancia general en toda la República…”, dando por hecho que es aplicable a todos. Con mayor detalle, en la primera parte del Artículo 2 señala que “Son sujetos regulados por esta Ley, los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales…”. Esto reafirma que aplica a todos pero además, que no sólo protege a los titulares de los datos, sino también obliga cuando se reciben, tratan o difunden datos personales de otros particulares.

Al referirse este Artículo a “tratamiento”, se debe entender como 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. Es determinante entender, que existe obligación no sólo por obtener datos personales, sino también por almacenarlos y utilizarlos. En este sentido, este instrumento jurídico contempla la obligación también para los sujetos que tenían almacenados datos personales antes de la aplicación de esta Ley.

En la segunda parte del Artículo 2 se determina que existen dos excepciones.

I. Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de información Crediticia y demás disposiciones aplicables; y
II. Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

La primera excepción se debe a que las sociedades de información crediticia cuentan con su propia regulación.

La segunda excepción, tiene su razón en que la Ley protege los datos personales pero no a nivel de la información que se comparte con los círculos más cercanos o familiares y que no tiene fines de divulgación o comercialización, sino simplemente con motivos de convivencia o comunicación familiar. Por ejemplo, las agendas o directorios personales de contactos.

Por su parte, el RLFPDPPP en su Artículo 1, indica que su objeto es el de reglamentar las disposiciones establecidas en la LFPDPPP, en el Artículo 2 señala una serie de definiciones adicionales a las del Artículo 3 de la LFPDPPP y su ámbito objetivo de aplicación queda en el Artículo 3 donde menciona que "… Reglamento será de aplicación al tratamiento de datos personales que obren en soportes físicos o electrónicos, que hagan posible el acceso a los datos personales con arreglo a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización…".

1.4.3. ¿Qué son los datos personales?.

De acuerdo con la LFPDPPP en su Artículo 3 fracción V, los datos personales son: "Cualquier información concerniente a una persona física identificada o identificable" y esta definición se complementa con lo establecido en el tercer párrafo del Artículo 3 del RLFPDPPP que dice "…los datos personales podrán estar expresados en forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a una persona física identificada o persona física identificable".

En calidad de expertos en el tema, el Instituto Federal de Acceso a la Información Pública y Protección de Datos (IFAI) y la propia Ley, hacen una distinción para ciertos datos que se consideran como sensibles o no sensibles.

A continuación, se mencionan los tipos de datos personales, así como algunos ejemplos para mayor claridad en este punto:

- **No sensibles**
  - ***Datos de identificación:*** nombre, domicilio, teléfono, correo electrónico, firma, RFC, CURP, fecha de nacimiento, edad, nacionalidad, estado civil, etcétera.
  - ***Datos patrimoniales:*** información fiscal, historial crediticia, cuentas bancarias, ingresos y egresos, etcétera.
  - ***Datos académicos:*** trayectoria educativa, título, número de cédula, certificados, etcétera.
  - ***Datos laborales:*** puesto, domicilio, correo electrónico y teléfono del trabajo.

- **Sensibles**
  - ***Datos ideológicos:*** creencias religiosas, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, vida y hábitos sexuales, origen étnico y racial.
  - ***Características personales:*** tipo de sangre, ADN, huella digital, color de piel, iris, y cabello, señales particulares, etc.
  - ***Datos de salud:*** estado de salud, historial clínico, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, etc.
  - ***Características físicas:*** color de piel, iris, y cabello, señales particulares, vida y hábitos sexuales, origen étnico y racial, etcétera.

Para el caso de los datos sensibles, por su relevancia, la propia LFPDPPP establece una mayor protección y la refiere en su fracción VI del Artículo 3 como: “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, preferencia sexual".

1.4.4 Otros conceptos relevantes relacionados con la LFPDPPP y su Reglamento.

Para mayor información se enuncia y describe brevemente otros conceptos que establece la LFPDPPP en sus Artículos 3 y 6, así como en los Artículos 2 y 9 del RLFPDPPP, que son muy importantes en referencia a la protección de datos personales y a los derechos y obligaciones, los cuales serán tratados con mayor detalle en el Capítulo III del presente proyecto integrador.

- **Responsable:** Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.
- **Titular:** Persona física a quien corresponden los datos personales.
- **Tratamiento:** Obtención, uso, divulgación o almacenamiento de datos personales por cualquier medio.
- **Aviso de privacidad:** Documento físico, electrónico o en cualquier otro formato que genera el responsable y pone a disposición del titular previo al tratamiento de sus datos.
- **Derechos ARCO:** Son los derechos de acceso, rectificación, cancelación y rectificación.
- **Entorno digital:** Ámbito conformado por el hardware, software, redes, aplicaciones, servicios o cualquier otra tecnología de la sociedad de la información que permita el intercambio o procesamiento informatizado o digitalizado de datos.
- **Listado de exclusión:** Base de datos que registra la negativa de un titular al tratamiento de sus datos personales.
- **Medidas de seguridad administrativas:** Conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la

concienciación, formación y capacitación del personal, en materia de protección de datos personales.

- **Medidas de seguridad físicas:** Conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología.
- **Medidas de seguridad técnicas:** Conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar que los accesos a la base de datos de información sea por usuarios autorizados, para que se realicen sólo las actividades autorizadas, se incluyan acciones para la adquisición de, operación, desarrollo y mantenimiento de sistemas seguros y se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales.

Principios

- **Licitud:** Obliga al responsable a tratar los datos con apego a las leyes.
- **Consentimiento:** Facultad para decidir si se comparte o no su información.
- **Finalidad:** Los datos solo pueden ser tratados para el fin que se estableció en el aviso de privacidad.
- **Lealtad:** Obligación del responsable de proteger los intereses del titular.
- **Calidad:** Que los datos sean exactos, completos, pertinentes y correctos.
- **Información:** Qué tipo de información se recaba y para qué.
- **Proporcionalidad:** Datos estrictamente necesarios.
- **Responsabilidad:** Cumplimiento de los principios.

1.5. Definición conceptual de Metodología de Mejores Prácticas.

Siendo el objetivo principal del presente trabajo proponer una Metodología de Mejores Prácticas para implementar la LFPDPPP y su Reglamento, se delimitó su concepto al punto de vista enfocado a la administración y el derecho, quienes la definen como el

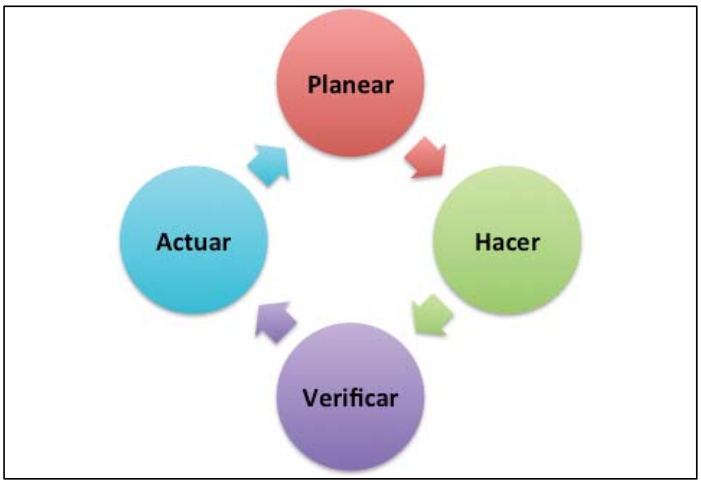
arte de aplicar el método conveniente a una obra o actividad determinada[20] o a un procedimiento ordenado que permite cumplir los objetivos que se proponen.

En cuanto a la determinación de mejores o buenas prácticas, es un concepto de la administración que engloba aspectos como la estandarización, la medición, monitoreo, el incremento de la satisfacción del cliente, el logro de objetivos y la mejora continua como en el caso de la norma ISO9001:2008[21] para sistemas de gestión de calidad. Desde la administración e implementación de un proyecto, de acuerdo con el Instituto de Administración de Proyectos[22] (PMI por sus siglas en inglés), una buena práctica es la aplicación de habilidades, herramientas y técnicas que pueden aumentar las posibilidades de éxito de un proyecto.

Una buena práctica también implica un ciclo o fases, por lo que es importante para efectos del presente trabajo, incluir como una referencia para la metodología de implementación que se propone en el Capítulo IV, el Ciclo de Deming, que aún y cuando su enfoque es para lograr la mejora continua en una organización o empresa, puede ser utilizado como una herramienta para apoyar la metodología de implementación de la LFPDDPP.

El ciclo de Deming está representado en el siguiente gráfico acompañado de una breve explicación de cada fase.

[20] De Pina Vara, Rafael. (1988). Diccionario de Derecho. (15 ava ed.), Porrúa, Pp. 352,México, D.F.
[21] International Organization for Standardization (ISO). *Norma ISO9001:2008*. http://www.iso.org/iso/home/standards/management-standards/iso_9000.htm
[22] Project Management Institute. (2008). *Guía del PMBOK*. (4ª. Edición). Pp. 4-6. Newtown Square, Pennsylvania. USA.



Gráfica 2. Fuente: Ciclo de Deming. Administración de proyectos, Global Knowledge Training, LLC, P.38. 2013.

Planear: consiste en definir los objetivos y los medios para conseguirlos.
Hacer: Se refiere al acto de ejecutar lo planeado y contempla el organizar, dirigir, asignar recursos y supervisar la ejecución.
Verificar: Implica comprobar que se alcanzan los objetivos previstos con los recursos previamente asignados, monitoreando y evaluando cada fase.
Actuar: Se refiere a analizar y corregir las posibles desviaciones detectadas, así como también se debe proponer mejoras a los procesos ya empleados.

Se puede decir entonces que una buena práctica, es la suma de las técnicas, las herramientas, las formas de trabajo, los métodos o soluciones de proceso que pueden ser identificadas como las más adecuadas o las mejores para realizar una cierta actividad.

Considerando todo lo antes expuesto, la definición de metodología de mejores prácticas que se utilizará es “Una serie de los pasos que representan la forma más efectiva de lograr un objetivo, utilizando un modelo probado que se adecue a la infraestructura y al contexto de una organización”.

Toda vez que en este Capítulo ya fue presentado el marco teórico conceptual del derecho a la protección de datos personales en posesión de los particulares desde su origen, base jurídica y figuras que lo conforman, además de haber definido los conceptos que serán utilizados durante todo el documento, se puede continuar al segundo Capítulo en donde es analizado con mayor detalle la situación actual en la que se encuentran las empresas y los particulares en México en cuanto al apropiamiento, implementación y cumplimiento de la Ley y su Reglamento.

CAPÍTULO II: SITUACIÓN ACTUAL.

Este Capítulo ilustrará que a pesar del marco jurídico existente aún no se conocen la Ley y su Reglamento en la proporción debida y tampoco se tienen los avances adecuados en su implantación a nivel nacional.

2.1. Situación actual.

No existen estudios periódicos, estandarizados y actualizados para conocer el avance en el cumplimiento de la LFPDPPP y su Reglamento, sin embargo, después de una revisión minuciosa, para la presente problemática se optó por utilizar principalmente la base de información de Deloitte[23] de la que se presentan a continuación algunas gráficas:

Gráfica 3. Fuente: Termómetro. (2012). Privacidad de datos. LFPDPPP. Deloitte.

La empresa Deloitte, señala que pese a la entrada en vigor de la LFPDPPP el 26% de las compañías mexicanas aún no la conoce. (Gráfica 3).

[23]Deloitte. Termómetro. (2012). *Privacidad de datos. Ley Federal de Protección de Datos Personales en Posesión de los Particulares.* México.

Gráfica 4. Fuente: Termómetro. (2012). Privacidad de datos. LFPDPPP. Deloitte.

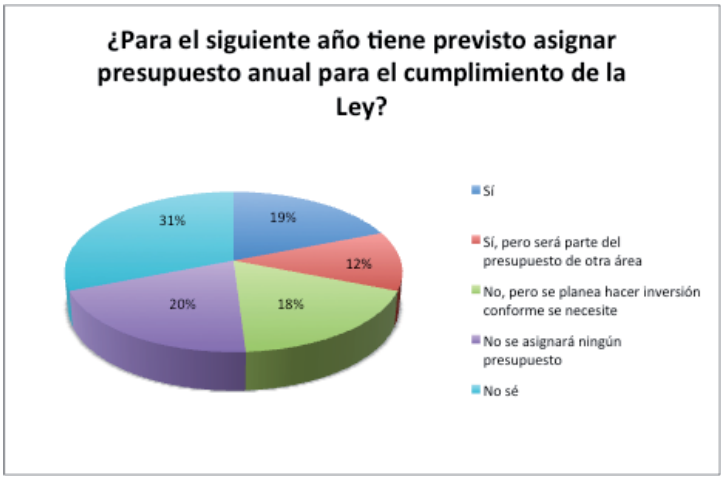
El 53% de los empleados de las compañías encuestadas no tienen pleno conocimiento de su responsabilidad y de las diversas sanciones que pueden derivarse de la Ley. (Gráfica 4).

Gráfica 5. Fuente: Termómetro. (2012). Privacidad de datos. LFPDPPP. Deloitte.

Debido a la importancia que tienen la concientización y conocimiento de la Ley, también se cuestionó a los participantes sobre la existencia de un programa al respecto; el 40% indicó que en su empresa no existe tal programa. (Gráfica 5).

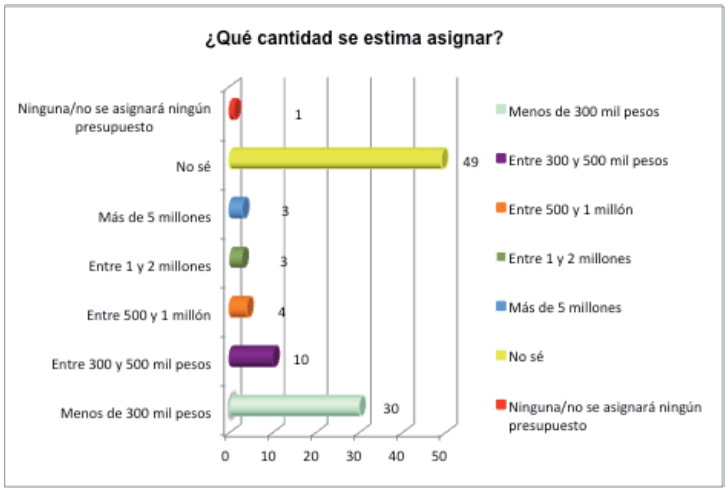
Gráfica 6. Fuente: Termómetro. (2012). Privacidad de datos. LFPDPPP. Deloitte.

Sólo el 17% de las empresas encuestadas han realizado completamente modificaciones a sus procesos de negocio para lograr el cumplimiento de la Ley. (Gráfica 6.)



Gráfica 7. Fuente: Termómetro. (2012). Privacidad de datos. LFPDPPP. Deloitte.

El 31% tienen previsto asignar un presupuesto económico anual o parte del presupuesto de otra área para lograr el cumplimiento de la Ley. (Gráfica 7).



Gráfica 8. Fuente: Termómetro. (2012). Privacidad de datos. LFPDPPP. Deloitte.

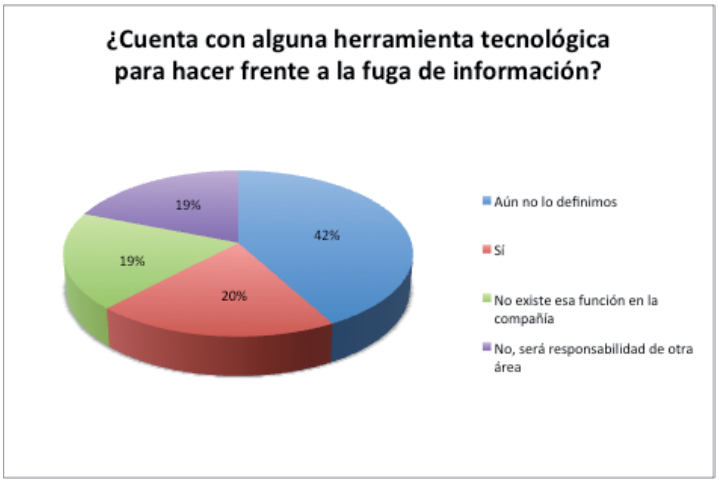
En cuanto al presupuesto estimado a asignar de acuerdo a los encuestados, el 49% manifestó desconocer cuanto asignará. (Gráfica 8).

Gráfica 9. Fuente: Termómetro. (2012). Privacidad de datos. LFPDPPP. Deloitte.

En el tema de contar con el aviso de privacidad necesario de acuerdo a la Ley, 53% informaron que ya cuentan con él, lo que puede considerarse como un cumplimiento bajo pese a que a partir de julio del 2011 ya lo debería de haber tenido. (Gráfica 9).

Gráfica 10. Fuente: Termómetro. (2012). Privacidad de datos. LFPDPPP. Deloitte.

A pesar de que el proceso para la atención de derechos ARCO inició el 6 de enero de 2012, sólo el 30% de las empresas encuestadas ya cuentan con los procesos y métodos necesarios para medir la atención de dichos derechos. (Gráfica 10).



Gráfica 11. Fuente: Termómetro. (2012). Privacidad de datos. LFPDPPP. Deloitte.

42% de las empresas aún no cuentan con una definición del uso de las TI para el soporte a las compañías; principalmente para hacer frente a la fuga de la información, además de emplear instrumentos tecnológicos para cumplir con la Ley. (Gráfica 11).

Gráfica 12. Fuente: Termómetro. (2012). Privacidad de datos. LFPDPPP. Deloitte.

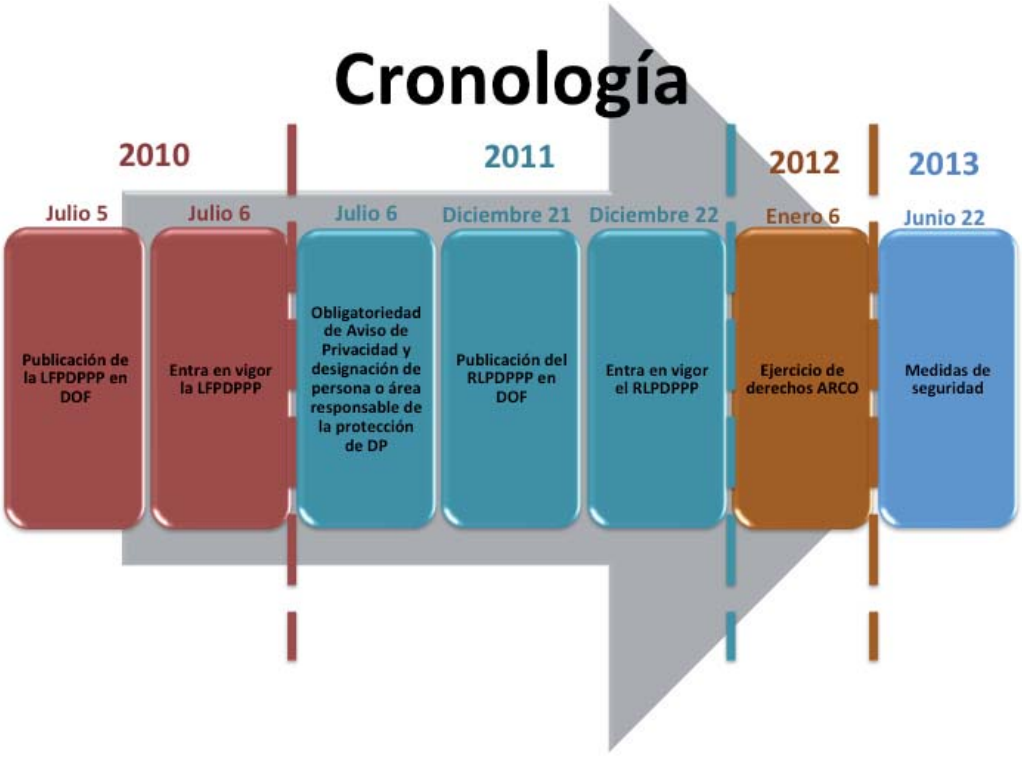
Al preguntar si las empresas cuentan con los recursos internos necesarios para cumplir con la Ley, sólo el 58% de los participantes declara que en su organización sí se cuenta con dichos recursos. (Gráfica 12.).

Después de analizar las gráficas e información anteriores, es claro que algunas empresas comenzaron a trabajar en la capacitación de su personal en materia de la LFPDPPP, así como en la adecuación o implementación de medidas para su cumplimiento, pese a ello, aún quedan muchas áreas de oportunidad para lograr el cumplimiento de la Ley y su Reglamento, como la falta de una metodología de mejores prácticas y otras herramientas que los apoye para la implementación de la Ley.

2.2. Cronología de cumplimiento.

Han sido diversas fechas las que la LFPDPPP y su Reglamento, han marcado como límite para el cumplimiento por parte de los responsables y en general por todos los sujetos obligados respecto a su exigibilidad.

Por lo anterior, a continuación se expone la cronología de eventos y en su caso, de la aplicación de la LFDPPP y su Reglamento.



Gráfica 13. Fuente: Elaboración propia con datos de la LFPDPPP y del RLFPDPPP.

Esta cronología es sumamente importante porque establece con precisión las fechas de la exigibilidad de la Ley, su Reglamento y los principales hitos, evitando confusiones para su cumplimiento.

2.3. Problemática.

Después de haber analizado los datos expuestos anteriormente, se puede determinar que si bien han existido avances en varios rubros para el cumplimiento de la LFPDPPP y su Reglamento, aún quedan muchos aspectos por cubrir.

Es claro que actualmente no existe una herramienta o metodología que permita, utilizando una combinación de las mejores prácticas, resolver entre otros, los siguientes problemas:

- Un alto porcentaje de las empresas no están cumpliendo con la totalidad de los requerimientos conforme a la Ley y su Reglamento.
- Existe un bajo porcentaje de cumplimiento con respecto del aviso de privacidad.
- Muchas empresas no cuentan con un programa de comunicación o concientización de la Ley.
- Los empleados no conocen sus responsabilidades y sanciones respecto de la LFPDPPP.
- Las empresas no cuentan con un presupuesto definido para la implementación y cumplimiento de la Ley.
- Las empresas no cuentan con un proceso definido para la atención de los derechos ARCO.
- Un alto porcentaje de las empresas no cuenta con los instrumentos tecnológicos necesarios para cumplir con la Ley.

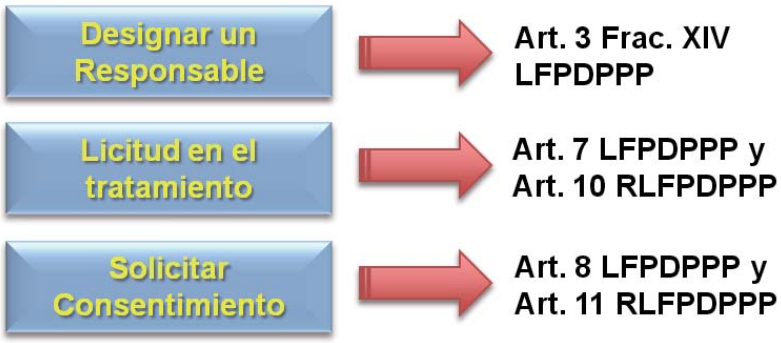
Como se ha visto en este Capítulo, se confirma la importancia de contar con una metodología de mejores prácticas que permita realizar una adecuada y exitosa implantación de la LFPDPPP y su Reglamento, es por ello que en el siguiente Capítulo se determinará y se analizarán las principales obligaciones que los particulares deben cumplir en relación a los datos personales.

CAPÍTULO III: ¿CUÁLES SON LAS PRINCIPALES OBLIGACIONES A CUMPLIR POR LOS PARTICULARES (PERSONAS Y EMPRESAS) CON RESPECTO DE LOS DATOS PERSONALES?.

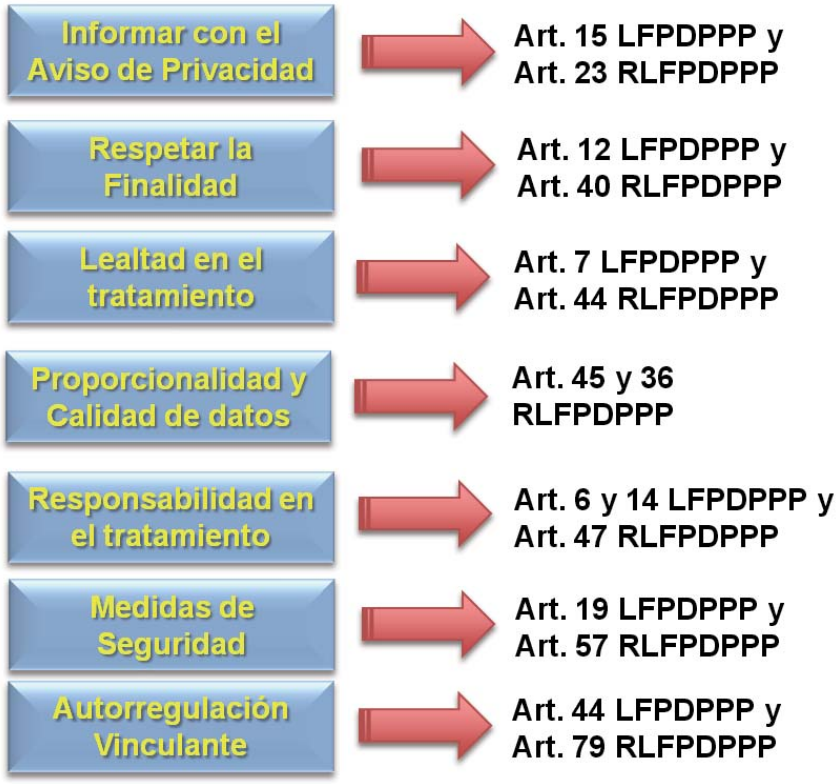
Considerando lo expuesto en los Capítulos I y II, en este Capítulo se plantean las principales obligaciones que los particulares y empresas deben cumplir de conformidad con la LFPDPPP y su Reglamento.

Proteger los datos personales implica la observancia de una serie de principios y obligaciones por parte del responsable y del encargado que trata los datos para garantizar la privacidad de dichos datos.

En el siguiente cuadro se presentan las principales obligaciones que deben cumplirse de conformidad con la Ley y su Reglamento:



Gráfica 14. Fuente: Elaboración propia con datos de la LFPDPPP y del RLFPDPPP.



Gráfica 14. Fuente: Elaboración propia con datos de la LFPDPPP y del RLFPDPPP.

3.1. Designar un responsable.

De conformidad con el Artículo 3 fracción XIV, el responsable es la "persona física o moral de carácter privado que decide sobre el tratamiento de datos personales" y de conformidad con la fracción IX, el encargado es la "persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable".

Aunque en estricto sentido no existe un Artículo que obligue a la determinación de un responsable físicamente hablando, se considera que tiene una gran importancia por ser la figura encargada del cumplimiento real de muchas de las obligaciones establecidas en la LFPDPPP y su Reglamento, por ello es importante hacer una distinción entre el responsable "empresa" y el responsable "persona o departamento". El responsable

“empresa” como su denominación dice, es la organización o persona moral y en el caso del responsable “persona o departamento” es una persona o personas físicas designadas por la organización para llevar a cabo las actividades que establecen la Ley y su Reglamento, de ahí se deriva la importancia de contar con un responsable físico designado e identificado, que puede llamarse encargado (sin confundirlo con el externo que pueda contratarse para tratar datos personales) u oficial de privacidad.

No está por demás señalar que al momento del desarrollo del presente trabajo se ha incluido la obligación que debió cumplirse desde el pasado 6 de julio de 2011 para nombrar a la persona o departamento de datos personales.

3.2. Licitud en el tratamiento.

Este principio obliga al responsable a que el tratamiento de los datos personales sea con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional, es decir, que la posesión de datos debe ser legal y legítima, considerando las atribuciones del tratante, obteniendo los datos por los medios establecidos en la Ley y su Reglamento y utilizarlos exclusivamente para los fines que fueron recabados.

3.3. Solicitar consentimiento.

En este caso, el responsable deberá obtener el consentimiento para el tratamiento de los datos personales. Esta solicitud deberá ir referida a una finalidad o finalidades determinadas, previstas en el aviso de privacidad. Es importante señalar que cuando los datos personales se obtengan directamente de su titular, el consentimiento deberá ser previo al tratamiento. El consentimiento puede ser tácito o expreso.

Debemos resaltar que hay tres elementos fundamentales en el consentimiento que otorga el titular de los datos:

- Debe ser otorgado de manera libre
- Debe ser expreso

- Debe hacerlo informado

3.4. Informar con el aviso de privacidad.

Este principio obliga al responsable a dar a conocer al titular la información relativa a la existencia y características principales del tratamiento a que serán sometidos sus datos personales a través del aviso de privacidad.

El aviso de privacidad es una de las obligaciones más importantes que los responsables del tratamiento deben considerar puesto que es el mecanismo para informar a los titulares lo que pasará con sus datos y lo que confiere el carácter de licitud al tratamiento. Se debe informar correctamente al titular en el momento de recabar sus datos, el fundamento, el motivo y el propósito para los cuales serán tratados.

Este aviso debe tener cuando menos las siguientes características:

- Ser sencillo
- Utilizar un lenguaje claro y comprensible
- Con la estructura y diseño que facilite su entendimiento

Su difusión puede ser mediante el uso de formatos físicos, electrónicos, medios verbales o cualquier otra tecnología que cumpla el objetivo de informar al titular.

Deberá contar cuando menos con los siguientes elementos:

- La identidad y domicilio del responsable que recaba los datos
- Las finalidades del tratamiento de los datos
- Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos

- Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en la LFPDPPP
- En su caso, las transferencias de datos que se efectúen
- El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad
- Cuando se trate de datos personales sensibles, deberá señalarse expresamente en el aviso que se trata de dichos datos

3.5. Respetar la finalidad.

Se refiere a que los datos personales sólo podrán ser tratados para el cumplimiento de la finalidad o finalidades establecidas en el aviso de privacidad. El responsable, identificará y distinguirá en el aviso de privacidad, entre las finalidades de origen y necesarias para la relación jurídica, de aquellas que no lo son.

3.6. Lealtad en el tratamiento.

Este principio establece la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

Como en otros casos, los principios van ligados o se complementan unos con otros, por ello, cuando se habla de lealtad en el tratamiento, se debe pensar en la ética en la recolección de datos, que no sea de forma fraudulenta, desleal o ilícita.

3.7. Proporcionalidad y Calidad de datos.

En este caso la LFPDPPP determina que sólo podrán ser objeto de tratamiento los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las que se hayan obtenido, por lo que el responsable está obligado a realizar esfuerzos razonables para que los datos personales tratados sean los mínimos

necesarios de acuerdo con la finalidad del tratamiento que tenga lugar, lo que se conoce como criterio de minimización.

El principio de calidad se refiere a que los datos personales tratados deben ser exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para lo que son tratados.

Por lo anterior, cuando se analiza el principio de proporcionalidad, también se debe considerar el principio de calidad ya que en el primero hablamos de recabar sólo los datos necesarios e importantes en relación con la finalidad y en el segundo, estamos considerando que sean correctos y pertinentes también con respecto a la finalidad por lo que se complementan.

3.8. Responsabilidad en el tratamiento.

El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión y podrá valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que determine adecuado para tales fines.

El responsable podrá adoptar, cuando menos, las siguientes medidas:

- Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización del responsable.
- Poner en práctica un programa de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales.
- Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.

- Destinar recursos para la instrumentación de los programas y políticas de privacidad.
- Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.
- Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.
- Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.
- Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.
- Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones establecidos en la LFPDPPP y su reglamento.
- Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permitan rastrear a los datos personales durante su tratamiento.

3.9. Medidas de seguridad.

El responsable y en su caso, el encargado, tienen la obligación de establecer y mantener las medidas de seguridad administrativas, físicas y técnicas para la protección de los datos personales, entendiendo para tales efectos, como medidas de seguridad, el control o grupo de controles de seguridad para proteger los datos personales. Considerando que la información es un activo que debe protegerse mediante un conjunto coherente de procesos y sistemas diseñados, administrados y mantenidos por la propia organización, el IFAI generó la "Guía para la elaboración de un Documento de Seguridad"[24], que puede servir como ejemplo para elaborar el

[24]Instituto Federal de Acceso a la Información Pública (IFAI). (2009). *Guía para la elaboración de un documento de seguridad*. V1.4. México.

documento propio de la empresa de conformidad con sus características particulares. Se puede decir que el modelo del documento considera principalmente un catálogo de sistemas de datos personales, estructura y descripción de los sistemas de datos personales, medidas de seguridad implementadas y el procedimiento para la cancelación de un sistema de datos personales.

Considerando lo anterior y de manera enunciativa, más no limitativa, las acciones que el responsable deberá contemplar para establecer y mantener la seguridad de los datos personales son:

- Elaborar un inventario de datos personales y de los sistemas de tratamiento.
- Determinar las funciones y obligaciones de las personas que traten datos personales.
- Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.
- Establecer las medidas de seguridad aplicables a los datos personales e identificar aquellas implementadas de manera efectiva.
- Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquellas faltantes que resultan necesarias para la protección de los datos personales.
- Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes derivadas del análisis de brecha.
- Llevar a cabo revisiones o auditorías.
- Capacitar al personal que efectúe el tratamiento.
- Realizar un registro de las medidas de almacenamiento de los datos personales.

Estas medidas de seguridad son sumamente importantes porque serán las que le permitan al responsable garantizar al titular la integridad, confiabilidad, confidencialidad y disponibilidad de los datos recabados, evitando su alteración, pérdida, transmisión y accesos no autorizados promoviendo la confianza del titular de los datos.

3.10. Autorregulación vinculante.

Aunque no es una obligación, se considera que la autorregulación vinculante es una acción que complementa y aporta diversos elementos para fortalecer la protección de los datos personales. El Artículo 44 de la LFPDPPP, establece que las personas físicas o morales, podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos personales y podrán traducirse en códigos deontológicos o de buena práctica profesional.

La importancia de la autorregulación vinculante queda clara toda vez que la Secretaría de Economía desarrolló los parámetros para el correcto desarrollo de los esquemas de autorregulación vinculante a que se refiere el Artículo 44 de la LFDPDPPP, publicados en el *Diario Oficial de la Federación*, el 17 de enero de 2013.

Debemos entender a la autorregulación como aquellas actividades complementarias que los responsables se comprometen a realizar adicionalmente a lo establecido en la Ley y su Reglamento y que de conformidad con los esquemas de autorregulación establecidos deben contar con mecanismos de medición de la eficacia con que cumplen con la protección de datos y al mismo tiempo, prever medidas correctivas eficaces en caso de incumplimiento de los esquemas generando mayor confianza en los titulares de datos y en el Instituto Federal de Acceso a la Información y Protección de Datos.

Los esquemas pueden ser a través de acreditaciones, certificaciones, auditorías, evaluaciones, que se traducen en códigos deontológicos, códigos de buenas prácticas profesionales, políticas de privacidad, reglas de privacidad corporativas, sellos de confianza y certificaciones.

Es importante señalar que la mayoría de los principios y/o las obligaciones establecidas en la LFPDPPP y su Reglamento, están íntimamente relacionadas con la utilización o

posible utilización de tecnologías de la información y comunicación. En muchos casos las medidas de seguridad deben realizarse a través del uso de tecnología.

3.11. Sanciones.

Como se ha visto durante este Capítulo, existen una serie de obligaciones que deben cumplir los responsables de acuerdo con la Ley y su Reglamento, sin embargo, también están establecidas las sanciones por el incumplimiento y en términos generales, podríamos dividirlas en las siguientes que ya incluyen las sanciones administrativas como el apercibimiento:

Tipo	Descripción
Patrimoniales	Multas que van desde 100 hasta 320,000 días de salario mínimo vigente en el Distrito Federal (DSMVDF), que en 2013 es de $64.76 pesos, es decir, la multa sería de $6,476.00 hasta $20,723,200.00. Para la primera falta, la sanción es el apercibimiento que aplica en caso de no cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada. Asimismo, existen otra serie de conductas como el actuar con negligencia o dolo, declarar dolosamente que no existen datos personales, omitir en el aviso de privacidad uno o varios elementos, entre otras más, que se sancionan con multa de 100 a 160,000 (DSMVDF) y otras que van desde 200 a 320,000 (DSMVDF).
Penales	• De 3 meses a 3 años de prisión a quien siendo responsable, vulnere la seguridad de datos personales bajo su custodia con ánimo de lucro.

	• Prisión de 6 meses a 5 años a quien con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño. En caso de datos personales sensibles el monto de la pena se incrementará hasta 2 veces.

Durante este Capítulo fueron presentadas las principales obligaciones que los particulares deben cumplir conforme la LFPDPPP y su Reglamento obteniendo con ello lo que los particulares están obligados a hacer. En el siguiente Capítulo se propone una metodología que facilite dicho cumplimiento utilizando algunas de las mejores prácticas que sirvieron a las personas físicas o morales que ya han implementado la LFPDPPP y su Reglamento.

CAPÍTULO IV: Propuesta de metodología de mejores prácticas para la implementación de la LFPDPPP.

Una vez desarrollado el marco teórico conceptual, detectadas la problemática y situación actual y habiendo determinado las principales obligaciones establecidas en la LFPDPPP y su Reglamento, en este Capítulo se presenta la propuesta de metodología de mejores prácticas para la implementación exitosa de la citada Ley y su Reglamento, considerando que los temas en que los particulares deben poner mayor énfasis, son principalmente, contar con canales de comunicación efectivos con los titulares para efectos del aviso de privacidad y el ejercicio de sus derechos ARCO, la seguridad administrativa, física y técnica en el manejo de los datos personales y readecuar sus procesos para que los titulares puedan acceder a los citados derechos ARCO.

Como se planteó en el Capítulo III, la Ley y su Reglamento nos obliga a cumplir con los 8 principios: Licitud, Consentimiento, Información, Calidad, Finalidad, Lealtad, Proporcionalidad y Responsabilidad, por lo que la metodología debe estar alineada a dicho cumplimiento.

Es importante señalar que esta propuesta se basa en conceptos de:

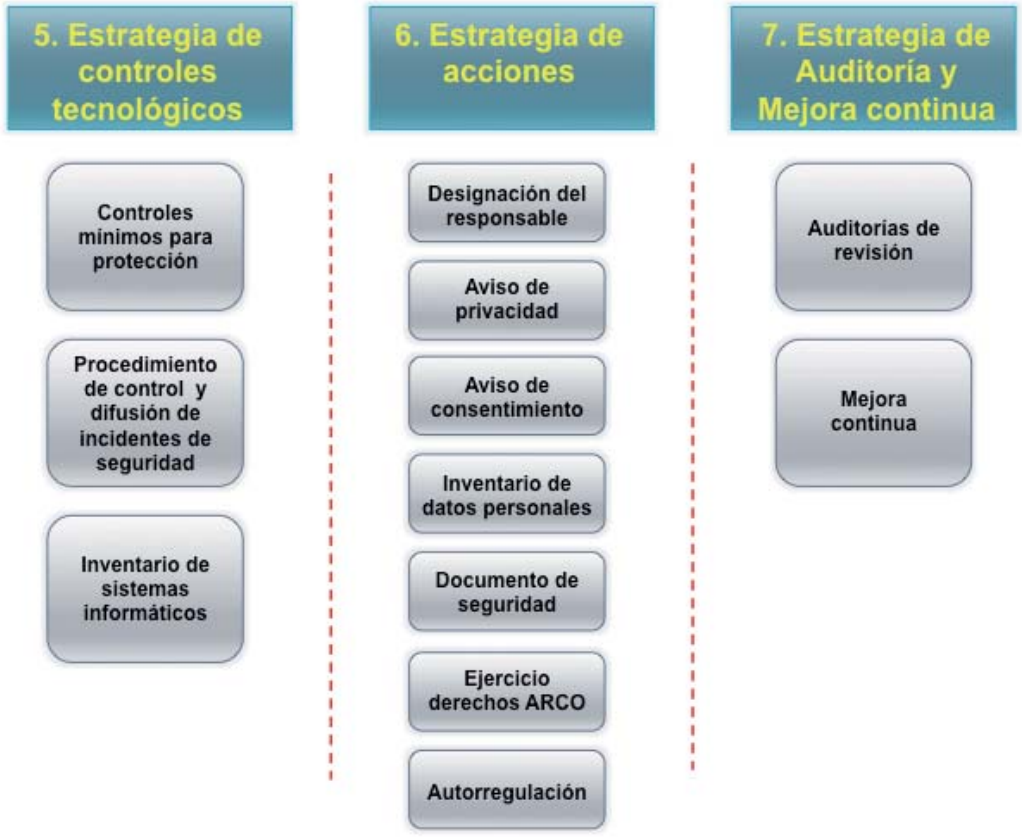
- Mejora continua.
- Gestión de la calidad.
- El ciclo de Deming.
- Las mejores prácticas de administración de proyectos.
- Diferentes documentos emitidos por el IFAI.
- La experiencia de diversas empresas que ya implementaron la Ley y su Reglamento.
- La experiencia de consultorías especializadas como *Pricewaterhouse Coopers* y *SCITUM* entre otras.
- Los resultados de los estudios realizados por la *AMIPCI* y *DELOITTE*.
- Experiencias propias en el ámbito de la protección de datos personales.

La metodología que se desarrolla a continuación, se divide en siete estrategias principales y cada una de ellas, contiene una serie de actividades que apoyarán el cumplimiento adecuado.

Es importante señalar que dependiendo de las características particulares y del tamaño de cada empresa, se pueden hacer ajustes a las actividades de la metodología.

Con el propósito de visualizar de manera simple las estrategias y actividades, se presenta el esquema general:

Gráfica 15. Fuente: Elaboración propia con datos de la LFPDPPP, del RLFPDPPP y otros documentos.



Gráfica 15. Fuente: Elaboración propia con datos de la LFPDPPP, del RLFPDPPP y otros documentos.

4.1. Estrategia de Diagnóstico y Plan de implementación.

Considerando que para el éxito de cualquier proyecto que implique la modificación de los procesos y ajustes en la "forma de cómo se vienen haciendo" ciertas actividades, lo primero es determinar la situación actual de la empresa.

Se debe integrar un diagnóstico participativo con la totalidad de las áreas y el personal de las mismas, incluyendo por supuesto, a los directivos.

En congruencia con las obligaciones de la Ley y su Reglamento, se deben determinar los siguientes aspectos:

- ¿Qué personal conoce y qué tanto entiende de la Ley, su Reglamento y las implicaciones para ellos y su empresa?.
- ¿La empresa ya cumple en alguna medida con la Ley y su Reglamento?.
- Identificar los procesos de negocio actuales en los que se tratan datos personales, considerando qué datos personales se están manejando, en qué parte están estos datos y las medidas de seguridad que existen actualmente.
- Identificar el flujo de información, es decir, determinar las fuentes (¿cómo?) y orígenes (¿de dónde?) de los datos personales que se están manejando.
- ¿Cuenta con presupuesto asignado para cumplir con las medidas físicas, tecnológicas y humanas para el cumplimiento de la Ley y su Reglamento?.
- Realizar un inventario de datos personales determinando si son o no son datos sensibles, si son o no necesarios para los fines para los que se recaban además de identificar los riesgos existentes en relación al manejo actual de los datos personales.

Como parte de esta estrategia y una vez establecido el diagnóstico y la situación actual de la empresa, debemos generar el plan de implementación con un cronograma y calendario de actividades, con tiempos y responsables, incluyendo cuando menos las siguientes estrategias:

4.2. Estrategia de comunicación.

Sin duda esta es una de la estrategias más importantes porque en ésta se deben incluir todos los mecanismos de comunicación, tanto interna como externa, para que todo el personal de la empresa, proveedores y titulares o clientes, estén plenamente informados de los cambios que se realizarán en la organización como consecuencia del cumplimiento de la Ley y su Reglamento, así como de las responsabilidades y

sanciones a las que pueden hacerse acreedores y en el caso de los titulares, los derechos que pueden ejercer en cuanto a sus datos personales.

Se deben proporcionar pláticas de sensibilización además de capacitación a los puestos clave en todos los niveles de la organización (directivos, operativos y técnicos), en relación a la importancia de proteger los datos personales, también de las estrategias de implementación, cambios de procedimientos y medidas físicas, técnicas y administrativas que serán aplicados en sus áreas, es decir, que se logre un entendimiento pleno de la Ley y su Reglamento.

Generar con apego a la Ley y su Reglamento, información clara y precisa dirigida a los clientes en cuanto al aviso de privacidad, la política de confidencialidad y las medidas que la empresa ha implementado para la protección de sus datos personales, así como de los mecanismos para ejercer sus derechos ARCO.

Es de suma importancia crear un programa permanente de comunicación interna y externa respecto de la protección de datos personales.

4.3. Estrategia de roles y funciones.

Como ya fue visto en los Capítulos anteriores, una de las obligaciones de la Ley y su Reglamento, es el designar una persona o departamento responsable (oficial de privacidad, además de un encargado) de la protección de datos personales en la organización (como ya se explicó en el Capítulo III, es la persona física o área designada para encargarse del cumplimiento de la Ley y su Reglamento) que tendrá la función principal de dar trámite a las solicitudes de los titulares para el ejercicio de sus derechos ARCO y será el principal promotor de la protección de datos personales.

Es muy claro que si la figura del oficial de privacidad no tiene una silla en la junta directiva de la empresa, la implementación de la Ley y su Reglamento no tendrá éxito, ya que los directivos deben involucrarse y entender la importancia del rol del oficial de

privacidad y por ende, apoyarlo para que las acciones que deban realizarse permeen a todos los niveles de la organización. Por lo anterior, en esta estrategia se propone que se integre una Junta de Protección de Datos Personales, en la que participen, como miembros titulares, un representante de cada área de la empresa de primera línea; de acuerdo a la configuración de cada empresa pueden ser: Dirección, Administración, Finanzas, Producción y Ventas.

La Junta de Protección de Datos Personales será la responsable de proporcionar el apoyo necesario en cuanto a recursos físicos, humanos y materiales para el mejor cumplimiento de la Ley y su Reglamento.

También deberá integrarse un grupo de capacitación con representantes de todas las áreas a nivel operativo que permanentemente capacite e involucre a toda la empresa en los temas de tratamiento y protección de datos personales.

4.4. Estrategia de procesos.

En esta estrategia se deben incluir los procesos y políticas necesarios para cumplir con la Ley y su Reglamento. Cuando menos deberán incluir la definición, desarrollo e implementación de:

- **La política de protección de datos personales y datos sensibles.** Esta política debe definir claramente los términos, uso y finalidades, así como los mecanismos para ejercer los derechos ARCO.
- **Definición de la política de confidencialidad de la empresa**. La finalidad de esta política es establecer los lineamientos bajo los cuales se manejará la información en la empresa por cada uno de sus miembros, garantizando la privacidad y confidencialidad de la información y debe incluir los objetivos, procesos y sistemas para tales efectos.
- **Modelo de responsabilidades.** Se debe establecer con toda precisión la definición de quien es el responsable, custodio, titular y encargado de la

seguridad de los datos personales y su tratamiento, así como el domicilio y datos de contacto.

- **Definir los diferentes procesos a implantar.** Es muy importante establecer los procesos que se seguirán para la obtención de datos personales y datos sensibles, el acceso, respaldo y atención de incidentes, además del proceso para el intercambio seguro de los datos considerando las características particulares de la empresa, la industria a la que pertenece y el tamaño, entre otros criterios.
- **Definición de procedimientos para la entrega del aviso de privacidad y del consentimiento expreso para datos sensibles.** Se deben establecer los mecanismos para la entrega del aviso de privacidad y las formas en que se recabará el consentimiento expreso de los titulares para el cabal cumplimiento de la Ley y su Reglamento.

4.5. Estrategia de controles tecnológicos.

Considerando los avances en la tecnología y que actualmente se encuentra al alcance de la mayoría de las personas o empresas que recaban datos personales, los controles tecnológicos mínimos que se deberán implementar para la protección de dichos datos son:

- **Generar el documento de seguridad de datos personales y el procedimiento de actualización.** Para este control es recomendable tomar como base la “Guía para la elaboración de un Documento de Seguridad”, que como ya se mencionó anteriormente, fue elaborada por el IFAI, considerando a la información como un activo que debe protegerse.
- **Procedimiento de acceso y autenticación.** Desde el punto de vista tecnológico, este control es muy importante porque nos permite prevenir el ingreso de personas no autorizadas a nuestras instalaciones pero también a nuestros sistemas, además de ser un mecanismo de seguimiento de las actividades de cada usuario.

- **Procedimiento de almacenamiento de datos.** Este control refiere a la forma en la que se almacena o guarda la información, que como ya fue visto, de acuerdo a la Ley y su Reglamento, puede ser en soportes físicos, electrónicos o ambos.
- **Procedimiento para blindar la base de datos y prevenir posibles fugas de información**. Aquí se deberán establecer todos los candados necesarios para garantizar la integridad, confidencialidad y disponibilidad de los datos personales, evitando su alteración, daño, pérdida, destrucción y uso no autorizado.
- **Procedimiento para la eliminación de datos personales y sensibles**. Se deberá establecer el procedimiento necesario para que los datos personales puedan ser eliminados de la base de datos una vez concluido el uso de los mismos o al ejercer el derecho establecido en la Ley y su Reglamento.
- **Procedimiento de control y difusión de incidentes de seguridad.** Se deberán establecer las funciones y mecanismos para un manejo de incidentes que garantice una respuesta rápida, eficaz y sistemática de los incidentes de seguridad que se presenten y en su caso, la adecuada notificación al titular.
- **Procedimiento para el ejercicio de derechos ARCO.** Independientemente de que este procedimiento debe ser informado mediante el aviso de privacidad, en este control y con apego a la Ley y su Reglamento, se deberán definir los pasos a seguir, los documentos a presentar, ante quien se presentarán y los tiempos de respuesta de la solicitud de derechos ARCO.
- **Procedimiento para el intercambio de información con terceros.** Establecer los mecanismos y las condiciones en las que se podrán llevar a cabo intercambio de información, especificando la sensibilidad de la información.
- **Inventario de sistemas informáticos que tratan datos personales y sensibles.** Se deberá integrar un inventario de sistemas informáticos que tratan datos personales considerando lo establecido en la “Guía para la elaboración de un Documento de Seguridad” del IFAI y cuando menos deberá considerar la unidad administrativa, el nombre, cargo, funciones y obligaciones del responsable del sistema.

4.6. Estrategia de acciones.

Como consecuencia del establecimiento de las estrategias que se han planteado, en este caso las acciones que deberán realizarse son:

- **Designar al responsable físico o área responsable de la protección de datos personales.** Independientemente de que la Ley indica que se debe contar con un departamento de datos personales (aclarando que no es exactamente una obligación porque puede haber empresas pequeñas -pymes o mipymes- que reduzcan las funciones a una misma persona responsable, por ejemplo, el caso de una pizzería pequeña o negocio similar), por una simple cuestión de orden, funcionalidad y determinación de responsabilidad debemos contar con ello, sin embargo, la persona o personas de ese departamento deberán contar con las capacidades técnicas y administrativas, para ello se les deberá proporcionar toda la capacitación necesaria para el adecuado desempeño de dicha función.
- **Desarrollar el aviso de privacidad completo y también la versión simplificada y llevar a cabo la entrega del aviso.** El aviso de privacidad es sumamente importante como se ha comentado a través de todo el documento ya que es la manera en que le vamos a informar al titular de los datos, qué datos, cómo y para qué se utilizará su información. Asimismo, se deberá establecer los mecanismos (desde la entrega física hasta la electrónica) para garantizar que el titular recibirá y/o conocerá el aviso de privacidad, considerando formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.
- **Desarrollar y obtener el aviso de consentimiento y en el caso del consentimiento expreso, llevar a cabo su obtención.** La importancia de este aviso radica en que es el mecanismo por el cual hacemos que el titular tenga conciencia de los datos que proporciona y que los proporciona para fines específicos. Es vital que otorgue el consentimiento según sea el caso, tácito o expreso para el tratamiento de sus datos.
- **Generar el documento de seguridad de datos personales.** Como se ha visto en párrafos anteriores, es indispensable contar con un documento de seguridad

de datos personales porque en este se detallan las prácticas, lineamientos y medidas de seguridad que aplican en la empresa.

- **Procedimiento para que los titulares puedan ejercer sus derechos ARCO.** Se deberá contar con un procedimiento claro y puntual de la manera en que los titulares podrán ejercer su derecho al Acceso, Rectificación, Cancelación y Oposición sobre el tratamiento de sus datos personales. El procedimiento deberá ser claro y estar alineado con los requisitos establecidos en la Ley.
- **Ejecutar el programa de capacitación en materia de protección de datos personales.** La capacitación es un punto coyuntural en el éxito de la metodología y la implantación efectiva de la Ley. Si no se les enseña a los integrantes de una empresa la importancia de la privacidad y de la protección de datos personales, no se logrará la implementación de la Ley. Por ello el programa de capacitación debe ser permanente y procurar el conocimiento, desarrollo de habilidades y estrategias necesarias para la protección de datos personales.
- **Ejecutar el plan permanente de comunicación interna y externa.** La información es el elemento que nos permitirá que todos en la empresa estén al tanto de lo que pasa en relación al tratamiento de los datos personales, su importancia y en su caso las sanciones por el mal manejo de los mismos. Entre más enterados estén los miembros de la organización, mejor aplicarán la Ley. De igual forma, entre más informados estén los titulares de que sus datos están protegidos y manejados conforme a la Ley, serán clientes leales a la empresa.
- **Autorregulación vinculante.** Se debe considerar un mecanismo de gran importancia en materia de protección de datos personales ya que es la forma en que las empresas pueden voluntariamente adoptar una serie de principios, normas y procedimientos establecidos por el IFAI y que tienen por objeto regular el comportamiento de los responsables y encargados respecto del tratamiento de datos personales que realicen, sin embargo, se deberá visualizar como el verdadero compromiso de un “responsable” sobre la protección de los datos personales.

4.7.Estrategia de auditorías y mejora continua.

Lo que no se mide y evalúa, no puede mejorarse, por ello esta estrategia es de vital importancia porque con los resultados de la auditoría, se puede determinar el grado de cumplimiento de la Ley y su Reglamento, la efectividad de las acciones y en su caso, las posibles desviaciones que puedan presentarse.

También es un mecanismo para que los titulares de los datos personales, los directivos, los empleados de la empresa y las autoridades midan el grado de eficiencia y eficacia con que se están protegiendo los datos personales, el cumplimiento de los planes y programas que se establecieron para el cumplimiento de la Ley y se aseguren los mejores procesos para la protección de los datos personales.

Derivado de las auditorías realizadas y como parte de las mejores prácticas se deberán llevar a cabo procesos de mejora continua a través de las acciones correctivas y preventivas que se hayan determinado, así como la adecuada toma de decisiones por parte de la alta dirección.

Para una mayor efectividad, las auditorías deberán ser realizadas por una entidad externa a la empresa, independientemente de las auditorías internas en caso de contar con áreas de contraloría internas.

4.8. Consideraciones y factores críticos de éxito.

Como en cualquier proyecto es importante tener presentes ciertas consideraciones y factores críticos de éxito como los que se enlistan a continuación:

- Poco interés e involucramiento de la alta dirección de la empresa
- Falta de concientización en la importancia en la protección de datos personales
- Falta de capacitación del personal
- Inadecuada asignación de presupuesto

- Falta de seguimiento al plan de implementación
- Utilización de herramientas tecnológicas inadecuadas
- Inadecuado entendimiento y apropiamiento de la Ley y su Reglamento
- Cumplir con los plazos establecidos en la Ley y su Reglamento
- Poca o nula comunicación respecto de los compromisos de la Ley y su Reglamento.

Aunado a lo anterior, se deberá considerar que definitivamente las empresas tendrán que cumplir con la LFPDPPP y su Reglamento, lo que seguramente involucrará, como en otros casos, a las áreas de tecnología de la información y en muchos de éstos, será necesario considerar un presupuesto que no existía para la protección de la información, la seguridad de las bases de datos, la comunicación y todo lo que involucra los procesos cotidianos de operación y del negocio de la propia empresa.

Así es como en este capítulo, se presentó la propuesta de metodología que es la "receta". Utilizando prácticamente los mismos recursos humanos (área legal, recursos humanos, finanzas, administración y tecnología de la información) con los que actualmente cuentan los particulares o empresas y sin sobrecargarse administrativamente ni financieramente, se puede implementar la Ley y dar cumplimiento haciendo uso de las siete estrategias que en este Capítulo se han planteado; involucran un diagnóstico que permite generar un plan de acción con una estrategia de comunicación y capacitación, considerando los procesos y la tecnología de la información como estructura y herramienta para lograr la meta de implementar exitosamente la Ley y su Reglamento en beneficio de los titulares y los responsables.

Conclusiones.

Aún y cuando desde el 2010 está vigente en México la Ley Federal de Protección de Datos Personales en posesión de los Particulares, es muy alta la estadística de empresas y personas que aún al día de hoy, no conocen las obligaciones de la Ley y mucho menos están cumpliendo con los principales requisitos.

Indudablemente derivado de los rápidos avances en la tecnología, cada vez más, es inminente el peligro de que los datos e incluso las identidades sean robados o utilizados indebidamente y sin el respectivo consentimiento, por ello es que la implementación de la LFPDPPP y su Reglamento, es la forma de garantizar a los titulares el control sobre su identidad e información, sobre la forma en que se recaba, el objeto y su fin, así como su transmisión, que como se vio durante el presente trabajo, también se conoce como el derecho a la autodeterminación informativa.

La protección de datos personales es un reto que el Derecho y la tecnología tienen que resolver en forma conjunta, porque es la misma tecnología que protege los datos personales la que los vulnera y la única forma de salvaguardarlos, es implementar adecuadamente la LFPDPPPP y su Reglamento.

Por lo anterior, es vital que ahora que se cuenta con una legislación que protege los datos personales, también se cuente con una metodología de mejores prácticas que facilite la incorporación y cumplimiento de dicha Ley en las empresas.

Con el presente documento se cumple el objetivo de proponer una solución estratégica que coadyuve a través de una metodología a la implementación de la LFPDPPP, para resolver parte de la problemática en el sentido de contar con una herramienta o camino a seguir para implementar adecuadamente la Ley.

Esta metodología fue desarrollada considerando la LFPDPPP y su Reglamento, las mejores prácticas y las experiencias de quienes ya han recorrido el camino de la

implementación de la LFPDPPP, tal es el caso de General Motors de México S de R.L. de C.V., de la Universidad La Salle (ULSA), SCITUM, S.A. de C.V. y Medibast, S.A. de C.V., considerando los aspectos jurídicos, administrativos y tecnológicos para cumplir con eficiencia y eficacia en beneficio de los titulares.

Esta propuesta de metodología, se puede implementar tomando la decisión de nombrar en la empresa a un responsable de llevarla a cabo con la autoridad suficiente a nivel de la alta dirección, utilizando los recursos internos, pero apoyándose, de ser posible, en asesores externos que puedan tener una visión holística y sin prejuicios de lo que se debe hacer.

No debemos olvidar que la privacidad y la protección de datos son derechos irrenunciables e inalienables. En una sociedad donde la información se ha vuelto, tal vez, el activo más valioso, la información personal como los registros médicos, financieros, educativos, entre otros, deberán ser tratados y protegidos de la mejor manera posible. Afortunadamente en México, ya contamos con la LFPDPPP y su Reglamento, por ello las empresas y las instituciones deben entender que el respeto a este derecho es un valor agregado en sus gestiones, porque lo que generará mayor lealtad de sus clientes y por lo tanto no debe ser visto como una obligación más a cumplir, sino como algo positivo para todos los involucrados.

Para cumplir con la efectividad debida, las empresas y las instituciones deben asignar un presupuesto en función de sus características para implementar las medidas de seguridad y protección de datos personales considerando los aspectos tecnológicos, jurídicos y administrativos.

Las empresas deben tener presente que no cumplir con la LFPDPPP y su Reglamento, además de que lesiona uno de los derechos fundamentales de todos los mexicanos, también conlleva consecuencias importantes incluyendo multas sustanciales y

demandas legales que afectarán directamente la imagen, clientela y salud financiera de la empresa.[25]

Como se analizó en diferentes Capítulos de la presente propuesta, la autorregulación vinculante es un elemento adicional a la LFPDPPP y su Reglamento y permite incluir o adherirse a reglas, parámetros o estándares específicos que demuestran un mayor nivel de compromiso de los responsables sobre el tratamiento de los datos personales así como con los titulares de los mismos.

Es importante señalar que el contar con una metodología para la implantación y cumplimiento de la LFPDPPP y su Reglamento tiene grandes beneficios, como:

- Contar con una herramienta general que se adapta a cada empresa (micro, mediana o grande) y que facilita la adopción de la Ley Federal de Protección de Datos Personales y su Reglamento, alineando los aspectos jurídicos, administrativos y tecnológicos.
- El incremento o mantenimiento de la confianza de los clientes.
- La posibilidad de convertir a México en un país referente en la implementación eficiente y eficaz de la Protección de Datos Personales en Latinoamérica.
- Recorrer un camino a través de una guía previamente probada que evitará la pérdida de tiempo, dinero y esfuerzo.
- Contar con experiencias, conocimientos e información para difundir a toda la sociedad a través de diferentes medios.

Finalmente y basándose en todos los argumentos establecidos en la presente propuesta de solución estratégica, queda claro que el mejor camino a seguir para lograr el cumplimiento de la LFPDPPP y su Reglamento es a través de una metodología que indique los pasos a seguir, combinando los requisitos a cumplir, las mejores prácticas y el uso de la tecnología de forma integral, pero que al mismo tiempo, contenga los

[25] Jaramillo Islas Rubí. (2011). *¿Cómo puede una empresa darle cumplimiento a la LFPDPPP?*. Magazcitum. Pp. 8-15. México.

mecanismos necesarios para detectar las desviaciones que se presenten durante la implementación para lograr de manera eficiente y eficaz la protección de los datos personales en posesión de los particulares.

BIBLIOGRAFÍA.

- **Abelson, Hal, Ledden Ken y Harris Lewis**. (2008). Blown to bits. Your life, Liberty and Happines after the digital explosion. Addison-Wesley.
- **Agencia Española de Protección de Datos**. (2005). *Código de protección de datos.* Ed. La Ley. Madrid, España.
- **Carbonell, Miguel. Davara, Isabel. Luna,Issa**. (2010). *Ley de Protección de Datos Personales para el Distrito Federal comentada.* Info-UNAM. (1ª. Ed.). México, D.F. Instituto Federal de Acceso a la Información Pública del Distrito Federal.
- **De Pina Vara, Rafael.** (1988). *Diccionario de D*erecho. (15 ava ed.). Porrúa, Pp. 352. México, D.F.
- **Díaz Rojo, José Antonio**. (2002). *Privacidad, ¿Neologismo o barbarismo?* Revista de Estudios Literarios. No. 21. Universidad Complutense. Madrid, España.
- **Feregino Toris, Erika Gabriela**. (2012). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Aspectos Prácticos*. México, D.F. Editorial ISEF.
- **García González, Aristeo**. (2011). *La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparad.* Boletín Mexicano de Derecho Comparado, UNAM. México, D.F.
- **H. Cámara de Diputados**. (2010). *Protección de Datos Personales: Compendio de Lecturas y Legislación*. Alonso Editores. México, D.F.
- **Instituto Federal de Acceso a la Información Pública (IFAI)**. (2007). *Reforma al Artículo 6º. Constitucional que establece el acceso a la información pública como un derecho fundamental de los mexicanos (3ª ed.)*. México, D.F.
- **Instituto Federal de Acceso a la Información Pública (IFAI)**. (2009). *Guía para la elaboración de un documento de seguridad*. V1.4. México, D.F.
- **Jaramillo Islas, Rubí**. (julio-septiembre 2011). *¿Cómo puede una empresa darle cumplimiento a la LFPDPPP?* Magazcitum, año 2, número 3. Pp. 8-15. México.
- **Peschard Mariscal, Jacqueline**. (2008). *El derecho a la protección de datos personales*. IFAI. México, D.F.

- **Piñar Mañas, José Luis**. (2008).*"¿Existe Privacidad?"*, Lección magistral impartida en la apertura solemne del curso académico en la Universidad San Pablo-CEU de Madrid. Madrid, España. P. 8.
- **Prior Francesc y Santomá Javier**. (2008). *Revisión de Mejores Prácticas en Modelos de Negocio Utilizados en Entidades Financieras*. IESE Business School, Universidad de Navarra. Madrid, España.
- **Project Management Institute**. (2008). *Guía del PMBOK*. (4ª. Edición). Pp. 4-6. Newtown Square, Pennsylvania. USA.
- **Ramírez, Verónica**. (2011). *Compartiendo experiencias en la Implementación de la Ley de Protección de Datos*. General Motors de México, S. de R.L. de C.V.

Internet

- **Asociación Mexicana de Internet (AMIPCI)**. (2012). *Primer Estudio sobre Protección de Datos Personales entre Usuarios y empresas*. Secretaría de Economía y AMIPCI. Recuperado de http://www.amipci.org.mx/?P=editomultimediafile&Multimedia=95&Type=1 (consultada el 21 de junio de 2012).
- **Borghello, Cristian**. (2000-2009). *Seguridad Lógica-Identificación y Autentificación*. Seguridad de la Información (Segu.Info). Recuperado de http://www.segu-info.com.ar/logica/identificacion.htm (consultada el 5 de marzo de 2013).
- **BleinConsulting**. (2012). *Ley federal de Protección de Datos Personales en Posesión de Particulares, Retos operativos y culturales para las empresas*. The Biz. Recuperado de www.bleinconsulting.com (consultada el 5 de marzo de 2013).
- **Claro, Magdalena**. (2010). *La incorporación de tecnologías digitales en educación. Modelos de identificación de buenas prácticas*. CEPAL. Recuperado de http://www.eclac.org/cgi-bin/getProd.asp?xml=/publicaciones/xml/8/40278/P40278.xml&xsl=/dds/tpl/p9f.xsl&base=/dds/tpl/top-bottom.xsl (consultada el 26 de septiembre de 2012).
- **Definición.De**. (2013). *Definición de metodología*. Recuperado de

http://definicion.de/metodologia/#ixzz2PYscvhY5 (consultada el 5 de marzo de 2013).

- **Deloitte**. (2012). *Estudio: Termómetro: Privacidad de datos. Ley Federal de Protección de Datos Personales en Posesión de los Particulares.* Recuperado de http://www.deloitte.com/assets/Dcom-Mexico/Local%20Assets/Documents/mx%28es-mx%29Estudio_LFPDPPP_Feb12.pdf (consultada el 2 de junio de 2013).
- **Evans, Ernesto**. (2012). *Desafíos en la protección de datos, ¿Qué pasa con los datos que almacenan las clínicas o en las bases de datos de los operadores de telefonía, o del gobierno?* La Tercera. Recuperado de http://www.latercera.com/noticia/opinion/ideas-y-debates/2012/02/895-429238-9-desafios-en-la-proteccion-de-datos.shtml (consultada el 26 de septiembre de 2012).
- **García, P**. (2013). *La importancia de la protección de datos personales*. Educa Transparencia. Santiago, Chile. Recuperado de http://www.educatransparencia.cl/portal/novedad/la-importancia-de-la-proteccion-de-los-datos-personales. (consultada el 2 de junio de 2013).
- **Gómez Cruz, Martha E**. (2012). *En México, la cultura de privacidad y protección de datos personales es escasa*. Addictware. Recuperado dehttp://www.addictware.com.mx/index.php/ti-en-numeros/2400-privacidad-proteccion-datos-deloitte (consultada el 20 de julio de 2012).
- **International Organization for Standardization (ISO).** *Norma ISO9001:2008. Recuperado de* http://www.iso.org/iso/home/standards/management-standards/iso_9000.htm (consultada el 20 de octubre de 2013).
- **La Historia con mapas**. (2011). *Las Leyes de Protección de Datos en el Mundo*. BlogSpot. Recuperado de http://lahistoriaconmapas.blogspot.com/2011/01/las-leyes-de-proteccion-de-datos-en-el.html (consultada el 20 de julio de 2012).
- **Méndez Olivares, Héctor**. (2012). *Llegó el día D para la aplicación de la LFPDPPP*. Computer World México. México, D.F. Recuperado de http://www.computerworldmexico.mx/Articulos/24732.htm (consultada el 27 de agosto de 2012).

- **Organización de Naciones Unidas (ONU)**. (1948). *"Declaración Universal de Derechos Humanos"*. Artículo 12. París. Recuperado de http://www.un.org/spanish/aboutun/hrights.htm (consultada el 5 de marzo de 2013).
- **Organización Panamericana de la Salud (OPS)**. *Concepto de Buenas Prácticas en la Salud*. Recuperado de http://www.ops.org.bo/textocompleto/prensa/concurso-buenas-practicas/conceptos.pdf (consultada el 9 de agosto de 2012).
- **Proyecto de Implantación Ley Protección de Datos.** (2012). *Información-Documentación*. Recuperado de http://www.pc-express-solutions.com/lopd/dossier_lopd_pcexpress.pdf (consultada el 20 de julio de 2012).
- **Real Academia de la Lengua Española**. *Definición de metodología*. Recuperado de http://lema.rae.es/drae/ (consultada el 5 de marzo de 2013).
- **Reyes Krafft, Alfredo Alejandro**. (2011). *b: Secure Conference.* NetMedia Publishing. Recuperado de http://www.mattica.com/2011/03/bsecure-conference-2011-inicia-esta-semana (consultada el 20 de julio de 2012).

Legislación

- **Constitución Política de los Estados Unidos Mexicanos**. Últimas reformas publicadas. *Diario Oficial de la Federación*. 20 julio 2007. México.
- **Constitución Política de los Estados Unidos Mexicanos**. Reforma al Artículo 6º de la Constitución Política de los Estados Unidos Mexicanos*. Diario Oficial de la Federación*. 6 de marzo de 2007. México.
- **Constitución Política de los Estados Unidos Mexicanos**. Reforma al Artículo 16 de la Constitución Política de los Estados Unidos Mexicanos*. Diario Oficial de la Federación*.1º. de junio de 2009. México.
- **Constitución Política de los Estados Unidos Mexicanos**. Reforma al Artículo 73, fracción XXIX-O de la Constitución Política de los Estados Unidos Mexicanos. *Diario Oficial de la Federación*. 30 de abril de 2009. México.
- **Convención Americana sobre Derechos Humanos (Pacto de San José).**

(1969). Suscrita en la conferencia especializada interamericana sobre derechos humanos (B-32). *Artículo 11, apartado 2*. San José, Costa Rica, 7 al 22 de noviembre de 1969.

- **Consejo de Europa**. (1981). *Convenio 108, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.* Estrasburgo. *Diario Oficial de las Comunidades Europeas (DOCE).*
- **Instituto Federal de Acceso a la Información Pública (IFAI)**. (2007). *Reforma al Artículo 6º. Constitucional*. México.
- **Ley Federal de Protección de Datos Personales en Posesión de los Particulares**. *Diario Oficial de la Federación*. Publicada el 5 de julio de 2010 y entró en vigor el 6 de julio de 2010.
- **Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental**. *Diario Oficial de la Federación*. Publicada el 11 de junio de 2002 y entró en vigor el 12 de junio de 2002. Última reforma publicada el 8 de junio de 2012.
- **Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, El Honor y la Propia Imagen en el Distrito Federal**. *Gaceta Oficial del Distrito Federal.* Publicado el 19 de mayo de 2006 y entró en vigor el 20 de mayo de 2006.
- **Organización de Naciones Unidas (ONU)**. Oficina del Alto Comisionado para los Derechos Humanos. (1966). *Pacto Internacional de Derechos Civiles y Políticos*. Resolución 2200 A (XXI) de la Asamblea General, aprobada el 16 de diciembre de 1966.
- **Parlamento Europeo y del Consejo**. (1995). Directiva 95/46/CE, *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*. Luxemburgo. *Diario Oficial de las Comunidades Europeas (DOCE).*
- **Parlamento Europeo y del Consejo**. (2002). Directiva 2002/58/CE*, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)*. 12 de julio de 2002. Bruselas. *Diario Oficial de las*

Comunidades Europeas (DOCE).

- **Parámetros para el correcto desarrollo de los esquemas de autorregulación vinculante a que se refiere el Artículo 44 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares**. *Diario Oficial de la Federación.* México, D.F. 17 enero 2013.
- **Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares**. *Diario Oficial de la Federación*. Publicado el 21 de diciembre de 2011 y entró en vigor el 22 de diciembre de 2011.
- **Unión Europea**. (1950). *Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales*. *Artículo 8. Derecho al respeto a la vida privada y familiar.* Roma, Italia. *Diario Oficial de las Comunidades Europeas (DOCE).*