AUREN

Estudio de Cultura sobre Tratamiento de Datos Personales en el Sector de las Tecnologías de Información

CANIETI
www.canieti.org

SE
SECRETARÍA DE ECONOMÍA

PROSOFT 2.0

Contenido

Introducción

Hoy en día la información es poder y en los últimos años se han creado numerosas empresas especializadas en la recopilación de todo tipo de datos personales; en su gran mayoría para fines comerciales, un ejemplo de ello son los navegadores y las redes sociales. Toda la información recopilada es cuidadosamente archivada, a la espera de que entre a formar parte activa de las numerosas bases de datos que controlan hasta el más insignificante dato. Lo preocupante de la situación es la inseguridad que manejan estas empresas las cuales se encargan de administrar o sustraer estos datos poniendo en peligro la integridad de las personas.

El periodista y escritor norteamericano Stephen Baker, a través de su libro *Numerati,* expone que un grupo de mafia cibernética de la que nadie puede escapar, se dedican a rastrear toda la información que dejamos plasmada a través de Internet, móviles, tarjetas de crédito, etc.; manipulando nuestra conducta sin que nos demos cuenta. Cada vez que accedemos a Internet, cada llamada telefónica, cada mensaje de móvil o cada compra con tarjeta de crédito, envía información a una base de datos, donde es analizada y procesada por los Numerati.

Este libro está fundamentado en datos verídicos, basados en situaciones de la vida diaria, peligros que se corren y de los cuales no nos damos cuenta. Un ejemplo es el uso de tarjetas de puntos de las tiendas comerciales; para adquirir dichas tarjetas, los clientes deben proporcionar sus datos personales a la empresa, y cada vez que el cliente compra un producto de la tienda y presenta su tarjeta, se genera una cierta cantidad de puntos, los cuales después se podrán canjear por otros artículos, parece ser un gran beneficio, pero estas tarjetas están alimentando una base de datos acerca de las compras que realiza su cliente, por semana, mes o por año. Estos se vuelven una información muy valiosa para las empresas, ya que la tienda comercial puede usar la información para saber que vender a sus clientes o puede vender la información a otras empresas. Así mismo los datos recabados sin el consentimiento del Titular pueden ser usados para actos ilícitos poniendo en peligro la integridad de las personas, por ejemplo el robo de identidad o fraude.

Lo anterior mantiene en alerta a distintas organizaciones y países por lo que han expedido leyes que protejan al usuario sobre la comisión de estos delitos.

Contexto y oportunidad

Las empresas Mexicanas, están sujetas a la actual legislación sobre privacidad y protección de datos. Así, están obligados a garantizar el derecho a la información de los ciudadanos cuando se obtienen sus datos personales; a asegurar los requisitos de calidad de la información, incluyendo la obtención de los datos adecuados y no excesivos para las finalidades legítimas para las que se van a utilizar; la actualización de los mismos; las garantías especiales para los datos más sensibles como los de ideología, vida sexual o salud; las obligaciones en materia de seguridad de los datos y la confidencialidad en el Tratamiento de los datos personales.

Del mismo modo, los ciudadanos tienen una serie de derechos que pueden ejercer para controlar el uso de sus datos de carácter personal y, específicamente, el de acceder y conocer la información que sobre ellos tienen los Responsables de Tratamientos y rectificar y cancelar la información inexacta, incompleta, inadecuada o excesiva que obre en poder de dichos Responsables

Antecedentes sobre el tema de la ley de privacidad

La privacidad es un derecho humano básico. Esta sirve de fundamento a la dignidad y a otros valores tales como la libertad de asociación y la libertad de expresión. La privacidad se ha vuelto uno de los derechos humanos contemporáneos más importantes.

La privacidad es reconocida alrededor del mundo en distintas regiones y culturas. Está protegida en la Declaración Universal de Derechos Humanos, en el Pacto Internacional de Derechos Civiles y Políticos, y en muchos otros tratados internacionales y regionales de Derechos Humanos. Prácticamente todos los países en el mundo incluyen el derecho a la privacidad en su Constitución. Como mínimo, estas disposiciones incluyen los derechos de inviolabilidad del domicilio y el secreto de las comunicaciones.

Recientemente las constituciones del mundo incluyen derechos específicos para acceder y controlar la propia información personal.

Facetas de la Privacidad

La privacidad puede ser dividida en los siguientes conceptos separados pero relacionados:

1. Privacidad de la Información, la cual incluye el establecimiento de reglas que gobiernen la recolección y manejo de datos personales tales como información crediticia, y registros médicos y gubernamentales. Esta también se conoce como "protección de datos".

2. Privacidad corporal, la cual se refiere a la protección del ser físico de las personas ante procedimientos invasivos tales como pruebas genéticas, pruebas de drogas y registro de cavidades.

3. Privacidad de las comunicaciones, la cual se refiere a la seguridad y privacidad del correo, las llamadas telefónicas, los correos electrónicos y otras formas de comunicación.

4. Privacidad territorial, que se refiere a la fijación de límites a la intromisión en los medios domésticos y otros tales como el centro laboral o el espacio público. Este incluye los allanamientos, el video vigilancia y el control de identificación.

Antecedentes normativos internacionales

Como antecedentes normativos Internacionales se enuncian los siguientes:

En 1970 Alemania aprueba la primera Ley de protección de datos (Datenschutz)[1]

En Suecia, en 1973, entro en vigor la primera ley en el mundo para la protección de la información de particulares. Le sucede Estados Unidos en 1974 con una ley de carácter general (*PrivacyAct*), luego, entre 1977 y 1979, países como Canadá, Francia, Dinamarca, Noruega, Austria y Luxemburgo publicaron leyes de protección de datos. Es hasta el 28 de enero de 1981 que se realiza el primer convenio internacional de protección de datos, firmado por países miembros del Consejo Europeo, mejor conocido como “Convenio 108” o “Convenio de Estrasburgo”. De este modo la República Federal Alemana, Francia, Dinamarca, Austria y Luxemburgo contaron con el primer instrumento vinculatorio de carácter

[1] Gabriel Sánchez Pérez, “Ley de protección de datos Personales en el mundo y la protección de datos biométricos Parte I” , en la página: http://revista.seguridad.unam.mx/numero-13/leyes-de-protecci%C3%B3n-de-datos-personales-en-el-mundo-y-la-protecci%C3%B3n-de-datos-biom%C3%A9tricos-%E2%80%93, (5/03/12)

internacional sobre protección de datos, al cual se le sumaron en un lapso de 11 años países como Islandia, Gran Bretaña, Irlanda, Holanda, Portugal, España y Bélgica.

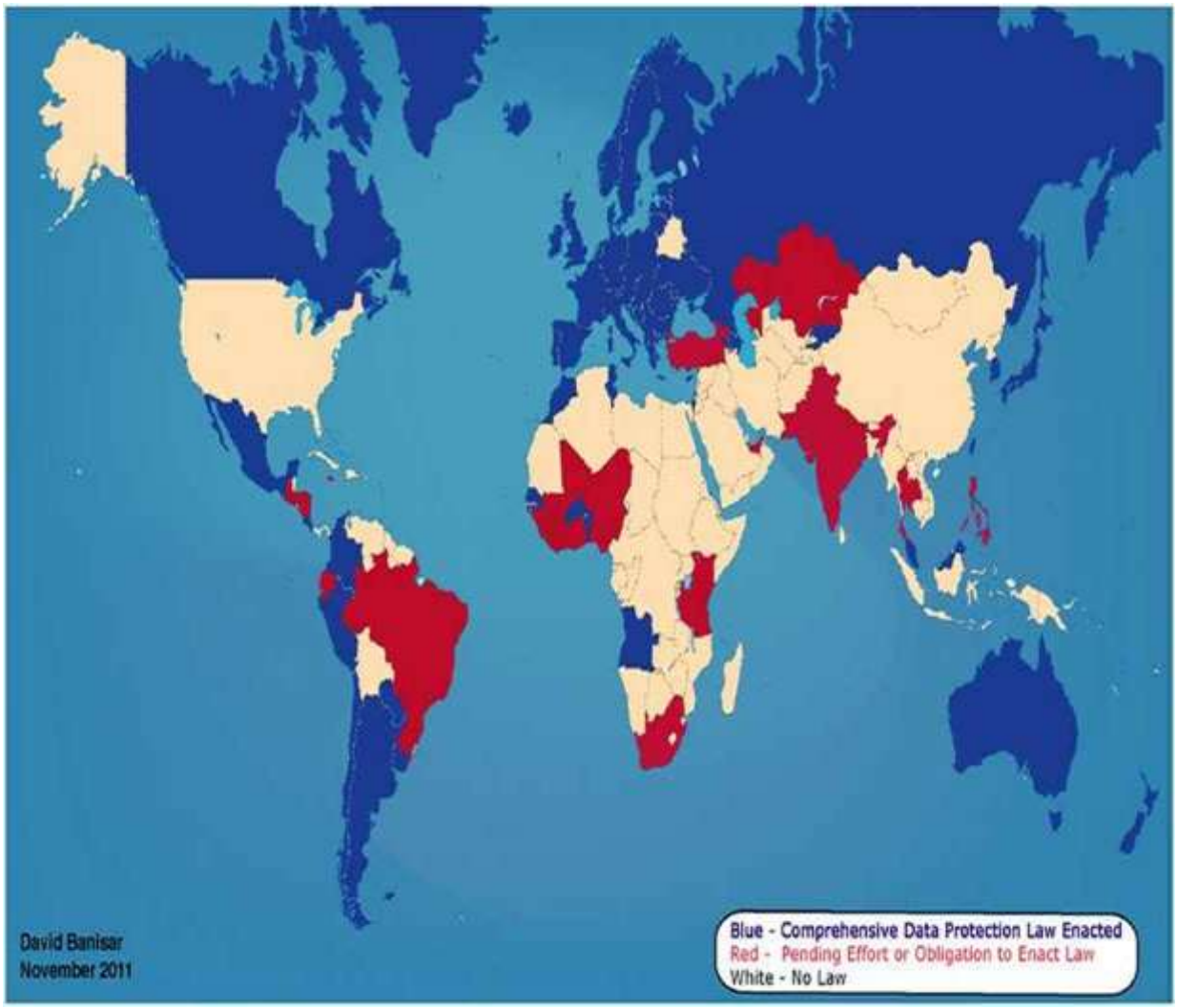
Hoy en día se habla de dos marcos normativos en el mundo: el modelo europeo y el modelo americano este último, que sólo siguen Estados Unidos y Canadá (cuadro 1).

Modelo Europeo (protección de datos)	Modelo Americano (privacidad)
Enfoque preventivo	Todo se resuelve en las cortes
Socialmente orientado	Enfoque individual
Confianza en el gobierno (cohesión y salvaguardias)	Confianza en el mercado (enfoque de negocios)
Los datos se recaban cuando es necesario	Los datos se recaban cuando es conveniente
Los derechos y las excepciones se prevén en Ley	Los alcances jurídicos se resuelven caso por caso en las cortes
Existen autoridades especializadas e independientes	No existen autoridades concretas, sino algunas sectoriales
Se protege a todo individuo que esté en territorio europeo	No se protege a ciudadanos no estadounidenses

Cuadro 1. Comparativo de modelos de marcos legislativos de Ley de Protección de Datos

Es hasta 1997 cuando un país latinoamericano, Brasil, promulga una Ley de Protección de Datos. Le siguió Argentina en el año 2000[2]"

[2] Antonio Oliveros Dávila , "Ley Federal de Protección de Datos Personales en Posesión de Particulares ", en la página: http://www.magazcitum.com.mx/?p=1169, (20/03/12)



David Banisar publicó un mapa con las leyes de protección de datos personales aplicadas en el mundo. La clasificación de Banisar parece evaluar únicamente el modelo europeo de protección de datos personales, ya que no incluye a los Estados Unidos como parte de los países con legislación sobre protección de datos personales.[3]

[3]Gabriel Sánchez Pérez, "Ley de protección de datos Personales en el mundo y la protección de datos biométricos Parte I", en la página http://revista.seguridad.unam.mx/numero-13/leyes-de-protecci%C3%B3n-de-datos-personales-en-el-mundo-y-la-protecci%C3%B3n-de-datos-biom%C3%A9tricos-%E2%80%93, (5/03/12)

OCDE (Organización para la cooperación y el desarrollo económico).

"En 1980 en el marco de la **Organización para la Cooperación y el Desarrollo Económico -OCDE-** se emitió una recomendación que contiene las "Directrices relativas a la protección de la privacidad y flujos transfronterizos de datos personales", que constituyó el primer instrumento supranacional que analiza a profundidad el derecho a la protección de datos. Su adopción se funda en la comprobación por parte del Consejo de la OCDE de la inexistencia de una regulación uniforme en esta materia en los distintos Estados miembros, lo cual dificultaba el flujo de los datos personales entre ellos mismos.

La OCDE fue fundada en 1960, cuando 18 países europeos, Estados Unidos y Canadá han unido sus fuerzas para fundar una organización dedicada al desarrollo global. Hoy, la OCDE tiene 34 países miembros en todo el mundo, desde América del Norte y América del Sur a Europa, a través de la región Asia-Pacífico. Estos incluyen muchos de los países más avanzados, sino también las economías emergentes como México, Chile y Turquía. Su sede central se encuentra en el Château de la Muette, en la ciudad de París (Francia).

En la OCDE, los representantes de los países miembros se reúnen para intercambiar información y armonizar políticas con el objetivo de maximizar su crecimiento económico y colaborar a su desarrollo y al de los países no miembros.

Los países miembros de hoy en la OCDE.-

1. Allemagne Alemania
2. Australie Australia
3. Autriche Austria
4. Belgique Bélgica
5. Canada Canadá
6. Chili Chile
7. Corée Corea
8. Danemark Dinamarca
9. Espagne España
10. Estonie Estonia
11. Etats-Unis Estados Unidos
12. Finlande Finlandia
13. France Francia
14. Grèce Grecia
15. Hongrie Hungría
16. Irlande Irlanda
17. Islande Islandia
18. Israël Israel
19. Italie Italia
20. Japon Japón
21. Luxembourg Luxemburgo
22. Mexique México
23. Norvège Noruega
24. Nouvelle-Zélande Nueva Zelanda
25. Pays-Bas Países Bajos
26. Pologne Polonia
27. Portugal Portugal
28. Républiqueslovaque La República Eslovaca
29. Républiquetchèque La República Checa
30. Royaume-Uni Reino Unido
31. Slovénie Eslovenia
32. Suède Ante
33. Suisse Suiza
34. Turquie Turquía

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) decidió elaborar en 1980 unas líneas directrices sobre política internacional de protección de la privacidad y los flujos transfronterizos de datos personales.

Las directrices sobre protección de la privacidad y flujos transfronterizos de datos personales ("directrices de privacidad") fueron adoptadas como una recomendación del Consejo de la OCDE apoyando los tres principios que aglutinan a los países de la OCDE: democracia pluralista, respeto de los derechos humanos y economías de mercado abiertas. Se hicieron efectivas el 23 de septiembre de 1980.

Los principios establecidos en las directrices de privacidad se caracterizan por su claridad y flexibilidad de aplicación, y por su formulación, que es lo suficientemente general para permitir su adaptación a los cambios tecnológicos. Los principios abarcan todos los medios del procesamiento informático de datos sobre individuos (desde computadoras locales a redes con complejas ramificaciones nacionales e internacionales), todos los tipos de procesamiento de datos personales (desde la administración de personal hasta la compilación de perfiles de consumidores) y todas las categorías de datos (desde datos de tráfico hasta datos de contenidos, desde el más trivial al más delicado). Los principios se pueden aplicar en los ámbitos nacional e internacional.

El 11 de abril de 1985 los ministros de la OCDE adoptaron la Declaración sobre flujos de datos Transfronterizos.

En la conferencia ministerial de la OCDE "Un mundo sin fronteras" celebrada en 1998 en Ottawa, los ministros reafirmaron su compromiso sobre la protección de la privacidad de la redes globales para garantizar el respeto de importantes derechos, generar confianza en las redes globales y evitar restricciones innecesarias en los flujos transfronterizos de datos personales.

En el ámbito del derecho internacional, el derecho a los datos personales se encuentra legislado en directivas en la Unión Europea. La principal es **la Directiva 95/46/CE del Parlamento Europeo y del Consejo**, del 24 de octubre de 1995 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, como su nombre oficial lo indica.[4]

[4]Issa Luna Pla, " La Protección de datos personales en el Distrito Federal" En la Biblioteca Jurídica virtual de la UNAM, en la páginahttp://www.juridicas.unam.mx/publica/rev/decoin/cont/15/cmt/cmt5.htm, (16/03/12)

Organización de las Naciones Unidas (ONU)

La Organización de las Naciones Unidas emitió en 1990 la Resolución 45/95 que contiene una lista básica de principios para la protección de datos personales de aplicación mundial, como el de exactitud de los mismos, la determinación de su finalidad, su acceso y la no discriminación."[5]

Directrices para la regulación de los archivos de datos personales informatizados.

Adoptadas mediante resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990 Los procedimientos para llevar a la práctica las normas relativas a los archivos de datos personales informatizados se dejan a la iniciativa de cada Estado, con sujeción a las siguientes orientaciones:

A. Principios Relativos a las Garantías Mínimas que deben Prever las Legislaciones Nacionales

1. Principio de legalidad y lealtad
2. Principio de exactitud
3. Principio de especificación de la finalidad
4. Principio de acceso de la persona interesada
5. Principio de no discriminación
6. Facultad para hacer excepciones
7. Principio de seguridad
8. Supervisión y sanciones
9. Flujo transfronterizo de datos
10. Campo de aplicación

Los presentes principios deben hacerse aplicables, en primer lugar, a todos los archivos informatizados públicos y privados, así como, mediante extensión optativa y sujeta a los ajustes correspondientes, a los archivos manuales. Pueden dictarse disposiciones especiales, también optativas, para hacer aplicable la

[5]Instituto Federal de Acceso a la Información Pública. "La Protección de Datos personales en México : Una propuesta para deliberar", en la página http://ieaip.org.mx/biblioteca_virtual/datos_personales/5.pdf , (16/03/12), Última actualización: junio del 2008

totalidad o parte de los principios a los archivos relativos a personas jurídicas, especialmente cuando contengan alguna información relativa a individuos.

B. Aplicación de las Directrices a archivos de datos personales mantenidos por Organizaciones Internacionales

Gubernamentales

Las presentes directrices serán de aplicación a los archivos de datos personales que mantengan las organizaciones internacionales gubernamentales, sujetas a cualquier ajuste que sea preciso para tener en cuenta cualquier diferencia que pueda existir entre archivos para fines internos, como aquellos que conciernen a la gestión de personal, y archivos para fines externos, relativos a terceros que tengan relaciones con la organización.

Cada organización debe designar a la autoridad legalmente competente para supervisar la observancia de estas directrices.

Cláusula humanitaria

Puede preverse específicamente una excepción a estos principios cuando la finalidad del archivo sea la protección de los derechos humanos y las libertades fundamentales de la persona afectada, o la ayuda humanitaria. Debe preverse una excepción similar en la legislación nacional para las organizaciones internacionales gubernamentales cuyo acuerdo organizativo no impida la puesta en práctica de la referida legislación nacional, así como para las organizaciones internacionales no gubernamentales a las que sea aplicable esta ley.

APEC (Foro de Cooperación Económica Asia-Pacífico)

Igualmente, en el **Foro de Cooperación Economía Asia Pacífico -APEC-**, en 1999, se estableció un Grupo de Manejo del Comercio Electrónico que tiene dentro de sus principales actividades el desarrollo de legislaciones y políticas compatibles entre las economías participantes en el campo de la privacidad. Por ello, APEC ha emitido lineamientos generales en la materia, con el fin de que éstos se establezcan en los cuerpos legales correspondientes para lograr un flujo de datos seguro, pero al mismo tiempo, sin obstáculos para fomentar el comercio.

El Foro de Cooperación Económica Asia-Pacífico fue Creado en 1989; Es un mecanismo de cooperación y concertación económica orientado hacia la promoción y facilitación de:

- Comercio
- Inversiones
- Cooperación económica y técnica
- Desarrollo económico regional.

Este foro cuenta con 21 Miembros:

1. Australia
2. Brunei
3. Canadá
4. Chile
5. Corea del Sur
6. Estados Unidos
7. Filipinas
8. Hong Kong
9. Indonesia
10. Japón
11. Malasia
12. México (1993)
13. Nueva Zelanda
14. Papúa Nueva Guinea
15. Perú
16. República de China (Taipéi)
17. República Popular China
18. Rusia
19. Singapur
20. Tailandia
21. Vietnam
22. Secretaría General con sede en Singapur.

Marco de privacidad de APEC

Fue desarrollado y aprobado en 2004 y toma en cuenta:

- Los Principios de Protección de la Privacidad y el Flujo Transfronterizo de Datos (OCDE, 1980)
- La Directiva Europea 95/46/CE.

Permite la transferencia regional de datos en beneficio de consumidores, empresas y gobiernos.

Sus objetivos son:

- Impulsar la apropiada protección de la información personal.
- Prevenir la creación de barreras innecesarias al flujo de información
- Promover que empresas multinacionales utilicen métodos uniformes para recabar y procesar datos personales
- Facilitar esfuerzos nacionales e internacionales para exigir la protección de datos personales.

Principios de protección

- Prevención de daños: Evitar el mal uso de datos;
- Aviso: Informar al Titular sobre las políticas de manejo de datos; Límites a la recolección: Los datos se recaban por medios legales y justos con el consentimiento del individuo;
- Uso de información personal: Los datos recabados deben usarse para cumplir el propósito de la recolección;
- Elección: Brindarle al Titular la opción de decidir en torno a la recolección, uso y transferencia de los datos
- Integridad de la información personal: la información debe ser exacta, completa y actualizada;
- Medidas de seguridad: Apropiadas para evitar riesgos.
- Acceso y Corrección: Que existan mecanismos que le garanticen al Titular los derechos de acceso y corrección;

- Responsabilidad: Medidas para que el Responsable actué con diligencia en el manejo de datos.

Los principios están diseñados para que cada economía participante pueda implementarlos según su cultura de privacidad y sistema legal.

Grupo Rector de Comercio Electrónico (ECSG)

Fue creado en 1999 como misión especial de los Oficiales de Alto Rango, coordina actividades de promoción del comercio electrónico a través de regulaciones y políticas claras, transparentes y consistentes.

Las actividades actuales del grupo incluyen:

- El Subgrupo de Privacidad de Datos y;
- El Subgrupo de Comercio sin Papel.
- Dentro de APEC se ha impulsado la iniciativa denominada Cross BorderPrivacy Rules System con el propósito de facilita la implementación del Marco de Privacidad de APEC.
- Las economías participantes se comprometieron a desarrollar de manera conjunta un sistema práctico enfocado a implementar y verificar el cumplimiento efectivo del marco de privacidad de APEC.

Países que cuentan con Ley de Privacidad (Solo se mencionan algunos)

Estados Unidos

“Estados Unidos, cuentan con un marco jurídico amplio en materia de privacidad, dado que su ley de Privacidad data desde 1974 “PrivacyAct” cuyo objeto es regular la obtención y el uso de la información personal dentro del sector público, mismo que adopta una política de autorregulación que se encuentra a cargo en gran medida del sector privado, respondiendo satisfactoriamente a las demandas y necesidades de sus grandes corporaciones y protegiendo en la medida de lo posible los derechos básicos de los consumidores y de los ciudadanos con base en la primera enmienda de la Constitución de los Estados Unidos de América del Norte.

Podemos decir que los Estados Unidos han adoptado una política más flexible sobre privacidad y protección de datos que la Unión Europea, cuyo objetivo es

proteger y tutelar los derechos de consumidores, la población vulnerable y más aún que se caracteriza por la adopción de un esquema más liberal para el sector empresarial." [6]

Cabe mencionar que en la Unión Americana hay Estados que cuentan con su propia ley en relación a temas de privacidad.

Canadá

"En Canadá se originó la primer Ley formal en 1977, y en 1982 la Carta Canadiense de Derechos y Libertades indica que toda persona tiene derecho a la vida, libertad y seguridad y el derecho a estar libre de búsqueda irrazonable o incautación"[7].

La Ley de Privacidad, aprobada en 1983 por el Parlamento de Canadá, regula cómo las instituciones del gobierno federal obtienen, utilizan y revelan su información personal.

"En enero de 2012, la Corte de Apelaciones de Ontario declaró que la ley común en Canadá reconoce el derecho a la intimidad personal, más específicamente identificado como un "delito de intromisión en la intimidad" así como teniendo en cuenta que la apropiación de la personalidad ya es reconocido como un agravio en la Ley de Ontario".[8]

En Canadá la máxima autoridad de protección de los datos personales es el Comisionado de Privacidad que administra dos piezas legislativas para la protección de datos personales, en materia de ficheros públicos regulados por la "PrivacyAct" y para los ficheros privados.

Canadá cuenta con un Comisionado de Información, el cual tiene como función garantizar el pleno ejercicio del derecho de acceso a la información pública gubernamental.

La ventaja de este modelo es que existe una sola autoridad en materia de protección de datos, que se encarga de garantizar el adecuado Tratamiento de los mismos en posesión de los entes públicos y privados, además de ser una autoridad con autonomía técnica, presupuestaria y de gestión.

[6] Cristos Velasco San Martín, "Boletín de política informática 2001: Artículo de Privacidad y protección de datos personales en Internet ¿Es necesario contar con una regulación específica en México?", páginas 4,5.
[7] Canadian privacy law, http://es.wikipedia.org/wiki, (18/06/12).
[8] Agencia de Protección de Datos, "Estructuras orgánicas y funciones", por Ornelas, Lina, página 8.

Las desventajas residen en que al ser una autoridad unipersonal y no un órgano colegiado, no se cuenta con pluralidad en la toma de decisiones en torno al cumplimiento de las leyes en la materia.

Asimismo, al existir dos autoridades, una encargada del acceso a la información y otra de la protección de datos personales, en los casos en que entran en pugna ambos derechos fundamentales, a pesar de que se han creado mecanismos de consulta y comunicación entre ambas autoridades, ello retrasa la resolución de los asuntos alargando una respuesta expedita al ciudadano además de la negociación que se da para imponer uno u otro criterio.

España

"La Constitución de Españaen su artículo 20 establece los derechos de expresión, producción y creación artística, la libertad de cátedra y el derecho a la información. Motivo por el cual se crea la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos Personales (LORTAD) de 1992 que, en correspondencia con la Ley Reglamentaria en su artículo 18.4 de la Constitución, establece la garantía del derecho al honor y la intimidad personal y familiar, constituyendo el régimen de protección jurídica de los datos personales. España sigue la doctrina francesa liberal y sus antecedentes históricos sobre la protección de los derechos de la personalidad. Francia cuenta con la Ley del 10 de febrero de 1987, que fue modificada el 8 de junio de 1993, la cual establece laprotección de datos personales y crea la Comisión Nacional de Informática y de Libertades"[9]

La Ley Orgánica de Protección de Datos (LOPD) Española de 1999, ha sido utilizada como firme referente del modelo europeo en materia de protección de datos, por países Latinoamericanos.

Brasil

[La Constitución Brasileña de 1987, incorporó en su texto el derecho y garantía constitucional de *Habeas Data,* el cual inicialmente sólo se atribuía al derecho que tenía toda persona para acceder a la información que le concernía, al considerarse "una modalidad de acción exhibitoria análoga a la del habeas corpus".

[9]Issa Luna Pla , " La Protección de datos personales en el Distrito Federal" En la Biblioteca Jurídica virtual de la UNAM, en la página http://www.juridicas.unam.mx/publica/rev/decoin/cont/15/cmt/cmt5.htm, (18/06/12)

Sin embargo, con el paso del tiempo, la estructuración y ampliación del contenido de aquél derecho ha extendido estas facultades primeras a otras más, tales como los de actualización (o la puesta al día -el"up date"anglosajón- de los datos), la rectificación y la cancelación de los datos personales que le conciernen a una persona, sí los datos fueren inexactos, incompletos o ilegales.

El ciudadano brasileño, con base en el texto constitucional, puede válidamente tener derecho no sólo al simple acceso a la información o datos personales que le concierne, cualquiera sea el soporte en el que se encuentre (documento escrito, fílmico, audio-visual, de sonido, o la mezcla de los anteriores: documento electrónico y/o informático o telemático), sea público o privado sino también a poder solicitar su revisión, actualización, rectificación, bloqueo o cancelación de la información si estos datos no se ajustarán a los suministrados personalmente o hayan sido recolectados oficiosamente por el Estado, con autorización expresa y escrita del Titular.

Con base a lo anterior el congreso expidió la Ley 9507 del 12 de noviembre de 1997 que reguló el "derecho de acceso a informaciones" y el "rito procesal del Habeas Data"].[10]

Argentina

En el documento La Visión Constitucional del Habeas Data, Por D. Libardo Orlando Riascos Gómez en el Capítulo Primero "El Habeas Data en las Constituciones Latinoamericanas", Apartado 1.-"Constitucion de la República Argentina", nos muestra un resumen de como entro en vigor la Ley 25326 y su Reglamento 1558 que a continuación se cita:

"En la Constitución de la República de Argentina de 1994, en el inciso 1º y 3º del artículo 43, se regula la "acción" de Habeas Data de la siguiente forma:

> *Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por la Constitución, un tratado o*

[10] Riascos Gómez, Libardo Orlando, "La Visión Constitucional del Habeas Data, Capitulo Primero -El Habeas Data en las Constituciones Latinoamericanas-, -Constitución del Estado Federativo del Brasil-" en la página http://www.informatica-juridica.com/trabajos/La_vision_constitucional_del_habeas_data.asp, (16/06/12)

una Ley. En el caso, el juez podrá declarar la inconstitucionalidad de la norma en que se funde el acto u omisión lesiva.

Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística.

La Constitución Federal Argentina reguló normativamente en el artículo 43 la acción de amparo, como un mecanismo jurisdiccional especial y de trámite expedito para la defensa y garantías de los derechos y libertades de la persona humana, reconocidos en la Constitución, en las leyes e incluso en los tratados públicos reconocidos por el Estado Argentino, siempre y cuando se deba a una acción u omisión de autoridades públicas o de carácter particular "que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta".

El inciso 3º del artículo 43, regula la acción de amparo con fines y objetivos específicos, los cuales apuntan en principio, a proteger los datos o informaciones personales que consten en registros o bancos de datos públicos o privados y siempre que éstos o aquellas sirvan para "proveer informes"; y a posteriori, "y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos".

A raíz de la inclusión del inciso 3º en el artículo 43 y la amplitud de interpretación y alcance que la Corte Suprema de Justicia de la Nación le había prodigado a dicha parte de la norma constitucional desde 1994. En efecto, el Congreso Nacional en el año 2000 "dictó una ley de protección de datos de carácter personal (25326) que incluye entre sus disposiciones un sector en el que se reglamenta la acción de hábeas data que se ventilan ante la justicia federal".

Con base a lo mostrado en el documento de La Visión Constitucional del Habeas Data,se resumen a lo siguiente la Ley de Protección de Datos de Carácter Personal (Ley 25326) entro en vigor en el 2000 y su Reglamento (1558) entro en vigor el 3 de diciembre del 2001, esta ley surge en base a las modificaciones que se hicieron en la constitución en donde se regulo el Inciso 1 y 3 del Artículo 43.

Uruguay

"El 11 de agosto de 2008 se aprueba en Uruguay la Ley N° 18.331 sobre Protección de Datos Personales y Acción de Habeas Data. Es una avanzada legislación que indica que "el derecho a la protección de datos personales es inherente a la persona humana". La Unidad Reguladora y de Control de Datos Personales (URCDP) fue creada por el artículo 31 de la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data como un órgano desconcentrado de la AGESIC ("Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento", de Uruguay).

Establecido por la Ley Nº 18.331, la protección de datos personales aplicara tanto al sector púbico como al privado como a continuación se cita:

Ley de Protección de Datos Personales y Acción de "Habeas Data"

Artículo 3º. Ámbito objetivo.- El régimen de la presente ley será de aplicación a los datos personales registrados en cualquier soporte que los haga susceptibles de Tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado."[11]

Perú

[La Ley de Protección de Datos Personales peruana fue publicada el 3 de julio del 2011.

La Constitución Política del Estado, vigente desde 1993, estableció en el inciso VI del Artículo 2, que toda persona tiene derecho: "A que los servicios informáticos, computarizados o no, públicos o privados no suministren informaciones que afecten la intimidad personal y familiar"de forma que, aun sin autoridad administrativa y sin legislación propia, la protección de los datos personales ha existido, con rango constitucional y separada de la protección de los derechos vinculados a la privacidad o intimidad desde 1993; y ha estado, además, acompañada de la correspondiente acción de garantía, a través del Habeas Data que conforme al artículo 200, de la propia Constitución "procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o

[11] Unidad Reguladora y de Control de Datos Personales, en la página http://www.datospersonales.gub.uy/sitio/, (18/06/2012)

amenaza los derechos a que se refiere el artículo 2, incisos 5 y 6 de la Constitución."

Esta figura se legisló, se interpretó y se desarrolló, principalmente, como herramienta de acceso a la información y así puede apreciarse del contenido de la Ley 26301, Ley de Habeas Data, de mayo de 1994, pero es con la entrada en vigencia del Código Procesal Constitucional en diciembre de 2004, que reguló de forma unificada el Habeas Corpus, el Amparo, la Acción de Cumplimiento, la Acción Popular, la Acción de Inconstitucionalidad y el Habeas Data, que esta última se describe como una acción de garantía en protección del derecho de acceso" a la información que incluye los derechos a conocer, actualizar, incluir, suprimir o rectificar información o datos personales.][12]

Costa Rica

[El 5 de Septiembre del 2011, el Poder Ejecutivo de la República de Costa Rica publicó la Ley No. 8968 de Protección de la Persona frente al Tratamiento de los Datos Personales.

La Ley No. 8968 consta de cuatro secciones principales con un total de 34 artículos y tres disposiciones transitorias.

Dicha Ley tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al Tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.

El ámbito de aplicación de esta Ley es aplicable para Organismos Públicos o Privados, esta Ley crea la Agencia de Protección de Datos de los Habitantes (Prodhab) que se encuentra adscrita al Ministerio de Justicia y Paz y goza de personalidad jurídica, entre las atribuciones que la Ley le otorga, las principales son: (i) velar por el cumplimiento de la normativa en materia de protección de datos, tanto por parte de personas físicas o jurídicas privadas, como por entes y órganos públicos; y (ii) fomentar entre los habitantes el conocimiento de los

[12] Quiroga León, José Álvaro, "Ley y Autoridad Nacional de Protección de Datos Personales en el Perú, OCDE,"http://www.oecd.org/internet/interneteconomy/49211904.pdf, (20/04/12)

derechos concernientes al acopio, el almacenamiento, la transferencia y el uso de sus datos personales, entre otras.][13]

Iniciativas que han realizado otros países para el cumplimento de la Ley de protección de datos Personales.

Anteriormente se señaló en el apartado de la OCDE, en su último párrafo, que todos los países de la Unión Europea se rigen por la Directiva 95/46/CE,que fue publicada en el Diario Oficial (DO L 281) el 23 de Noviembre de 1995 y entro en vigor el 13 de Diciembre de 1995, la cual constituye el texto de referencia, a escala europea, en materia de protección de datos personales. Crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE). Con ese objeto, la Directiva fija límites estrictos para la recopilación y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la protección de los mencionados datos. La cual ponemos a su disposición para su mayor conocimiento en el siguiente link: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:ES:NOT

Directiva 95/46/CE

La Directiva tiene como objetivo proteger los derechos y las libertades de las personas en lo que respecta al tratamiento de datos personales, estableciendo principios de orientación para determinar la licitud de dicho tratamiento. Dichos principios se refieren a:

- La calidad de los datos
    - La legitimación del tratamiento
    - Las categorías especiales de tratamiento
    - La información a los afectados por dicho tratamiento
    - El derecho de acceso del interesado a los datos
    - Las excepciones y limitaciones
    - El derecho del interesado a oponerse al tratamiento
    - La confidencialidad y la seguridad del tratamiento
    - La notificación del tratamiento a la autoridad de control

[13] Cristos Velasco San Martín “Ley de protección de datos de Costa Rica” en la Pagina http://www.protecciondedatos.org.mx/2011/09/ley-proteccin-datos-costa-rica/ Última actualización 9 de Diciembre 2011

Las legislaciones nacionales deben prever un recurso judicial para los casos en los que el responsable del tratamiento de datos no respete los derechos de los interesados. Además, las personas que sufran un perjuicio como consecuencia de un tratamiento ilícito de sus datos personales tendrán derecho a obtener la reparación del perjuicio sufrido.

Se autorizará la transferencia de datos personales de un Estado miembro a un tercer país que garantice un nivel de protección adecuado; por el contrario, no se autorizará la transferencia a terceros países que no dispongan de tal nivel de protección, salvo contadas excepciones que se enumeran en el texto.

La Directiva pretende facilitar la elaboración de códigos de conducta nacionales y comunitarios que contribuyan a una correcta aplicación de las disposiciones nacionales y comunitarias.

Cada Estado miembro designará una o varias autoridades públicas independientes encargadas de controlar la aplicación en su territorio de las disposiciones adoptadas por los Estados miembros en aplicación de la presente directiva.

Se crea un grupo para la protección de las personas en lo que respecta al tratamiento de datos personales, que estará compuesto por representantes de las autoridades de control nacionales, por representantes de las autoridades de control de las instituciones y organismos comunitarios y por un representante de la Comisión.

Otras Directivas, Clausulas y Reglamento utilizados para la protección de datos en la Unión Europea.

Directiva sobre la Privacidad y las Comunicaciones Electrónicas

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, se publicó el 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas
En ella se incluyen disposiciones sobre una serie de temas más o menos sensibles, como la conservación de los datos de conexión por parte de los Estados miembros a efectos de vigilancia policial (retención de datos), el envío de mensajes electrónicos no solicitados, la utilización de los denominados «chivatos» (*cookies*) y la inclusión de datos personales en las guías públicas.

Más información en:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:ES:NOT

Cláusulas Contractuales tipo para la Transferencia de Datos Personales a Terceros Países

Decisión 2004/915/CE de la Comisión, de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países [Diario Oficial L 385 de 29.12.2004].

La Comisión Europea aprobó nuevas cláusulas contractuales tipo que podrán utilizar las empresas para garantizar adecuadamente la transferencia de datos personales de la UE a terceros países. Estas nuevas cláusulas se añadirán a las ya existentes en el marco de la Decisión de la Comisión de junio de 2001.

Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE [Diario Oficial L 181 de 4.7.2001].

Esta Decisión define las cláusulas contractuales tipo que garantizarán un nivel adecuado de protección de los datos personales transferidos de la UE a terceros países. La decisión obliga a los Estados miembros a reconocer que las sociedades u organismos que utilicen esas cláusulas tipo en contratos relativos a transferencias de datos personales a terceros países garantizan un «nivel adecuado de protección» de los datos.

Más información:

Decisión 2004/915/CE:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0915:ES:NOT

Decisión 2001/497/CE:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001D0497:ES:NOT

P*rotección de Datos por las Instituciones y Organismos de la Comunidad*

Reglamento 45/2001/CE del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos

Este Reglamento se propone garantizar la protección de los datos personales en el marco de las instituciones y organismos de la Unión Europea. El texto contempla lo siguiente:

- Disposiciones que garantizan un nivel de protección elevado para los datos personales tratados por las instituciones y los organismos comunitarios;
- Creación de una instancia de vigilancia independiente encargada de controlar la aplicación de dichas disposiciones

Más información en:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0045:ES:NOT

A continuación se perfilan algunos países de la Unión Europea que han mostrado un avance sobre la Ley de Privacidad.

Alemania

Valoración: sólido marco legal y regulatorio, entre los mejores en el mundo con reguladores y sociedad civil altamente calificados; pero las acciones del Gobierno y de los servicios de seguridad degradan seriamente las protecciones.

Los hechos más importantes que ha realizado Alemania para cumplir con la ley de protección de datos personales.-

- Protecciones constitucionales a la privacidad de las comunicaciones; aunque el Tribunal Federal Constitucional también creó en 1983 el derecho a la autodeterminación informativa; los fallos del tribunal han sido en su mayoría protectores de la privacidad.

- La ley de protección de datos está entre las más estrictas; se han añadido enmiendas en áreas de regulación entre ellas las de video vigilancia, tarjetas inteligentes, supresión de elementos de identificación, etc.

- Protecciones legales adicionales fueron creadas en 2008 para la privacidad de los empleados.

- Los reguladores federales y estatales se hallan entre los más meticulosos y entre los líderes mundiales.

- El régimen de vigilancia de las comunicaciones permite interceptaciones automatizadas sin orden judicial; amplio uso de poderes de vigilancia de comunicaciones, entre los más altos en el mundo; las investigaciones han mostrado que ocurren interceptaciones ilegales.

- La información de los abonados debe ser registrada incluso para servicios de comunicaciones prepagados.

- Su activa sociedad civil es un ejemplo para el mundo: 34,000 personas presentaron un caso ante el Tribunal Constitucional apelando contra la retención de datos.

- Amplio uso de Circuito Cerrado de Televisión (CCTV) y de técnicas de vigilancia visual, aunque los tribunales y los reguladores han estado activos

oponiéndose a planes (entre ellos en un caso, a través de la cámara de un museo se podía ver el interior del apartamento privado del Canciller).

- La policía puede utilizar la tecnología GPS para rastrear sospechosos en casos de graves delitos, incluso sin una orden judicial.

- Se han incrementado los planes para la vigilancia para viajes y la vigilancia en las carreteras y la remoción de salvaguardas que fueron implantadas originalmente cuando los sistemas se pusieron en marcha.

- Pasaportes biométricos que incluyen huellas dactilares, pero no están almacenados en bases de datos centrales o locales.

- Las cédulas de identificación son obligatorias; aunque pueden incorporar huellas dactilares, de manera voluntaria, debido a que el plan original enfrentó una considerable oposición pública.

- Uso de escáneres corporales en el Aeropuerto de Hamburgo, aunque éstos son opcionales.

- La ley de diagnóstico genético prohíbe el uso de exámenes genéticos para empleados; los datos biométricos sólo pueden ser utilizados en el centro laboral con la aprobación del Consejo de Dirección o la Junta de Arbitraje de los trabajadores.

- El lanzamiento de identificaciones para e-Salud (e-Health) fue suspendido por motivos de seguridad; ahora existen planes para un "sistema seguro de administración de datos de pacientes".

- No existe una ley específica sobre privacidad, pero es parte del derecho consuetudinario; aunque ahora existen medios automatizados para que las autoridades tengan acceso a información financiera.

- No ha ratificado el Convenio sobre la Ciberdelincuencia del Consejo de Europa, pero fue parte del proceso del Tratado de Prüm.

- El ADN obtenido de convictos por delitos graves o reincidentes en la comisión de delitos menores, y de sospechosos acusados por delitos graves, se eliminan cuando ya no son necesarios; las muestras se retienen por el mismo periodo.

Bélgica

Valoración: a pesar de que el aspecto legal es fuerte con una sociedad civil activa, las medidas de vigilancia tecnológica son problemáticas, p.ej. el régimen de retención de datos y la identificación única para viajar.

Los hechos más importantes que ha realizado a Bélgica para cumplimiento de la Ley de protección de datos personales.-

- La Constitución belga reconoce el derecho a la privacidad y a las comunicaciones privadas;

- Leyes específicas se aplican a las comunicaciones electrónicas, entre otras, la regulación de vigilancia con cámaras, la privacidad médica, el crédito de consumo y la seguridad social.

- El régimen normativo de la protección de datos ha sido criticado por no plegarse a los requerimientos de la Unión Europea (UE); pero en la actualidad, Bélgica ha implantado completamente, en leyes, las directivas de la UE.

- La Autoridad de Protección de Datos informa al Parlamento; tiene grandes capacidades con 55 miembros en personal, pero el número de quejas es relativamente bajo; pública varias guías y recomendaciones sobre procesamiento de datos.

- También cuenta con comités que supervisan áreas de actividad específicas, p.ej. la de seguridad social y salud, la de registro nacional, etc.

- Amplio régimen normativo para la vigilancia de comunicaciones: el acceso a las comunicaciones se autoriza por la judicatura, aunque aparenta ser una autoridad judicial investigadora; puede exigir el descifrado de datos y obligar a los administradores de redes a cumplir órdenes; hay un significativo número de órdenes de interceptación, las cuales están en crecimiento.

- Una ley en 2001 prohibió el anonimato para suscriptores de telecomunicaciones, y puede prohibir cualquier servicio que dificulte la aplicación de la ley de interceptaciones telefónicas.

- Retención de datos de una hasta tres años, con una policía que favorece la política de tres años, aunque no está completamente a punto; la industria se ha opuesto a una vigilancia de gran alcance.

- En 2005 se estableció una nueva agencia para el "análisis de amenazas", por medio de la evaluación de información producto de vigilancia secreta en manos de otras agencias de inteligencia, la cual según la Autoridad de Protección de Datos carece de salvaguardas adecuadas.

- Amplio plan para la vigilancia de todos los vehículos y su movimiento en Bélgica.

- Uno de los primeros países en implantar la tecnología de Identificación por Radio Frecuencia (RFID, en inglés) en sus pasaportes.

- Uno de los primeros países también en implantar "identificadores inteligentes" para firmas digitales, y un número único de identificación en todos los servicios gubernamentales; y ahora la Identificación electrónica (ID, en inglés) puede ser utilizada para comprar boletos de tren a pesar de los problemas relacionados con la privacidad.

- Incluyó documentos de identificación para niños para ser utilizados en Internet.

- Existen reglas comunes para la vigilancia en el centro laboral y guías de la Comisión.

- La plataforma de e-Salud (e-Health), que no es obligatoria, para el intercambio de información dentro del sistema de salud, está basada en el consentimiento y en protecciones incorporadas.

- Todavía se aplica el secreto bancario, aunque existe un proyecto de ley para otorgar grandes poderes a los investigadores financieros

- Liderazgo: el gobierno ha promovido la creación de un Observatorio de Derechos en Internet.

- No ha ratificado el Convenio sobre la Ciberdelincuencia del Consejo de Europa.

- El ADN de aquellos convictos por "graves ofensas", tiene un periodo de retención de 10 años; la muestra es destruida una vez creado un perfil.

España

Los hechos más importantes que ha realizado a España para cumplimiento de la Ley de protección de datos personales

- Protección constitucional para la privacidad y la protección de datos.
- Las protecciones integrales son actualizadas de manera regular para incrementar las protecciones.
- El regulador es renombrado a nivel mundial; decisiones y guías enérgicas, así como la capacidad para expedir multas.
- Periodo de retención de 12 meses para datos de comunicaciones y prohibición del anonimato en teléfonos celulares prepagados.
- El uso de sistemas de Circuito Cerrado de Televisión (CCTV) está regulado y algunas veces se requieren métodos de información.
- El debate sobre las cédulas de identificación ha sufrido por la promoción unilateral de la cédula en vez de un análisis crítico de sus capacidades.
- El ADN se elimina luego de la absolución.
- Los sistemas de registro de e-Salud (e-Health) están emergiendo.
- Ratificó el Convenio sobre Ciberdelincuencia del Consejo de Europa
- Cuentan con una Ventanilla Única, para el registro y actualización de los datos de todos los ciudadanos, dicha ventanilla se encarga de realizar los respectivos cambios en todas las organizaciones que cuenten con los datos personales de los ciudadanos.

La Agencia Española de Protección de Datos y la Oficina de Seguridad de Datos proporcionan las siguientes guías de ayuda para la implementación de Privacidad

Guía de Seguridad de Datos Publicado por la Agencia Española de Protección de Datos Link:

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_SEGURIDAD_2010.pdf

Guía de Video Vigilancia Publicado por la Agencia Española de Protección de Datos Link: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf

Guía de cómo configurar la privacidad en Redes sociales (Publicado por Oficina de Seguridad del Internauta) Link: http://www.osi.es/es/protegete/protegete-en-internet/redes-sociales

Francia

Los hechos más importantes que ha realizado a Francia para cumplimiento de la Ley de protección de datos personales.-

- No está explícitamente señalada en la Constitución pero ha sido reglamentada para estar implícitamente; aunque ha habido recomendaciones para incluirla por medio de una reforma constitucional, éstas han sido ignoradas por el Presidente.

- Ley integral y leyes sectoriales para archivos, video vigilancia, empleo y protección al consumidor.

- La Comisión Nacional de Informática y Libertades (CNIL) realiza muchas labores alrededor del mundo; tiene poderes para imponer multas que no utiliza ampliamente y tiene poderes limitados sobre ciertas áreas de la actividad gubernamental.

- El nivel de actividad legal es muy alto.

- Los nuevos poderes de vigilancia han sido desplegados con implicancias preocupantes, p.ej. la Ley de Orientación y Programación para la Seguridad Interior (LOPSSI2) para acceder de manera remota, grabar, recolectar y transferir información en manos de los sistemas de Tecnologías de la Información.

- La policía puede acceder a registros sin orden judicial en casos de terrorismo.

- Hay una ley sobre el uso del registro de nombres de los pasajeros

- Ley de retención por 12 meses y puede ser utilizada para casos sobre propiedad intelectual; requiere la retención de información identificable de abonados.

- Las agencias de inteligencia y de la policía han establecido una plataforma para otorgarse a sí mismos un fácil acceso a datos de tráfico.

- Alto nivel de acción regulatoria y de parte de la sociedad civil, pero lamentablemente sólo se han logrado pequeños cambios en la política gubernamental.

- Muchas nuevas bases de datos y sistemas han sido establecidos para vigilar a varios grupos; algunos con muy altas tasas de error.

- Amplio uso de Circuito Cerrado de Televisión (CCTV).

- Datos biométricos recolectados para labores de control de fronteras y para pasaportes, aunque no existe ninguna señal de huellas dactilares en los pasaportes.

- La propuesta de expandir el proyecto de cédulas de identificación está todavía en suspenso debido a las protestas y críticas.

- Las normas sobre privacidad en el centro laboral han permitido la lectura de correos electrónicos por parte de los empleadores, pero el abuso de actividades en Internet no es suficiente para la finalización del contrato.

- Sistema nacional de registros e-Salud, pero con serias carencias en cuanto a protección de datos y muchas brechas de seguridad; el sistema está bajo revisión pero prevalecen otros problemas.

- La vigilancia financiera ha violado dos veces el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales según la Corte Europea de Derechos Humanos.

- ADN: tomado de convictos o de aquellos acusados de "graves delitos"; los datos de los convictos se retienen por 25 años, los de los sospechosos se

eliminan por petición de la fiscalía; las muestras se retienen por iguales periodos.

Suiza

Valoración: protecciones tradicionales fuertes pero que están siendo degradadas en los últimos años, con un ambicioso espionaje, débil regulación de los servicios secretos, entre ellas próximas deliberaciones sobre ampliaciones en vigilancia de las comunicaciones. Los reguladores están realizando un buen trabajo pero se ven limitados por los recursos.

Los hechos más importantes que ha realizado a Suiza para cumplimiento de la Ley de protección de datos personales.-

- Protección constitucional para la privacidad, las comunicaciones y la protección de datos, con alguna muy convincente jurisprudencia.

- La ley federal integral sólo requiere que se registren las compañías que utilizan datos sensibles o que transfieren información al extranjero.

- Enmiendas importantes se introdujeron para exigir una seguridad adecuada y para limitar los vacios.

- Protecciones adicionales para estadísticas sobre salud, datos médicos y legales e investigaciones médicas.

- El regulador a veces tiene posibilidades limitadas de intervenir; tiene que lidiar con volúmenes significativos de quejas a pesar de sus limitados recursos; los reguladores en los cantones también cuentan con recursos limitados; pero a menudo se toman decisiones notables.

- Se han tomado medidas drásticas sobre las interceptaciones de comunicaciones legales; aunque la vigilancia de las comunicaciones se ha expandido en 2007 por parte de los servicios secretos.

- existe un periodo de retención de seis meses; pero el gobierno se halla en consultas para expandirlo a 12 meses; instalación de Troyanos, gusanos, etc.,

- para vigilar las comunicaciones cifradas; se exige identificación para acceder a los servicios de comunicación, incluso en cafeterías y hoteles.

- La privacidad financiera está protegida por una ley de 1934, pero recientemente se han estado reduciendo estas protecciones.

- Se está ampliando el uso de sistemas de Circuito Cerrado de Televisión (CCTV) e incluso el uso de aviones radiocontrolados (drones).

- Los cambios en la emisión de pasaportes significa que todos los pasaportes nuevos contendrán dos huellas dactilares y existe una base de datos de huellas dactilares.

- Se han instituido controles "móviles " de inmigración.

- Las nuevas cédulas de identificación contendrán huellas dactilares.

- hay planes para implantar una identificación para salud obligatoria que voluntariamente incluirá el almacenamiento de información médica.

- una creciente base de datos de ADN para un número ampliado de propósitos (la lista de delitos con las razones por las cuales ésta podía ser obtenida, ha sido eliminada).

- El ADN puede ser utilizado para propósitos vinculados a seguros.

Reino Unido

Valoración: en la última década este país se ha vuelto en uno de los peores ejemplos de vigilancia entre los estados democráticos, pero ha habido algunos cambios notables y significativos en el pasado año que pueden probar que es posible superar la categoría de estado vigilante.

Los hechos más importantes que ha realizado a Reino Unido para cumplimiento de la Ley de protección de datos personales.-

- No existe una protección constitucional a pesar de una rica historia de privacidad.

- La ley de protección de datos ha sido criticada por su debilidad; aunque se le han hecho mejoras, el regulador recibe muchas quejas, lo que demuestra

que la concientización del público es alta; pero sus decisiones han indicado timidez que a menudo es percibido como "debilidad".

- Al regulador se le han otorgado grandes poderes y capacidades significativas para imponer multas.

- Amplios programas de vigilancia de bases de datos y redes han sido introducidos en la pasada década, aunque algunos están siendo desmantelados.
- Un más amplio uso de vigilancia visual, contempla la vigilancia de voz y está débil régimen regulatorio sobre acceso a datos con un amplio uso de estos poderes.

- La ley de interceptación de comunicaciones sólo requiere de una aprobación ministerial con un mecanismo de supervisión pobremente dotado a través de un "comisionado".

- Las propuestas de sistemas informáticos de salud han evitado instrumentar salvaguardas adecuadas.

- Cuentan con la base de datos de ADN más grande del mundo, aunque perdió un caso en la Corte Europea de Derechos Humanos que está conduciendo a un cambio en su política (a pesar del hecho que la decisión se tomó en 2008 y actualmente todavía persiste su política); el ADN se toma de convictos de delitos registrables, o de cualquier arrestado por un delito registrable; los perfiles se retienen de manera indefinida; las muestras se retienen.

Otros Países

Algunos países han comenzado a darle una gran importancia a la protección de datos biométricos, a sabiendas que muchos países que cuentan con una ley de protección de datos personales no incorporaron algún artículo que regule el almacenamiento de datos biométricos.
En el artículo .- Leyes de protección de datos personales en el mundo y la protección de datos biométricos Parte 2 escrito por Isai Rojas González, Gabriel Sánchez Pérez , menciona algunos países que recientemente ha empezado a tomarle interés a este tema.-

En Argentina en el 2009, la Dirección Nacional de Protección de Datos Personales resolvió, respecto a un banco de datos de aficionados al fútbol, que pueden ser tratados los datos biométricos, por ser datos estrictamente de identificación, cuando sean necesarios para la finalidad pretendida (seguridad en estadios de fútbol).

Australia. El comité de reforma de la ley de privacidad, recomendó que se agregaran los datos biométricos a la definición de datos sensibles.

Rusia. Actualmente, se encuentra en proceso de modificación a su ley federal de protección de datos de 2006, el propósito es mejorar algunos aspectos de seguridad. Uno de los cambios indica que el reglamento establecerá los requisitos de seguridad para el procesamiento de datos biométricos.

Perú. Recientemente adoptó la ley número 29.733 que se refiere a la protección de datos personales y señala en su artículo 2º que los datos biométricos son datos personales sensibles.

Futura legislación en Colombia. El documento con el texto conciliado y aprobado del proyecto de ley estatutaria número 184 de 2010 Senado, 046 de 2010 Cámara en Colombia, especifica en su título III, artículo 5º que los datos biométricos son considerados datos personales sensibles.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento

En México se tuvo por primera vez un indicio en la historia jurídica de esta protección el 6 de septiembre de 2001, cuando el Diputado Federal Miguel Barbosa Huerta presentó la iniciativa con proyecto de decreto que expide la Ley de Protección de Datos Personales, la cual fue turnada a la Comisión de Gobernación y de Seguridad Pública de la Cámara de Diputados para su estudio y dictamen.[14]

En la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental se incluyó un capítulo sobre la protección de datos personales. Aunque en el momento de promulgar esta Ley no existía en el texto constitucional un derecho expreso a la protección de los datos personales, la Ley reglamentó el derecho fundamental de las personas a su vida privada, previsto en el artículo 16° de la Constitución Política de los Estados Unidos Mexicanos. Así que los siguientes pasos de la agenda política llevaron a cambiar el texto constitucional para cubrir de manera más específica la materia de los datos personales.

En el año 2007 la Constitución Política Mexicana fue reformada en su artículo 6°, sobre el derecho de acceso a la información pública, y se estableció como un límite a dicho derecho, la protección de los datos personales en la fracción 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".*

Acto seguido se procedió en dos direcciones: a) Otorgar facultades legislativas al Congreso para normar la protección de los datos personales en manos privadas, y b) Establecer el derecho a la protección de los datos personales como un derecho derivado del resguardo de la vida privada, establecido en el artículo 16° de la Constitución.

Después de un largo debate legislativo, el 30 de abril de 2009 se publicó en el Diario Oficial de la Federación la reforma que adiciona una facultad más al

[14] Con base en: Comisión de Gobernación, Dictamen con Proyecto de decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, 33 así como la denominación del capítulo II del título segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, página 1

Congreso de la Unión: "XXIX-O", para legislar en materia de protección de datos personales en posesión de particulares".

Con esta provisión constitucional, el Congreso procedió a reformar el texto del artículo 16 constitucional que fue publicada en el Diario Oficial de la Federación del 1o. de junio de 2009, y a la letra añadió como segundo párrafo:

> *Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la Ley, la cual establecerá los supuestos de excepción a los principios que rijan el Tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.*

La Ley Federal de Protección de Datos Personales en Posesión de Particulares en adelante LFPDPPP, fue aprobada por el Congreso de la Unión el 27 de abril del 2010, esta misma Ley fue publicada en el Diario Oficial de la Federación el 5 de julio del 2010 y entró en vigor el 6 de Julio del 2010.

Objetivos y alcances de la Ley

La finalidad de la LFPDPPP es la de proteger los datos personales en posesión de los particulares, al regular y controlar su Tratamiento para garantizar la privacidad y el derecho a la autodeterminación informativaconsistente en la protección del titular frente a los posibles excesos del poder informático en bancos de datos, archivos o registros de las personas, sujetando a dicha regulación a todos aquellos particulares, personas físicas y morales de carácter privado que realicen la recolección y el Tratamiento de datos personales con fines de divulgación o utilización comercial, con la sola excepción de las sociedades de información crediticia y las personas que lleven a cabo la recolección de datos personales para fines de uso personal y sin fines de lucro.

Esta Ley se alinea a los compromisos internacionales adquiridos por México, como son las directrices de protección de la privacidad y el flujo transfronterizo de datos de la Organización para la Cooperación y Desarrollo Económico (OCDE), cumple con lineamientos para lograr un flujo de datos seguro por parte de APEC, así también cumple con la Resolución 45/95 por parte de la ONU y la Directiva 95/46/CE del Parlamento Europeo.

Reglamento de la LFPDPPP

El reglamento entro en vigor el 22 de diciembre del 2011.

Dicho Reglamento establece criterios, procesos y mecanismos que facilitan a las personas físicas y morales el cumplimento de sus obligaciones y a las personas a ejercer de mejor manera sus derechos[15]

Beneficios para las empresas

Como se mencionó anteriormente la Ley surge para proteger el derecho de autodeterminación informativa de las personas, sin embargo es importante mencionar que beneficios y ventajas obtienen las empresas.

Beneficios

- Mitiga los riesgos e impactos del incumplimiento de la Ley y su Reglamento.
- Establece controles para la protección de datos de carácter personal.
- Proporciona ventaja competitiva como empresa de cara a posibles colaboraciones o trato con terceros.
- Genera confianza a los clientes, proveedores y terceras partes implicadas, asegurando la protección de sus datos personales y, sobre todo, que no se hace uso indebido de los mismos. Lo anterior aporta una imagen de seriedad y profesionalismo que incrementa el valor y la reputación de la organización.
- Reduce el riesgo de pérdida, mal uso, y/o extracción indebida de información.

Ventajas

- Garantiza el pleno ejercicio de los derechos de las personas.
- Compromiso de confidencialidad por parte de los empleados y subcontratistas respecto de los datos que conozcan y traten por motivo de su trabajo esto es una garantía también para los clientes, proveedores, administraciones y terceras partes implicadas.
- Mejora la imagen, la reputación y la relación con terceros.
- Minimiza los costos al mitigar los riesgos detectados

[15]Secretaria de Economía , "El reglamento de la ley de protección de datos personales ya está en consulta Pública", en la página: http://www.economia.gob.mx/eventos-noticias/sala-deprensa/comunicados/6598-el-reglamento-de-la-ley-de-proteccion-de-datos-personales-ya-esta-en-consulta-publica; (27/01/12)

Metodología para el estudio de nivel de cultura de protección de datos personales en las empresas de TI y otros Sectores

Objetivo del Estudio

Objetivo General

Identificar la cultura y las prácticas actuales sobre protección y Tratamiento de los datos personales en las Empresas, a fin de conocer las brechas a cerrar para generar un ambiente empresarial con prácticas avanzadas en la materia, de manera que se incorporen a sus procesos cotidianos internos y evitar sanciones.

Objetivo Especifico

Medir el nivel de cultura de las empresas de TI en relación a la protección de datos personales de acuerdo a la Ley, CANIETI encargó a AUREN quien realizó este estudio para Identificar las prácticas en materia de protección de datos personales dentro de las Empresas de TI, considerando aspectos técnicos, organizacionales, operativos y legales, así mismo medir el nivel de entendimiento y cumplimiento de la LFPDPPP dentro del sector de las TI.

Alcance del estudio

De conformidad con la Cámara de Nacional de la Industria Electrónica de Telecomunicaciones y Tecnologías de la Información, CANIETI, conjuntamente con la Secretaría de Economía y considerando el impacto de la Ley de Protección de Datos Personales en Posesión de los Particulares sobre las empresas de TI, solicitaron la realización de este estudio.

Este estudio comprende a todas las Empresas encuestadas de diversos sectores; con significación especial para el Sector de Tecnología de Información, cabe mencionar que en el cuestionario se consideran otros sectores de las Empresas encuestadas, con el fin obtener un mayor grado de significación.

Actualmente en México, existen 3,237 empresas relacionadas con el sector de Tecnologías de la Información a nivel nacional, de acuerdo con los Censos Económicos 2009 (Resultados definitivos).[16]

[16] Información proporcionada por la Secretaria de Economía, (27/03/2012)

Actividad	Subrama/clase actividad	Unidades económicas
51121	Edición de software y edición de software integrada con la reproducción	448
51219	Servicios de postproducción y otros servicios para la industria fílmica y del video	66
51211	Producción de películas, programas para la televisión y otros materiales audiovisuales	101
51821	Procesamiento electrónico de información, hospedaje y otros servicios relacionados	121
54151	Servicios de diseño de sistemas de cómputo y servicios relacionados	2,257
561422	Servicios de recepción de llamadas telefónicas y promoción por teléfono	244
Total		**3237**

Fuente: INEGI. Directorio Estadístico Nacional de Unidades Económicas[17]

Respecto al tamaño de las empresas: Para el sector de TI, la estratificación de la micro, pequeñas y medianas empresas, publicado en el DOF del 30 de Junio de 2009[18] es la siguiente: **Estratificación**

Tamaño	Sector	Rango de número de trabajadores	Rango por ventas anuales (mdp)	Tope máximo combinado*
Micro	Todas	Hasta 10	Hasta $4	4.6
Pequeña	Comercio	Desde 11 hasta 30	Desde $4.01 hasta $100	93
	Industria y Servicios	Desde 11 hasta 50	Desde $4.01 hasta $100	95
Mediana	Comercio	Desde 31 hasta 100	Desde $100.01 hasta $250	235
	Servicios	Desde 51 hasta 100		
	Industria	Desde 51 hasta 250	Desde $100.01 hasta $250	250

*Tope Máximo Combinado = (Trabajadores) X 10% + (Ventas Anuales) X 90%.

[17] Instituto Nacional de Estadística y Geografía , Censo Económico 2009 en la página http://www.inegi.org.mx/Sistemas/denue/Default.aspx

[18] Diario Oficial de la Federación, en la página http://dof.gob.mx/nota_detalle.php?codigo=5096849&fecha=30/06/2009

Diseño Metodológico

Con el fin de alcanzar los objetivos del presente estudio, se analizaron fuentes de información en relación a la cultura sobre el Tratamiento de datos personales del Sector de Tecnologías de la Información y otros Sectores.

Para ello, se trazó una doble vía de actuación:

- De un lado, la generación de información desde una perspectiva técnico-legislativa, con información de expertos/profesionales en la materia.
- De otro, encuestas a Empresas Privadas de distintos Sectores para determinar el nivel de cultura que tienen sobre la Ley, con base en el universo registrado y proporcionado por la CANIETI.

Las encuestas se realizaron por los siguientes dos medios:

- Por página de internet mediante cuestionario
- Por entrevista telefónica

Esta metodología permite analizar y confrontar los estados real y formal de los elementos que intervienen en las Empresas en cuanto a su nivel de cultura sobre la Ley.

Marco estadístico de referencia

El estudio se desarrolla a través de la estadística descriptiva que tiene que ver con el diseño de planes de muestreo, procedimientos para resumir datos, elaborar gráficas y calcular medidas que ayuden a describir algunos hallazgos derivados de un conjunto de datos.

Se trazarán los objetos del análisis cuantitativo, complementado con el análisis cualitativo.

Se realizará una segmentación por Entidades Federativas, Sector, Giro, Volumen de Facturación, Número de empleados para identificar tamaño de la Empresa y localidad.

Determinación de tamaño de muestra

El método de selección de la muestra es estadístico, determinándose el tamaño de la misma mediante la fórmula correspondiente a una población finita, en la que se ha estimado un margen de error de +/- 5% para un nivel de confianza del 95%.

Universo o unidades de muestreo = 3,237
Error tolerable = 5%
Nivel de confianza = 95%
Error esperado =10%
Tamaño de la muestra = 191

Error de muestreo a considerar

Se ha estimado un margen de error de +/- 5%

Elaboración del instrumento para el estudio

La encuesta se desarrolló con base al objetivo general del estudio, el cual es identificar la cultura y las prácticas actuales sobre protección y Tratamiento de los datos personales en las Empresas a fin de conocer las brechas a cerrar para generar un ambiente empresarial con prácticas avanzadas en la materia.

La encuesta se desarrolló estableciendo reactivos enfocados a identificar de manera general si las Empresas tienen conocimiento sobre temas relevantes de la LFPDPPP. Se contemplaron respuestas cerradas para facilitar el llenado y envío.

Para la contestación de la encuesta se remitió un correo electrónico con la invitación a contestar la encuesta, en el cual se incluyó un enlace a la página de la Secretaría de Economía para su cumplimentación.

Los instrumentos se orientaran en temas como:

1 Conocimiento de las empresas sobre la clasificación por tipo de dato que maneja la Ley y el consentimiento que requiere sobre la misma.

2 Nivel de implementación de los requerimientos de la Ley (figuras, controles y procedimientos).

3 Medidas de seguridad establecidas.

4 Cumplimiento con principios dictados por la Ley

I. Licitud;

II. Consentimiento;

III. Información;

IV. Calidad;

V. Finalidad;

VI. Lealtad;

VII. Proporcionalidad,

VIII. Responsabilidad.

5 Identificación y controles establecidos para los Encargados del Tratamiento de datos personales.

6 Tratamiento de datos personales en la nube

7 Medidas de seguridad en el Tratamiento de datos

8 Vulnerabilidades de seguridad

Encuesta electrónica

La encuesta permaneció en línea durante un mes, estableciendo reactivos enfocados a identificar de manera muy general si las empresas tienen conocimiento sobre temas antes mencionados que contiene la LFPDPPP.

La Secretaria de Economía junto con CANIETI fueron quienes de proporcionaron el universo del presente estudio, sobre el que se determinó la muestra. Asimismo, la Secretaria de Economía se encargó de enviar las solicitudes a las empresas del sector privado para responder la encuesta, la cual estuvo a disposición de los mismos en los siguientes portales de internet:

- http://www.economia.gob.mx
- https://aurenencuestas.redit.com/CuestionarioPreguntas.aspx

A partir de la información recopilada en la encuesta realizada se procedió al Tratamiento de las contestaciones recibidas. En este estudio también se tomó en consideración respuesta de empresas de diferentes sectores.

Recolección y análisis de datos

En este contexto, tomando como base la definición de Tratamiento y de Encargado, se considera que dicha figura en gran medida podrá ser ejecutada por una empresa del sector de TI, ya que éstas ofrecen servicios, tales como: la obtención, uso, divulgación o almacenamiento de datos personales, así como facilitan el establecimiento de medidas de seguridad.

Para este estudio se analizan las disposiciones legales y otros contenidos, con el fin de sentar las bases de la Ley de Privacidad. Se han tenido en cuenta, principalmente, fuentes de carácter normativo, así como estudios e informes publicados en la materia que puedan enriquecer y orientar el proyecto de investigación.

Entre las referencias de carácter normativo destacan:

Internacionales

- Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales de la **OCDE de 1980.**
- Directrices para la regulación de los archivos de datos personales informatizados de la **ONU de 1990.**
- La Directiva 1995/46/EC de la **Unión Europea de 1998.**
- Marco de Privacidad Foro de Cooperación Económica Asia **Pacífico (APEC) de 1999.**

En México

- Artículo 6° de la Constitución Política de los Estados Unidos Mexicanos.
- Artículo 16° de la Constitución Política de los Estados Unidos Mexicanos.
- Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
- Ley Federal de Protección de Datos Personales en Posesión de Particulares y su Reglamento.

Algunos Estudios e Informes que se consideraron:

- *Resumen de* Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales
- Dictamen con Proyecto de decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, 33 así como la denominación del capítulo II del título segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, Comisión de Gobernación
- Estándares Internacionales sobre Protección de Datos Personales y Privacidad Resolución de Madrid.
- Comparative study on Different Approaches to New privacy Challenges , in Particular in the light of Technological Developments, Country studies United States of America by Chris Hoofnagle ; European Commission (DouweKorff, Editor).
- La Protección de datos personales en el Distrito Federal, de Issa Luna Pla, artículo biblioteca jurídica de la UNAM.
- Boletín de política informática 2001: Artículo de Privacidad y protección de datos personales en Internet ¿Es necesario contar con una regulación específica en México?, por Cristos Velasco San Martín
- Artículo "El reglamento de la Ley de Protección de Datos Personales ya está en Consulta Pública" por la Secretaria de Economía.
- Artículo Ley de protección de datos Personales en el mundo y la protección de datos biométricos Parte I por Gabriel Sánchez Pérez.
- Artículo Ley y Autoridad Nacional de Protección de Datos Personales en el Perú, OCDE, por José Álvaro Quiroga León.
- Privacidad y protección de datos: Un análisis de legislación comparada por SusanChenMok
- Estudios realizados por las agencias de protección de datos personales de diversos países.

Las agencias que se consultaron fueron las siguientes:

- Instituto Federal de Acceso a la Información y Protección de Datos Personales (México)
- Agencia de Protección de Datos AGPD (España)
- Comisionado de Privacidad (Canadá)
- Unidad Reguladora y de Control de Datos Personales (Uruguay)
- Autoridad Nacional de Protección de Datos (Perú)
- Agencia de Protección de Datos de los Habitantes (Costa Rica)

Técnica cualitativa

El enfoque Cualitativo se utiliza para descubrir y definir preguntas de investigación. Se basa en métodos de recolección de datos sin medición numérica y sin conteo.

El estudio cualitativo involucra la recolección de datos utilizando técnicas que no pretenden asociar las mediciones con números (no pretenden cuantificar), tales como observación no estructurada, entrevistas abiertas, revisión de documentos, evolución de experiencias personales, inspección de historias de vida, interacción con grupos o comunidades, e introspección[19]

El objetivo de esta fase es conocer las diferentes posiciones de expertos en el tema de la Ley Federal de Protección de Datos Personales e identificar como estos se relacionan con el estudio cuantitativo realizado para reforzar las conclusiones que a continuación se presentaran.

Dentro de estas fases se tomó en cuenta algunas conferencias de Protección de Datos (referenciadas a continuación), así también la opinión de algunos expertos sobre el tema en seminarios.

Conferencia:

IX Encuentro Iberoamericano.- El 31 de octubre de 2011 se celebró en la Ciudad de México el IX Encuentro Iberoamericano de Protección de Datos organizado por el Instituto Federal de Acceso a la Información y Protección de Datos y la Secretaría Permanente de la Red Iberoamericana de Protección de Datos.

[19]Con base en: M. Gómez, Marcelo "Introducción a la Metodología de la investigación Científica, Editorial Brujas".

Los integrantes de la Red Iberoamericana de Protección de Datos asumen el compromiso de adopción de estándares regionales e internacionales que garanticen un alto nivel de protección de los datos personales, facilitar un eficiente desarrollo de los flujos internacionales de datos que redunden en el desarrollo de actividades económicas con garantías para los ciudadanos, con independencia del país de su residencia.

Seminarios:

Modelos de autoridades de control en transparencia y protección de datos personales: una autoridad o doble autoridad. / Lina Ornelas – Directora General de Clasificación y Datos Personales del IFAI

Modelos de Autoridades de protección de datos

En este documento se comentan las ventajas de tener la LFPDPPP, también menciona una breve descripción de cómo está regulado la ley de protección de datos de algunos países (Portugal, Francia, Canadá, España, Reino Unido, entre otros países pertenecientes a la Unión Europea).

El impacto de las trasferencias internacionales de datos en américa latina. Las políticas preventivas y la autorregulación en la implantación de la normativa de protección de datos

PONENCIA IV: Experiencias sectoriales de autorregulación.

El modelo de autorregulación en México / Lina Ornelas Núñez

En esta presentación se comentan los beneficios que se tiene de implementar la ley, los cursos que ha impartido el IFAI, la experiencia con la que cuenta IFAI la cual la obtuvo desde el 2002 con la Ley Federal de Transparencia y Acceso a la Información.

Casos de Éxito

NOM-024-SSA3-2007.- Fue la primera en Política Pública en someterse a una PIA (Manifestaciones de Impacto a la Privacidad). El consultor que realizó la PIA fue ex director de la Agencia Española de Protección de Datos.

Análisis del Estudio

Técnica cualitativa

Se analiza a continuación la información recibida a través de la encuesta publicada para el estudio. Se recibió repuesta por parte de 221 empresas cubriendo el tamaño de muestra requerido de 191 empresas y presentando los siguientes datos.

Los resultados estadísticos que a continuación se muestran sobre el nivel de adecuación de la normativa en materia de protección de datos por sector, tamaño e industria por parte de las empresas encuestadas, corresponden a la parte cuantitativa de los trabajos de investigación del estudio, complementados con la información recabada en la fase cualitativa.

Con el objeto de facilitar su comprensión el análisis se ha dividido en 4 apartados

Importancia: Identificar en que empresas ha permeado más la Ley para lo cual nos basamos en la clasificación que realiza el INEGI y poder realizar un análisis en función de recursos industria o sector.

Objetivos:

1) Identificar por sector y tamaño el nivel de cumplimiento

2) Identificar los factores que contribuyen o impiden el cumplimiento

1. Empresas participantes en el estudio

    - Perfil del encuestado
    - Tipos de datos que maneja la Empresa

Importancia: Se identifica el nivel de implementación de los requerimientos de la Ley con el cual podemos inferir el conocimiento de la misma.

Objetivo: Cual es el estatus actual en las compañías en relación a los requerimientos de la Ley.

2. Estatus de cumplimiento con la ley de las empresas encuestadas y razones por las que no se cumple.

    - Figuras y procedimientos definidos dentro de la Empresa
    - Medidas de seguridad

- Aviso de privacidad
- Principio de finalidad
- Calidad de datos
- Principio de lealtad
- Responsabilidad

Importancia: La parte del responsable se abordó como parte de una de las hipótesis del estudio, se pensó que las TI pueden fungir un papel importante como encargados de tratamiento.

Objetivos:

1) Poder identificar si las compañías de TI cuentan con un nivel aceptable de controles, que aseguren el cumplimiento de la Ley

2) Determinar el nivel de madurez de las empresas de TI para promoverlos como encargados con un nivel de cumplimiento alto.

3. Encargado del Tratamiento.

Importancia: Debido a la tendencia actual sobre nuevas tecnologías y el impacto que puede tener el desconocimiento de la Ley, en relación a la protección de datos personales.

Objetivos: Identificar el nivel de concienciación en relación a la ubicación de datos personales en la nube

4. Datos Personales en la Nube

Nota 1: En algunos casos se han empleado redondeos no mostrando los decimales, incrementando la unidad si el primer decimal es superior a 5 y truncando los decimales y dejando el entero correspondiente si el primer decimal es inferior a 5. Como excepción en aquellos casos en que los datos sean menor a la unidad se aplicarán dos decimales.

Para efectos de este estudio en adelante tomaremos como definiciones las que establece el Artículo 3 de la LFPDPPP y el Artículo 2 del Reglamento de la LFPDPPP que a la letra citan.-

LFPDPPP

***Artículo 3**.- Para los efectos de esta Ley, se entenderá por:*

Aviso de Privacidad: Documento físico, electrónico o en cualquier otro formato generado por el Responsable que es puesto a disposición del Titular, previo al Tratamiento de sus datos personales, de conformidad con el artículo 15 de la presente Ley.

***Bases de datos:** El conjunto ordenado de datos personales referentes a una persona identificada o identificable*

***Consentimiento:** Manifestación de la voluntad del Titular de los datos mediante la cual se efectúa el Tratamiento de los mismos.*

***Datos personales:** Cualquier información concerniente a una persona física identificada o identificable.*

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

***Encargado:** La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del Responsable.*

***Ley:** Ley Federal de Protección de Datos Personales en Posesión de los Particulares.*

***Reglamento:** El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.*

***Responsable:** Persona física o moral de carácter privado que decide sobre el Tratamiento de datos personales.*

***Tercero:** La persona física o moral, nacional o extranjera, distinta del Titular o del Responsable de los datos.*

***Titular:** La persona física a quien corresponden los datos personales.*

***Tratamiento:** La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.*

***Transferencia:** Toda comunicación de datos realizada a persona distinta del Responsable o Encargado del Tratamiento.*

Reglamento de la LFPDPPP

Artículo 2. *Además de las definiciones establecidas en el artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, para los efectos del presente Reglamento se entenderá por:*

Derechos ARCO: *Son los derechos de acceso, rectificación, cancelación y oposición;*

Listado de exclusión: *Base de datos que tiene por objeto registrar de manera gratuita la negativa del 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, destinados para:*

a) Prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información;
b) Proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones;
c) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad, y
d) Garantizar la eliminación de datos de forma segura;

Medidas de seguridad técnicas: *Conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar que:*

a) El acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados;
b) El acceso referido en el inciso anterior sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
c) Se incluyan acciones para la adquisición¸ operación, desarrollo y mantenimiento de sistemas seguros, y
d) Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el Tratamiento de datos personales;

Persona física identificable*: Toda persona física cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información. No se considera persona física identificable cuando para lograr la identidad de ésta se requieran plazos o actividades desproporcionadas;*

Soporte electrónico: *Medio de almacenamiento al que se pueda acceder sólo mediante el uso de algún aparato con circuitos electrónicos que procese su*

contenido para examinar, modificar o almacenar los datos personales, incluidos los microfilms;

Soporte físico: *Medio de almacenamiento inteligible a simple vista, es decir, que no requiere de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos personales.*

1. Empresas participantes en el estudio

- Perfil del Encuestado

En este apartado se muestra la estratificación considerada para el estudio del perfil del encuestado, presentando el tipo de Empresas: Micros, Pequeñas o Medianas Empresas que participaron, así como un comparativo entre las empresas del Distrito Federal y las Entidades Federativas.

Las siguientes **Gráficas 1 y 1.1** proporcionan datos sobre el porcentaje de participación que tuvieron las empresas encuestadas, conforme a la Entidad federativa a la que pertenecen.

Gráfica 1: Porcentaje de Participación del Distrito Federal y Entidades Federativas en la Encuesta (%)

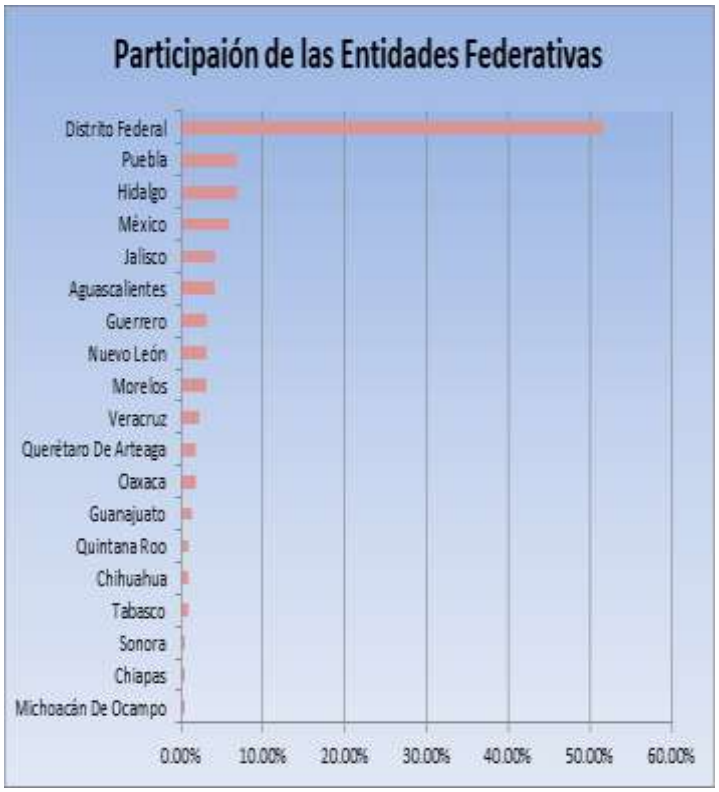
Porcentaje de Encuestados	
Distrito Federal	**52%**
Entidades Federativas	**48%**

Es significativo que las respuestas de las encuestas han sido del Distrito Federal, con un porcentaje del 52% lo que indica que las grandes urbes de población alcanzan un mayor compromiso en participar al responder a las cuestiones más avanzadas en estos momentos.

La participación del resto de Entidades Federativas con un 48% del total de las respuestas obtenidas, indica que hay una disociación entre el Distrito Federal y el resto de las Entidades Federativas.

Como resultado de esta primera cuestión cabe señalar que las Entidades Federativas tienen un menor grado de respuesta con las encuestas que la Secretaría de Economía pone a su disposición.

Gráfica 1.1 – Porcentaje de Participación del Distrito Federal y Entidades Federativas en la encuesta (%)



Participación de las Entidades Federativas	
Distrito Federal	51.58%
Hidalgo	6.79%
Puebla	6.79%
México	5.88%
Aguascalientes	4.07%
Jalisco	4.07%
Nuevo León	3.17%
Guerrero	3.17%
Morelos	3.17%
Veracruz	2.26%
Querétaro De A.	1.81%
Oaxaca	1.81%
Guanajuato	1.36%
Chihuahua	0.90%
Quintana Roo	0.90%
Tabasco	0.90%
Sonora	0.45%
Chiapas	0.45%
Michoacán De O.	0.45%

Finalmente se obtuvieron los siguientes resultados respecto a la participación de las Entidades Federativas en la encuesta:

Se comprueba una homogeneidad en las respuestas entre las Entidades Federativas respecto a las empresas que radican en su territorio.

La **Gráfica 2** y la **Tabla 2** muestran el nivel de participación que tuvieron en las encuestas las Empresas por Sector.

Gráfica 2: Sector de las Empresas Encuestadas (%)

Tabla 2:Sector de las Empresas Encuestadas (%)

Servicios	52%
Comercio	34%
Industria	14%

Con base en lo que contestaron los encuestado se obtuvo lo siguiente: El Sector de Servicios presento una mayor participación con un 52%, siguiéndole con un 34% el Sector Comercio y con un 14% el Sector Industria.

En este caso el sector que estamos analizando es el de Servicios y Comercio pues las PYMES del sector de las Tecnologías de Información conforman la gran mayoría en este grupo.

Obteniendo un 86% del total de las respuestas de las Empresas de Servicios y Comercio objeto de este estudio.

La **Gráfica 3** muestra el porcentaje de participación de los encuestados por el cargo que ocupan dentro de la Empresa identificando cuales pertenecen al Distrito Federal y cuales a otras Entidades Federativas.

Gráfico 3: Cargo que ocupan los encuestados (%)

Cargo que ocupan los encuestados				
Cargo	Distrito Federal	Entidades Federativas	Cargo	%
Dirección General	19%	33%	Dirección General	26%
Gerencia	20%	19%	Analista	20%
Analista	24%	17%	Gerencia	19%
Jefatura	11%	14%	Jefatura	13%
Dirección	11%	8%	Dirección	10%
Subdirección	3%	6%	Coordinación	8%
Coordinación	12%	4%	Subdirección	4%

Determinando lo siguiente: Si bien el mayor porcentaje de participación fue de las Empresas del Distrito Federal, la mayoría de los encuestados fue de nivel Analista, mientras que los participantes de otras Entidades Federativas que contestaron ocupan el cargo de Dirección General.

Es de destacar que en las Entidades Federativas la respuesta ha sido proporcionada directamente por el Director General (26%), seguido de los Gerentes y posteriormente por los Analistas y Jefaturas, indicando claramente que tienen interés sobre esta materia, aunque no apliquen su cumplimiento.

Las Direcciones de las empresas encuestadas tienen un bajo índice de participación (10%) lo que indica su bajo interés de la LFPDPPP y por consiguiente de su cumplimiento.

Gráfica 4: Tamaño de las Empresas Encuestadas con base en el importe de sus ventas (%)

Tamaño de las Empresas encuestadas con base en el importe de ventas				
Ventas	**Distrito Federal**	**Entidades Federativas**	**Ventas**	**Total general**
Menos de $4	64%	68%	Menos de $4	66%
$4 - $100	20%	18%	$4 - $100	19%
$101 - $250	7%	7%	$101 - $250	7%
Más de $250	9%	7%	Más de $250	8%

Unidades expresadas en 1.000.000 de Pesos

La **Gráfica 4** muestra el nivel de participación por tamaño de las Empresas, dependiendo del importe de ventas que generan, segmentadas por Distrito Federal y Entidades Federativas

La **Tabla 4.1** muestra un comparativo del cargo que tiene el encuestado frente al tamaño de la Empresa.

Los tamaños son bastante similares comparando el Distrito Federal y las Entidades Federativas.

Las Empresas que tienen un volumen de facturación menor a 4 millones de pesos mexicanos anuales suponen el 66% del total de facturación.

Con un volumen de facturación superior a 250 millones de pesos mexicanos han respondido el 8%.

Los datos proporcionados por INEGI incluyen un volumen de facturación de hasta 250 millones de pesos mexicanos, no obstante la encuesta al ser pública han contestado un número significativo de Empresas que facturan más de los 250 millones de pesos alcanzando un porcentaje del 8%, considerando que las Empresas grandes a nivel nacional son el menor porcentaje.

Por lo tanto la muestra de Empresas que ha respondido a los cuestionarios satisface en gran medida el objetivo de este estudio.

Tabla 4.1: Comparativo del cargo que tiene el encuestado frente el tamaño de las Empresas (sobre las ventas realizadas) (%)

Cargo y Ventas	Distrito Federal	Entidades Federativas
Dirección General	**19%**	**33%**
$101 - $250	1%	1%
$4 - $100	1%	6%
Menos de $4	18%	26%
Analista	**24%**	**17%**
$101 - $250	3%	2%
$4 - $100	11%	2%
Más de $250	1%	2%
Menos de $4	10%	11%
Gerencia	**20%**	**19%**
$101 - $250	1%	2%
$4 - $100	4%	4%
Más de $250	4%	5%
Menos de $4	11%	8%
Jefatura	**11%**	**14%**
$101 - $250	0%	3%
$4 - $100	1%	1%
Más de $250	2%	0%
Menos de $4	9%	10%
Dirección	**11%**	**8%**
$101 - $250	3%	0%
$4 - $100	1%	1%
Más de $250	1%	0%
Menos de $4	6%	7%
Coordinación	**12%**	**4%**
$4 - $100	4%	1%
Más de $250	1%	0%
Menos de $4	8%	3%
Subdirección	**3%**	**6%**
$4 - $100	0%	4%
Menos de $4	3%	2%

Con base en lo anterior, se determina lo siguiente: el 66% de las Empresas encuestadas generan ventas de menos de $4 millones de pesos al año, este porcentaje pertenecen a las micro empresas y el 19% genera ventas de $4 a $10 millones de pesos anuales, perteneciendo a las pequeñas Empresas. Por lo que podemos identificar que la mayoría de las Empresas que participaron en la encuesta son micro empresas.

Por lo que respecta a la **Tabla 4.1** con base al comparativo del cargo que tiene el encuestado frente al tamaño de las Empresas, se determina que las Empresas que pertenecen a otras Entidades Federativas que tuvieron mayor participación en la encuesta son micro empresas cuyos participantes tienen un cargo de Dirección General; mientras que de las empresas del Distrito Federal se obtuvo un mismo nivel de participación por parte de las Micro y Pequeñas Empresas y la mayoría de los encuestados ocupan un cargo de Analistas.

Las Empresas con facturación superior a 250 millones de pesos mexicanos que respondieron a la encuesta corresponden a los perfiles de Analistas y Jefatura, indicando que estas organizaciones cuentan con Responsables dedicados a la materia de privacidad si bien su conocimiento sobre la materia es escaso y su aplicación incompleta.

Las respuestas de las Empresas con facturación inferior a 250 millones de pesos mexicanos han sido proporcionadas por directivos lo que indica claramente el desconocimiento de la LFPDPPP y que no existen Responsables asignados a estas tareas.

Gráfica 5: Giro de la Empresa (%)

Giro de la Empresa	Porcentaje de Participación
Tecnología de la Información	24%
Otros Servicios	24%
Pequeña empresa (imprenta, tintorería, etc.)	15%
Consultoría de Negocios	9%
Servicios Financieros	5%
Servicios profesionales (médico, dentista, contador)	5%
Consultoría Legal	5%
Comunicaciones y Transporte	4%
Agropecuaria	2%
Seguros	2%
Logística	2%
Salud	1%
Construcción	1%

La **Gráfica 5** muestra el porcentaje de las Empresas que participaron en la encuesta, con base a su giro.

De lo anterior se determina que de las Empresas encuestadas, el giro que tuvo el mayor nivel de participación con **un 24% fue el de Tecnología de la Información**; mostrando un porcentaje igual el de Otros servicios, sin embargo este último engloba servicios diferentes a los identificados en la encuesta.

Conforme a los porcentajes anteriormente mostrados observamos que el Sector que presentó mayor participación en la encuesta es el de Servicios con un 52%, siguiéndole el sector Comercio con un 34% y el sector Industrial con 14% (Gráfica 2).

En general, los cargos que presentaron mayor participación en la encuesta son: Dirección General con 26%, Analistas con un 20% y la Gerencia con un 19%.

- **Tipos de datos que maneja la Empresa**

Para poder recabar, almacenar y tratar datos personales debemos identificar el tipo de dato que se desea tratar conforme a la clasificación que establece la Ley, para determinar el tipo de consentimiento que debemos solicitar del titular de los datos. Para poder identificar esta clasificación y determinar el tipo de consentimiento que necesitamos para el tratamiento de datos nos sujetaremos a lo establecido por el artículo 3 Fracción VI y artículo 8 de la Ley que a la letra dice.

Artículo 3.-

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

Articulo 8.-

Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente Ley.

El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos.

Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición.

Los datos financieros o patrimoniales requerirán el consentimiento expreso de su titular, salvo las excepciones a que se refieren los artículos 10 y 37 de la presente Ley.

El consentimiento podrá ser revocado en cualquier momento sin que se le atribuyan efectos retroactivos. Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.

Conforme a lo establecido en **Artículo 3 Fracción V** del Reglamento los "Datos personales es cualquier información concerniente a una persona física identificada o identificable".

La **Gráfica** muestra los tipos de datos que manejan las Empresas encuestadas.

Con base en los datos que proyectaron las encuestas agrupamos los tipos de datos personales en:

- Básicos
- Básicos, Financieros y Patrimoniales
- Básicos, Financieros, Patrimoniales y Sensibles

Gráfica 6: Tipos de datos que maneja la Empresa en cuanto a su tamaño (%)

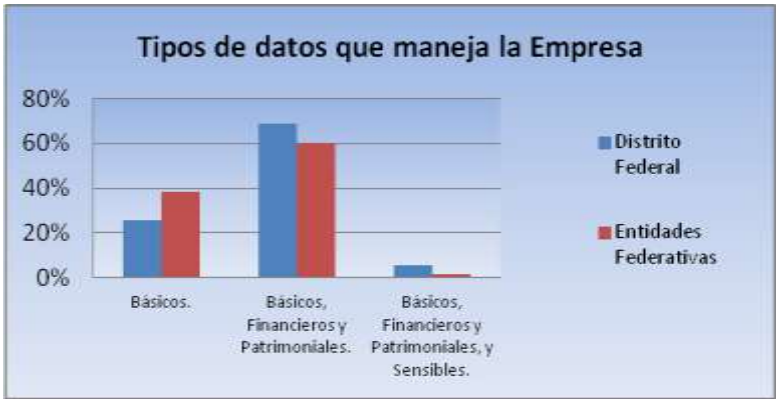
Tipos de datos que maneja la empresa en cuanto a tamaño						
Ventas	Básicos, Financieros y Patrimoniales, y Sensibles.	Básicos, Financieros y Patrimoniales.	Básicos.	Total general	Ventas	Total general
Más de $250	2.05%	3.08%	2.31%	7.44%	Más de $250	7.44%
$101 - $250	0.51%	7.44%	0.26%	8.21%	$101 - $250	8.21%
$4 - $100	0.26%	16.15%	3.85%	20.26%	$4 - $100	20.26%
Menos de $4	0.77%	37.95%	25.38%	64.10%	Menos de $4	64.10%
Total general	**4%**	**65%**	**32%**	**100%**	**Total general**	**100.00%**

Nota: Para mejor comprensión nos referiremos al tamaño de Empresas conforme a la siguiente referencia de ventas:

- Menos de $4 pertenece a Micro Empresas
- $4 - $100 pertenece a Pequeñas Empresas
- $101 - $250 pertenece a Medianas Empresas
- Más de $250 pertenece a Grandes Empresas

De lo anterior podemos observar que de las Empresas encuestadas, las Micro empresas del sector privado son las Empresas que más manejan datos personales entre básicos financieros y patrimoniales con un 37.95%, muy por encima de las Pequeñas Empresas que reportan un 20.26% de manejo de datos personales, mientras que las Grandes Empresas tratan un 7.44% de datos personales y sólo las Medianas Empresas tratan un 8.21% de datos personales; De los cuales los tipos de datos que más manejan las Empresas encuestadas son los Básicos, Patrimoniales y Financieros con un 65% y los que menos manejan son los sensibles con un tratamiento del 4%.

Gráfica 7: Tipos de datos que maneja la Empresa (%)



Tipos de Datos que Maneja la Compañía			
Tipo de Dato	Distrito Federal	Entidades Federativas	Total general
Básicos.	26%	38%	31%
Básicos, Financieros y Patrimoniales.	69%	60%	65%
Básicos, Financieros y Patrimoniales, y Sensibles.	5%	2%	4%

Nota: No se presentaron respuestas con manejo de datos básicos y sensibles, todas aquellas Empresas que contestaron que manejaban datos sensibles también relacionaron que manejaban datos financieros y patrimoniales.

La clasificación de tipos de datos de carácter personal está basada en el reglamento y específicamente en el tipo de consentimiento solicitado al Titular de los datos en el momento en que se recaban.

También nos hemos basado en la clasificación que la Ley Española y las publicaciones de Agencia Española de Protección de Datos tiene de la clasificación de datos personales (Básico, Medio y Alto).

Es muy significativo que el 4% de los encuestados reporta datos sensibles, lo que indica - como analizaremos posteriormente - que no se obtienen los consentimientos de los Titulares ni se tienen las medidas de seguridad apropiadas.

En este aspecto es de reseñar que los Titulares de los datos carecen del conocimiento de sus derechos respecto a la LFPDPPP al ceder sus datos financieros y sensibles sin consentimiento y sin comprobar las medidas de seguridad apropiadas.

Con base en lo anterior se determina que los datos que tratan la mayoría de las Empresas son de dos tipos, datos Básicos y Financieros y Patrimoniales con un 65%, mientras que las Empresas que sólo tratan datos básicos son el 31%, y sólo un 4% de las Empresas trata datos Básicos, Financieros y Patrimoniales y Sensibles.

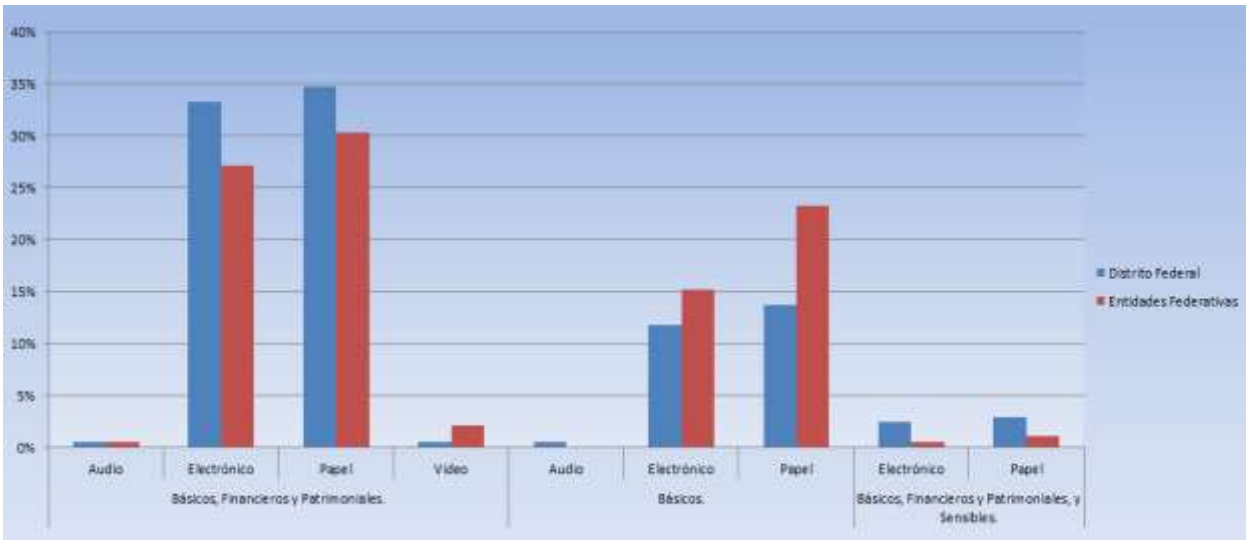
Cabe recalcar que solo en el artículo 3 de la respectiva Ley menciona a que se refiere los datos Personales Sensibles, pero en ningún otro artículo de la Ley o su Reglamento Explican a qué se refiere datos Personales Básicos y, Financieros y Patrimoniales.

Esto provoca una confusión tanto para el ciudadano como para el Empresario, ya que no se explica de manera clara lo que abarca cada una de estas clasificaciones.

Esto impacta en el tipo de consentimiento que se debe recabar del Titular para el Tratamiento de sus datos personales, así también sobre las medidas de seguridad que deben implementar los Responsables y Encargados; ya que no es los mismo tener medidas de seguridad para datos Básicos que para datos Financieros y Patrimoniales o Sensibles.

Esta falta de precisión de la Ley ocasiona confusión pudiendo provocar que no se implementen Medidas Seguridad o que estas sean inadecuadas al tipo de dato que se trate, perjudicando al Titular.

Gráfica 8: Tipo de Almacenamiento de Datos (%)



En la **Gráfica 8 y Tablas 8,** se muestran los medios en los que se almacenan los datos personales que obran en posesión de las Empresas encuestadas tanto del Distrito Federal como de las demás Entidades Federativas de la Republica.

Tabla 8 :Forma de Almacenamiento y Tipo de Datos utilizados segmentado por Distrito Federal y Entidades Federativas

Tipo de Almacenamiento			
Medio de Almacen	Distrito Federal	Entidades Federativas	Total general
Papel	51.22%	54.59%	53%
Electrónico	47.32%	42.70%	45%
Video	0.98%	0.54%	1%
Audio	0.49%	2.16%	1%

Tipos de Datos y Forma de Almacenamiento por parte de las Empresas		
Tipo de Dato y forma de Almacenamiento de Datos	Distrito Federal	Entidades Federativas
Básicos, Finan. yPatrim.	**68.78%**	**60.00%**
Papel	34.63%	30.27%
Electrónico	33.17%	27.03%
Video	0.49%	2.16%
Audio	0.49%	0.54%
Básicos	**25.85%**	**38.38%**
Papel	13.66%	23.24%
Electrónico	11.71%	15.14%
Audio	0.49%	0.00%
Básicos, Finan. yPatrim. ySen.	**5.37%**	**1.62%**
Papel	2.93%	1.08%
Electrónico	2.44%	0.54%

De lo anterior podemos decir que, del total de las Empresas encuestadas el 53% almacena sus datos personales en Papel, mientras que el 45% de las Empresas almacena sus datos personales en medios Electrónicos. Por lo anterior es relevante mencionar que encontrándonos en una era de avances tecnológicos, aún la mayoría de las Empresas sigue almacenando los datos personales en medios no automatizados como lo es el Papel.

El alto porcentaje de Tratamiento de información con datos de carácter personal en soporte papel es debido en su gran mayoría a dos razones principales, la primera de ellas a que se deben conservar justificantes de documentos oficiales y únicamente estos documentos son válidos en formato original no permitiéndose el formato electrónico, en segundo lugar las empresas pequeñas tienen cedidas sus gestiones a otras empresas por lo que no precisan de automatización en el Tratamiento de datos de carácter personal.

La Ley, ni el Reglamento de la misma no cuentan con fundamento para el tipo de almacenamiento para los datos personales dejando estos al libre albedrío de las Empresas, así mismo no se han hecho recomendaciones por parte del IFAI en cuanto a que tipo de almacenamiento es más recomendable; por el momento dicho Instituto sólo ha emitido estas recomendaciones en el caso de la Ley de Transparencia que es aplicable a entidades de carácter público.

2. Estatus de cumplimiento de la Ley; en las Empresas encuestadas y razones por las que no se cumple.

- **Figuras o Procedimientos definidos dentro de la Empresa**

La Ley establece las figuras y procedimientos que las Empresas deben implementar la para protección de los datos personales que obren en su posesión.

La Ley señala la necesidad de definir la figura del ***Responsable*** de los datos, entendido como la persona jurídica y/o física, de carácter privado que decide sobre el Tratamiento de los datos personales, es decir, toma decisiones sobre qué hacer con los mismos, es el Responsable desde que el dato es recabado, almacenado, tratado, hasta la eliminación del mismo, es el Responsable durante toda la vida del dato, aún que delegue responsabilidades a un Encargado.

La Ley define así mismo al ***Titular,*** siendo esta cualquier persona física a la cual pertenecen los datos, siendo esta cualquier información que lo haga identificable frente a la sociedad. Determinándole derechos y obligaciones para la protección efectiva de sus datos.

La figura del ***Encargado***, es establecida como aquella que tratará datos personales por cuenta de un Responsable, figura que desempeñará las funciones que el Responsable le delegue para el cumplimiento de la protección de datos, como consecuencia de la existencia de una relación jurídica que los vincula y delimita el ámbito de su actuación para la prestación de un servicio.

Dentro de los procedimientos que la Ley establece para la protección de los datos se encuentra el ejercicio de Derechos ***ARCO***:

Derechos de Acceso, Rectificación, Cancelación y Oposición: la Ley dota a los individuos de un conjunto de derechos que se traducen en el derecho a acceder a todos los extremos de su información personal, a rectificarla en caso de ser inexacta o incompleta, a cancelarla cuando resulte ser inadecuada o excesiva u oponerse al Tratamiento para una finalidad determinada por razones justificadas.

En este mismo sentido, la ley ha diseñado procedimientos sencillos y expeditos para que las personas puedan ejercer dichos derechos ante los Responsables, y en caso de que los Titulares consideren que sus pretensiones en el ejercicio de dichos derechos han sido transgredidas acudan a la autoridad garante.

Listado de ***exclusión*** creada para aquellos Titulares que se oponen al Tratamiento de sus datos para fines comerciales, aunque anteriormente hayan otorgado su

consentimiento, la lista de exclusión certifica que los Titulares no serán molestados en su persona garantizando la privacidad de sus datos.

España cuenta con una lista similar la cual es llamada como Lista Robinson.

El Servicio de Lista Robinson es un servicio de exclusión publicitaria gestionado por la Asociación Española de la Economía Digital, creado conforme a lo previsto en la normativa sobre Protección de Datos Española.

Este servicio se enmarca en el ámbito de la publicidad dirigida a nombre de una persona y a una dirección de correo postal, a una dirección de correo electrónico o a un número de teléfono concreto.

Cualquier persona puede inscribirse en el Servicio de Lista Robinson de forma gratuita. Para ello es necesario indicar, el medio a través del cual no desea recibir publicidad de entidades con las cuales no mantenga ni haya mantenido algún tipo de relación.

Las entidades deben consultar la Lista Robinson para no enviar comunicaciones comerciales a aquellas personas inscritas en el Servicio, cuando realicen acciones publicitarias dirigidas a personas que no sean sus clientes, socios, usuarios, para evitar ser sancionados por incumplimiento.

El propósito de la Ley al crear las figuras y procedimientos necesarios es crear un modelo de protección que garantice que los datos personales no serán tratados para fines de lucro, comerciales, garantizando la privacidad de los Titulares garantía individual establecida recientemente por la Constitución Política Mexicana.

En este apartado analizaremos de las empresas encuestadas, aquellas que cuentan con algún procedimiento o figura definida conforme a lo establecido en la Ley, así mismo en caso de no contar con alguna figura o procedimiento determinar las causas por las cuales no lo tienen definido. Finalmente mostraremos las Medidas que adoptan las empresas para garantizar el Tratamiento de los datos.

Gráfica 9: Figuras o Procedimientos definidos dentro de la Empresa (%)

En la gráfica se aprecia que el 31% de los encuestados no cuenta con ninguna figura o procedimiento referido por la Ley mientras que el 69% cuentan con algún Procedimiento o Figura (Responsable 28%, Titular 18%, Encargado 14%, ARCO 8% y Exclusión 1%).

Aunque las Empresas tienen asignado un Responsable de Seguridad (28%) y contrastando este porcentaje con el de Atención de Derechos ARCO (8%) se observa que no se aplican adecuadamente los principios de la LFPDPPP por lo que concluimos que los Responsables carecen de los conocimientos necesarios para cumplir la LFPDPPP.

Gráfica 10: Motivo por el cual no cuentan con alguna Figura o Procedimiento que Marca la Ley (%)

Ninguna de las Anteriores	%
Desconocimiento de la Ley y su Reglamento.	27.1%
Falta de entendimiento de la Ley.	2.4%
Falta de compromiso de la Administración.	1.3%
Otra.	0.5%

La **Gráfica 10**muestra las causas por las cuales las Empresas no cuentan con alguna Figura o Procedimiento definido por la Ley dentro de la Empresa.

Del 31% de las Empresas que no cuentan con alguna Figura o Procedimiento definido; el 27.1% señala que Desconoce la Ley y su Reglamento, el 2.4% No entiende la Ley y el 1.3% se debe a la Falta de compromiso de la Administración.

Si bien el IFAI y la Secretaría de Economía han realizado una labor de divulgación, observamos que el nivel de conocimiento es aún incipiente.

Es significativo que el 4% de los encuestados señala que no hay compromiso de la alta dirección para el cumplimiento de la Ley. En este momento ya se ha producido por parte del IFAI la primera sanción y consideramos que esta actuación incitará a las Empresas a cumplir con la LFPDPPP.

Tabla 10.1 Análisis por Giro de las Empresas encuestadas que cuentan con alguna Figura o Procedimiento (%)

Figura o Procedimiento	%
Generación de un Listado de exclusión	**1%**
Tecnología de la Información	0.97%
Consultoría Legal	0.16%
Atención a Derechos ARCO	**8%**
Consultoría Legal	2.91%
Servicios Financieros	2.26%
Tecnología de la Información	1.70%
Otros Servicios	0.65%
Consultoría de Negocios	0.49%
Seguros	0.16%
Encargado	**14%**
Tecnología de la Información	7.19%
Servicios Financieros	2.18%
Consultoría Legal	1.94%
Otros Servicios	1.78%
Consultoría de Negocios	1.13%
Servicios profesionales (médico, dentista, contador)	0.08%
Titular	**17%**
Tecnología de la Información	5.50%
Consultoría Legal	4.53%
Servicios Financieros	3.23%
Otros Servicios	2.26%
Consultoría de Negocios	1.62%
Seguros	0.16%
Agropecuaria	0.08%
Responsable	**28%**
Tecnología de la Información	8.81%
Consultoría Legal	5.01%
Otros Servicios	3.88%
Consultoría de Negocios	3.40%
Servicios Financieros	2.99%
Logística	1.46%
Construcción	1.13%
Seguros	0.65%
Pequeña Empresa (imprenta, tintorería, etc.)	0.32%
Salud	0.08%
Ninguno de los anteriores	**31%**
Otros Servicios	8.00%
Pequeña Empresa (imprenta, tintorería, etc.)	7.76%
Tecnología de la Información	5.25%
Servicios profesionales (médico, dentista, contador)	2.26%
Consultoría de Negocios	2.26%
Comunicaciones y Transporte	1.54%
Servicios Financieros	1.05%
Seguros	0.97%
Logística	0.65%
Consultoría Legal	0.65%
Agropecuaria	0.57%
Salud	0.32%

El análisis anterior muestra que el Giro de Tecnología de Información es el que mayor porcentaje de inclusión de Figuras y Procedimientos tiene conforme a la Ley, no obstante hace falta reforzar sus procedimientos para atención de Derechos ARCO. Observamos que los únicos Giros que cuentan con Listado de exclusión son el de Tecnologías de Información y Consultoría Legal con un 1%, mientras que para la atención de Derechos ARCO el Giro de Consultoría Legal se encuentra en primer lugar con 2.91 %, siguiéndole el Giro de Servicios Financiero con un 2.26% y quedando en tercera posición con un 1.7% el Giro de Tecnología de Información. También es importante destacar que en relación a la Figura de Responsable, el Giro de Tecnología de Información se encuentra en el primer lugar con 8.81%, en segundo lugar el de Consultoría Legal con 5.01% y en tercer lugar Otros Servicios el de con 3.88%.

Solo el 8% de las Empresas que cuentan con la figura de Responsable cuentan con un procedimiento para el ejercicio de los Derechos Arco, determinando que solo el 1.7% del Giro de Tecnología de la Información ejerce este procedimiento.

Estos datos demuestran que la gran mayoría de las Empresas encuestadas, creen estar cumpliendo con la Ley al contar con la figura del Responsable, pero ignoran, o no han concretado todo el procedimiento para el cumplimiento de la Ley, los motivos pueden ser la falta de entendimiento de la LFPDPPP y su Reglamento, y el interés de los directivos de las Empresas.

Para que la LFPDPPP sea conocida tanto por los Titulares para que ejerzan sus derechos y por las Empresas que deban aplicar los controles adecuados que establece la Ley debe hacerse cumplir de la manera en que se indica en la misma de lo contrario se produce el fenómeno inverso de incredulidad sobre la misma. En la medida en que las autoridades actúen y se aplique sanciones, se focalizará la atención para el cumplimiento con la Ley y se tomará conciencia de los Titulares y Empresas.

Los antecedentes históricos sobre la privacidad indican que el efecto de la no aplicación de sanciones a las Empresas implica laxitud por las autoridades en la aplicación de la Ley y por lo tanto que no se tome en serio la LFPDPPP, y no apliquen los preceptos descritos en la misma y su Reglamento ya que ello involucra costes de implantación y mantenimiento que dé inicio no se justifiquen.

- **Medidas de Seguridad**

La Ley impone a los particulares: personas físicas y morales de carácter privado; que realicen el Tratamiento de datos personales una serie de obligaciones y reglas para asegurar su uso y protección adecuados.

Un pilar básico y fundamental de un efectivo sistema de protección de datos personales es la garantía de la seguridad de la información, entendida ésta como la implementación de medidas administrativas, físicas y técnicas eficaces para garantizar y velar por la integridad, confidencialidad y disponibilidad de tus datos personales. Ello contribuye a minimizar los riesgos de acciones en contra de la información personal como robo, alteración o modificación, pérdida total o parcial, transmisiones indebidas o ilícitas, accesos no autorizados y robo de identidad, entre otras, que pueden lesionar los derechos o libertades de los Titulares.

Confidencialidad: Asegurar que sólo quienes estén autorizados pueden acceder a la información

Integridad: Asegurar que la información y sus métodos de proceso son exactos y completos solo el personal autorizado sea capaz de modificar la información o recursos de computo

Disponibilidad: Asegurar que los usuarios autorizados tiene acceso a la información y a sus activos asociados cuando lo requieran

Los Responsables no deberán adoptar medidas de seguridad menores a aquellas que mantengan para el manejo de su información.

Para la implementación de dichas medidas éstos deberán tomar en cuenta factores como riesgo existente y posibles consecuencias para los Titulares, la sensibilidad de los datos personales y el desarrollo tecnológico.

Los Responsables deberán realizar un análisis de riesgos de datos personales que les ayude a determinar sus áreas de peligro en caso de una vulneración, para así poder establecer las medidas de seguridad aplicables a los datos personales. Y además realizar un Análisis de brechas de las medidas de seguridad existentes y aquellas faltantes para cada tipo de dato y cada sistema de Tratamiento. Para posteriormente realizar un Plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brechas, lo cual le garantiza al Titular que sus datos se encontrán bajo los niveles más estrictos de seguridad impidiendo que sus datos sean vulnerados.

Para el caso de existir alguna vulneración en la seguridad de los datos personales tratados, es obligación del particular establecer un procedimiento para la atención

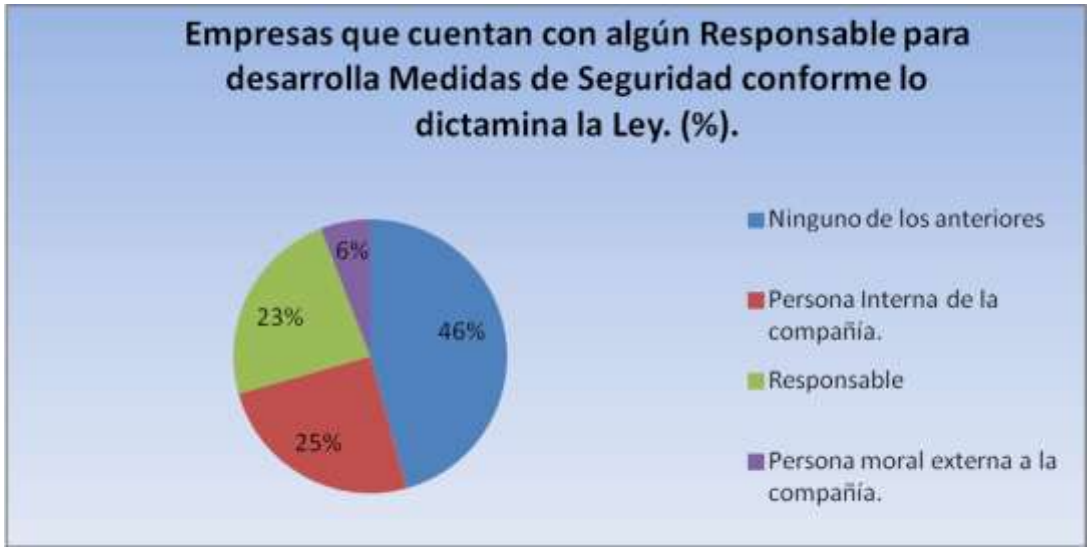
de estas vulneraciones que de manera pronta y eficiente, de solución al problema; así mismo tiene la obligación de hacer del conocimiento de la situación al Titular afectado a manera de que pueda tomar las medidas necesarias para la protección de sus datos, informándole al particular las medidas adoptadas para su solución.

La obligación de seguridad que regula la Ley y desarrolla el Reglamento, obliga a adoptar las medidas necesarias para proteger los datos, pero reconoce que ninguna Empresa puede garantizar al 100% que, con la adopción de dichas medidas, no vayan a producirse o existir incidencias.

Por ello, el Responsable debe acreditar que estableció y siguió las medidas de seguridad exigibles en cada caso, así evitará una posible sanción por parte del IFAI. Su comportamiento siempre será valorado en función de las circunstancias y exigencias de cada Tratamiento, pesando sobre él la carga de la prueba de que adoptó todas las medidas necesarias para evitar o reducir el posible daño.

En este apartado analizaremos si las Empresas encuestadas desarrollan e implementan las Medidas de Seguridad conforme a lo que estable la Ley.

Gráfica 11: Empresas que cuentan con algún Responsable para desarrollar Medidas de Seguridad conforme lo dictamina la Ley. (%)



La **Gráfica 11** muestra el porcentaje de Empresas encuestadas que cuentan con las Medidas de Seguridad que establece la Ley y que cuentan con una persona a cargo para su cumplimiento conforme a lo establecido en el Articulo 59 del Reglamento.

Con base a lo anterior se determina lo siguiente:El 54% de las Empresas encuestadas consideran que desarrollan Medidas de Seguridad conforme a lo establecido en la Ley, de estos el 49% deja esta responsabilidad a personal interno (incluyendo Responsable), y únicamente el 6% encarga estas medidas a una persona moral externa a la Empresa, destacando que el 46% restante de las Empresas encuestadas no identifica a un Responsable para las Medidas de Seguridad faltando al artículo 19 de la Ley, y al artículo 59 del Reglamento.

Tabla 11.1: Factores que consideran las Empresas para establecer las medidas de seguridad aplicables a los datos personales.

Factores que consideran las Empresas para establecer las Medidas de Seguridad aplicables a los datos personales. (Tabla obtenida del 54% de las Empresas que cuentan con Personal interno o externo de la Empresa para el Desarrollo de Medidas de Seguridad)					
Responsable		**Persona moral externa a la Empresa.**		**Persona Interna de la Empresa.**	
El riesgo inherente por tipo de dato personal.	20%	El riesgo inherente por tipo de dato personal.	17%	El riesgo inherente por tipo de dato personal.	23%
La sensibilidad de los datos personales tratados.	19%	La sensibilidad de los datos personales tratados.	14%	La sensibilidad de los datos personales tratados.	17%
El desarrollo tecnológico.	19%	El desarrollo tecnológico.	27%	El desarrollo tecnológico.	7%
Las posibles consecuencias de una vulneración para los Titulares.	17%	Las posibles consecuencias de una vulneración para los Titulares.	17%	Las posibles consecuencias de una vulneración para los Titulares.	16%
Las vulnerabilidades previas ocurridas en los sistemas de Tratamiento.	12%	Las vulnerabilidades previas ocurridas en los sistemas de Tratamiento.	17%	Las vulnerabilidades previas ocurridas en los sistemas de Tratamiento.	8%
El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.	7%	El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.	7%	El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.	11%
Otros factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al Responsable.	2%	Otros factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al Responsable.	0%	Otros factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al Responsable.	2%
El número de Titulares.	2%	El número de Titulares.	0%	El número de Titulares.	14%
Ninguna de las anteriores.	2%	Ninguna de las anteriores.	1%	Ninguna de las anteriores.	2%

Con base en lo anterior se determina lo siguiente: La **Tabla 11.1** muestra que el 54% de las empresas que consideran cuentan con personal interno o externo para desarrollar Medidas de Seguridad para el Tratamiento de Datos Personales consideran los factores establecidos por el Artículo 60 del Reglamento.

Muestra que el Responsable y el Personal Interno de la Empresa muestran una mayor disposición a considerar **el riesgo inherente por tipo de dato personal** (Responsable 20% y Persona Interna 23%), el Personal Externo tiene una mayor disposición a considerar el **desarrollo tecnológico.** Asimismo estos últimos consideran mayormente las vulnerabilidades previas ocurridas con un 17% contra un 12% del Responsable y 8% de Personal Interno.

Tabla 11.2: Acciones que considera el Responsable como Medidas de Seguridad (%)

Acciones que considera el Responsable como Medidas de Seguridad (Tabla obtenida del 54% de las Empresas que desarrollan Medidas de Seguridad					
Responsable		**Persona moral externa a la Empresa**		**Persona Interna de la Empresa**	
Elaborar un inventario de datos personales y de los sistemas de Tratamiento.	29%	Elaborar un inventario de datos personales y de los sistemas de Tratamiento.	24%	Elaborar un inventario de datos personales y de los sistemas de Tratamiento.	25%
Determinar las funciones y obligaciones de las personas que traten datos personales.	25%	Determinar las funciones y obligaciones de las personas que traten datos personales.	18%	Determinar las funciones y obligaciones de las personas que traten datos personales.	25%
Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.	18%	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.	19%	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.	15%
Llevar a cabo revisiones o auditorías.	11%	Llevar a cabo revisiones o auditorías.	6%	Llevar a cabo revisiones o auditorías.	16%
Capacitar al personal que efectúe el Tratamiento.	5%	Capacitar al personal que efectúe el Tratamiento.	1%	Capacitar al personal que efectúe el Tratamiento.	7%
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.	4%	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.	4%	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.	0%

Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.	3%	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.	22%	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.	5%
Realizar un registro de los medios de almacenamiento de los datos personales.	2%	Realizar un registro de los medios de almacenamiento de los datos personales.	4%	Realizar un registro de los medios de almacenamiento de los datos personales.	4%
Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.	1%	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.	1%	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.	1%
Ninguna de las anteriores.	1%	Ninguna de las anteriores.	1%	Ninguna de las anteriores.	1%

La **Tabla 11.2** muestra (con base al 54% de las Empresas que consideran cuentan con un Responsable o personal externo para desarrollar Medidas de Seguridad) las ***Acciones consideradas por parte de las Empresas para la seguridad de los datos personales***, resultando que tanto el Responsable, el Personal Externo y el Personal Interno de la Empresa tiene una mayor tendencia a tomar acciones como: Elaborar inventarios de datos personales y de los sistemas de Tratamiento.

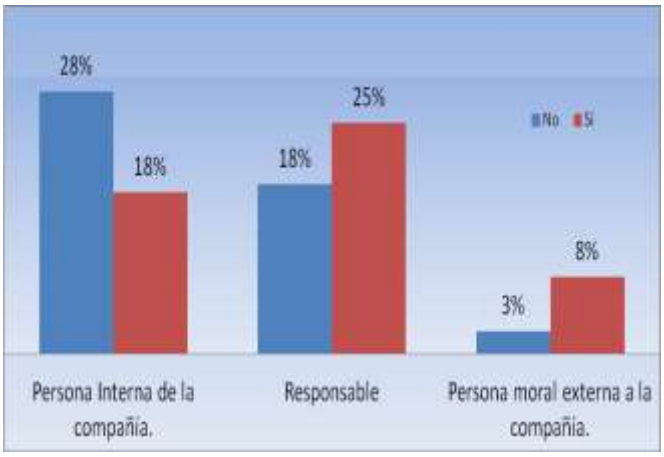
Asimismo, estos prestan poca atención a capacitar al personal que efectúe el Tratamiento de datos personales. (Responsable 5%, Personal Externo 1% y Personal Interno 7%).

Cabe señalar que mientras el Personal Externo a la Empresa toma interés alto en el *Establecer las Medidas de Seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva* con 22%, el Responsable muestra un interés del 3% y el Personal Interno 5%.

La conclusión sobre este apartado es que los Responsables carecen de los conocimientos necesarios para aplicar la LFPDPPP y el Reglamento por lo tanto los riesgos no son detectados y consecuentemente no son tomados en cuenta, así como que los análisis de brechas necesarios para elaborar planes de acción no han sido realizados.

Este apartado concluimos que las medidas de seguridad son adoptadas de forma intuitiva y sin un análisis y planes apegados a lo establecido en la LFPDPPP

Gráfica 12: ¿Se cuenta con algún procedimiento para la notificación de Vulnerabilidades? (%)



Cuentan con algún procedimiento para notificación de vulnerabilidades de seguridad		
Figura que desarrolla medidas de seguridad	**No**	**Si**
Persona Interna de la compañía.	28%	18%
Responsable	18%	25%
Persona moral externa a la compañía.	3%	8%
Total general	**49%**	**51%**

Las respuestas a esta cuestión han sido muy variadas ya que aunque cuenten con un procedimiento de notificación de vulnerabilidades estos no están considerando la LFPDPPP.

Los procedimientos de notificación de vulnerabilidades en su mayoría son para virus que afectan a los equipos de procesamiento de información.

Con base en lo anterior se tiene lo siguiente: El 54% de las Empresas que consideran cuentan con algún Responsable para establecer Medidas de Seguridad para datos personales, sea Personal Interno o Externo. Del 54% referido, el 51% **(contemplando que 54% equivale a 100%)** consideran que cuentan con algún procedimiento para notificar que hubo una vulneración de seguridad (27% a nivel general) y el 49% no cuentan con algún procedimiento para notificar que hubo una vulneración de seguridad.

Se concluye que el 27% de las Empresas desconocen o están aplicando inadecuadamente artículo 20 de la Ley, así también los artículos 64 y 65 del Reglamento (anteriormente mencionados) en relación al procedimiento para notificación de vulnerabilidades

Con el fin de obtener un porcentaje general de las Empresas que cuentan con algún Responsable para establecer Medidas de Seguridad para datos personales, se determinó que el 51% que considera cuenta con algún procedimiento para notificar que hubo una vulneración de seguridad equivale al 28% del total de Empresas.

Tabla 12.1: ¿Quiénes registran evidencias para demostrar la obtención del consentimiento del Titular? (%)

¿Quiénes registran evidencias para demostrar la obtención del consentimiento del Titular?	
¿Se registran evidencias para demostrar la obtención del consentimiento del Titular?	**Si**
Persona Interna de la Empresa.	**35%**
No	7%
Si	28%
Persona moral externa a la Empresa.	**16%**
No	1%
Si	15%
Responsable	**49%**
No	7%
Si	42%

En esta cuestión aunque las respuestas pueden parecer positivas no concuerdan con los datos que analizaremos posteriormente ya que las Empresas no cuentan con avisos de privacidad y por consiguiente esta respuesta tiene un sesgo de optimismo por parte del encuestado.

La **Tabla 12.2** muestra el tipo de consentimiento que recaban las Empresas encuestadas dependiendo del tipo de dato personal que manejan.

Tabla 12.2 Tipo de Consentimiento que se recaba de acuerdo al Tipo de datos que maneja la Empresa (%)

Tipo de consentimiento	Básicos.	Básicos, Financieros y patrimoniales.	Básicos, Financieros y Patrimoniales, y Sensibles.
Expreso	7%	12%	10%
Expreso y por Escrito	60%	50%	10%
Tácito	33%	37%	80%

La **Tabla 12.2** muestra que las disposiciones que establece la Ley son desconocidas o no han sido entendidas para la mayor parte de las Empresas, debido a los resultados de la encuesta muestran que el 60% de las Empresas que recaban datos de carácter Básico lo hacen mediante consentimiento expreso y por escrito, cuando por Ley sólo se requiere consentimiento tácito, y en forma contraria para recabar los datos de carácter Sensible la encuesta muestra que el

80% de las Empresas utilizan el consentimiento tácito en lugar del expreso y por escrito como requiere la Ley.

En este apartado de la encuesta los encuestados mostraron un sesgo significativo ya que como veremos más adelante carecen de los avisos de privacidad.

En algunos casos el guardar evidencias han sido debido a los registros de entrada a las instalaciones de las Empresas y a la documentación que deben conservar para para las relaciones contractuales.

Existiendo una confusión entre las evidencias de los registros de entrada y documentos contractuales que se conservan y la adecuada aplicación de la LFPDPP.

Así también en las anteriores graficas podemos observar que solo la mitad de las Empresas encuestadas cuentan con algún Responsable de seguridad ya sea interno o externo, de las cuales no cumplen con toda las medidas de seguridad que determina la Ley y su Reglamento.

Estas Empresas no cumplen con todas la medidas que menciona la Ley por desconocimiento o falta de entendimiento de la misma.

A medida que el Titular conozca la Ley y haga exigibles sus derecho las Empresa se obligara a implementar estas medidas seguridad.

- **Aviso de Privacidad**

Cuando se lleva a cabo la recopilación de datos personales de un Titular, el Responsable debe informarle de lo siguiente:

1) Su identidad y dirección.
2) Que sus datos van a ser almacenados en bases de datos, la finalidad para la que se recaban y los destinatarios de la información.
3) La posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición.
4) Las opciones y medios que el Responsable ofrezca a los Titulares para limitar el uso o divulgación de los datos

Esta comunicación se podrá facilitar al Titular por cualquier medio que permita asegurar que ha recibido la información que contempla este principio: de palabra, por escrito en un formulario, impreso. No es admisible una información genérica que no permita saber quién es el Responsable y para qué se están recabando los datos.

Se debe cumplir con este Principio de información cualquiera que sea el procedimiento de recopilación de datos. Estos procedimientos pueden ser de diversos tipos: formularios, encuestas, entrevistas, transmisión electrónica de datos, registros públicos, directorios electrónicos, currículos, páginas Web o teléfono.

En todo caso, el deber de información deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse prueba del mismo mientras persista el Tratamiento de datos del Titular. Así, el Responsable deberá conservar evidencia en el que conste el cumplimiento del deber de informar. Para el almacenamiento de los datos, el Responsable podrá utilizar medios informáticos o en otro formato como el papel.

En esta apartado analizaremos si las Empresas cuentan con Aviso de Privacidad, conforme a lo requerido por la Ley en los Artículo 15, 16, 17 y 18 de la Ley y Artículos 23 y 25 del Reglamento.

La **Gráfica 13** muestra el porcentaje de las Empresas encuestadas que cuentan o no con Aviso Privacidad.

Gráfico 13: Aviso de Privacidad

Tabla 13: Aviso de Privacidad (%)

Aviso de Privacidad	
No	73%
Si	27%

Con base en lo anterior se tienen los siguientes resultados: El 27 % de las Empresas encuestadas cuenta con Aviso de Privacidad y el 73% restante no cuentan con Aviso de Privacidad.

Estos datos indican claramente que las Empresas no están informando adecuadamente y por lo tanto aplicando la LFPDPPP en el momento de recabar datos personales.

El grado de cultura está en un estado incipiente y deberán tomarse medidas tanto para los Titulares como para las Empresas.

Tabla 13.1: En qué momento se da a conocer al Titular el Aviso de Privacidad (%)

En qué momento se da a conocer al Titular el Aviso de privacidad de acuerdo al 27% de las Empresas que cuentan con Aviso de Privacidad	
El aviso de privacidad se facilita en el momento en el que se recaba el dato (falto de los requerimientos que establece la Ley para un Aviso de Privacidad completo).	**53%**
El aviso de privacidad se facilita en el momento en el que se recaba el dato y se pone a disposición del Titular el nombre de la Empresa (Responsable que recaba los datos) y el domicilio así como las finalidades del Tratamiento de datos y se proveen los mecanismos (liga de página en internet) para que el Titular conozca el texto completo de aviso de privacidad (Aviso de Privacidad optimo)	**47%**

La **Tabla 13.1** muestra en que momento las Empresas que si cuentan con Aviso de Privacidad (27%), dan a conocer el Aviso de Privacidad al titular.

De lo anterior se determina que del 27% de las Empresas que cuentan con Aviso de Privacidad el 53% da a conocer su Aviso de Privacidad de manera incompleta, al momento en que se recaba los datos, considerado Aviso ilegal pues no cuenta con los requerimientos que establece la Ley; por el contrario, el 47% de las Empresas da a conocer su Aviso de Privacidad en el momento en el que se recaba el dato y se pone a disposición del Titular el nombre de la Empresa, el domicilio, y las finalidades del Tratamiento de datos, y se proveen los mecanismos (liga de página en internet) para que el Titular conozca el texto completo de aviso de privacidad siendo este un Aviso de privacidad óptimo y prudente al momento de recabar datos, pues se protege la Empresa y al mismo tiempo protegen los derechos de los Titulares.

Tabla 13.2: Del 27% de las Empresas que cuentan con Aviso de Privacidad ¿Qué elementos Contiene? (%)

Del 27 % Que cuenta con aviso de privacidad han contestado lo siguiente:	
De los siguientes elementos contienen Aviso de Privacidad.	
La identidad y domicilio del Responsable que los recaba.	**30%**
Las finalidades del Tratamiento de datos.	**26%**
Las opciones y medios que el Responsable ofrezca a los Titulares para limitar el uso o divulgación de los datos.	**18%**
Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley.	**15%**
Las transferencias de datos que se efectúen.	**9%**
El procedimiento y medio por el cual el Responsable comunicará a los Titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley.	**2%**

La **Tabla 13.2** muestra los elementos que contiene el Aviso de Privacidad,

Se muestra claramente que la aplicación de los elementos en los Avisos de Privacidad son incompletos a pesar de la Guía sobre Avisos de Privacidad que está disponible en la página del IFAI

Tabla 13.3: ¿Cómo se da conocer al Titular el Aviso de Privacidad? (%) (del 27% de las Empresas que cuentan con Aviso de Privacidad)

Del 27 % Que cuenta con aviso de privacidad han contestado lo siguiente:	
Como se da a conocer al Titular el Aviso de Privacidad.	
A través de cartel en recepción al ingreso a la Empresa (medio visual).	**28%**
A través de portal o página de internet (medio digital).	**25%**
A través de formatos impresos como boletín, documento enviado por correo tradicional.	**23%**
A través de correo electrónico (medios digitales).	**19%**
A través del teléfono viva voz o grabación en la contestadora telefónica (IVR) (medios sonoros).	**3%**
Otros.	**2%**
A través de medidas compensatorias.	**1%**

La **Tabla 13.3** muestra cómo se da a conocer al Titular el Aviso de Privacidad con base al 27% de las Empresas que cuentan con él.

De lo anterior se determina lo siguiente del 27% de las Empresas que tienen Aviso de Privacidad:

- El 30% define la identidad y domicilio del Responsable.
- El 26% tiene la finalidad del Tratamiento de datos.
- Sólo el 2% identifica el procedimiento y medio por el cual el Responsable comunicará a los Titulares de cambios al aviso de privacidad

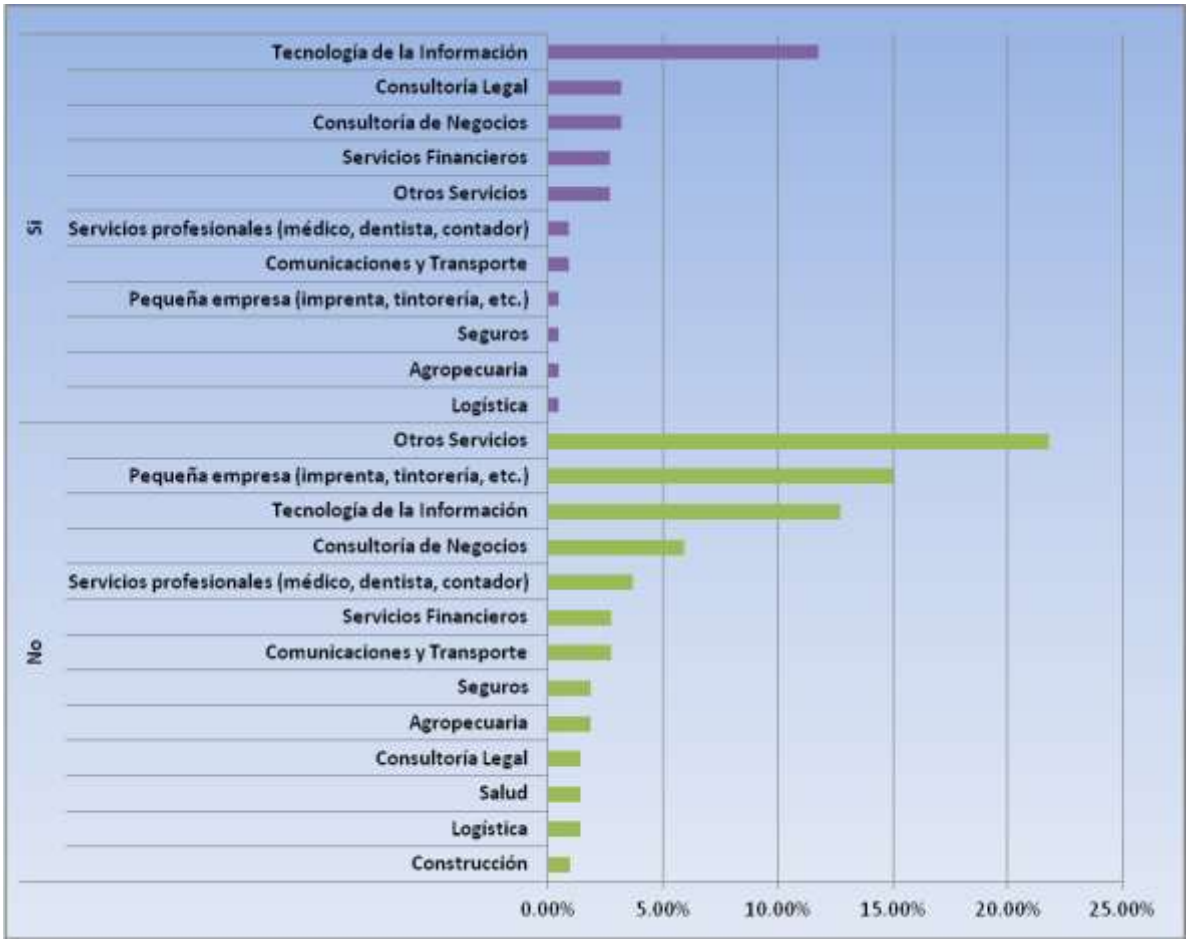
En relacionado a la forma en que se da a conocer el Aviso de Privacidad:

- El 28% da a conocer el Aviso de Privacidad por medio visuales.
- El 25% da a conocer el Aviso de Privacidad a través de portal o página de internet.
- Sólo el 2% da a conocer el Aviso de Privacidad a través del teléfono viva voz o grabación en la contestadora telefónica (IVR) (medios sonoros).

Estos datos refleja que aun contando con Avisos de Privacidad estos son inadecuados en su gran mayoría.

Este dato se correlaciona con el del conocimiento de la LFPDPPP y refleja que los Avisos de Privacidad se están utilizando de manera inadecuada.

Gráfica 13.4 Empresas que cuenta con Aviso de Privacidad por Giro (%)



La **Gráfica 13.4** muestra las Empresas que cuentan con Aviso de Privacidad por Giro

En esta gráfica podemos observar que el Giro que cumple mayormente con el Aviso de Privacidad es el Tecnología de Información con un 11.76%, siguiéndole el de Consultoría Legal y de Negocios con 3.17%.

Tabla 13.4 Empresas que cuenta con Aviso de Privacidad por Giro (%)

Que Empresa cuenta con Aviso de Privacidad de acuerdo a su Giro	%
No	**73%**
Otros Servicios	21.72%
Pequeña Empresa (imprenta, tintorería, etc.)	14.93%
Tecnología de la Información	12.67%
Consultoría de Negocios	5.88%
Servicios profesionales (médico, dentista, contador)	3.62%
Servicios Financieros	2.71%
Comunicaciones y Transporte	2.71%
Seguros	1.81%
Agropecuaria	1.81%
Salud	1.36%
Consultoría Legal	1.36%
Logística	1.36%
Construcción	0.90%
Si	**27%**
Tecnología de la Información	11.76%
Consultoría Legal	3.17%
Consultoría de Negocios	3.17%
Servicios Financieros	2.71%
Otros Servicios	2.71%
Comunicaciones y Transporte	0.90%
Servicios profesionales (médico, dentista, contador)	0.90%
Logística	0.45%
Pequeña Empresa (imprenta, tintorería, etc.)	0.45%
Agropecuaria	0.45%
Seguros	0.45%

Con base en lo anterior se determina que hay mayor número de Empresas encuestadas que no cuenta con Aviso de Privacidad con un 73% y sólo el 27% cuentan con el Aviso de Privacidad.

El índice de Empresas que cuentan con Avisos de Privacidad es del 27 %, sin embargo el contenido analizado en la tabla 12-2 nos muestra que estos avisos son incompletos.

Si bien el IFAI ha publicado una guía sobre cómo elaborar un aviso de privacidad esta guía no ha sido utilizada por las Empresas.

Siendo destacable que las Empresas del sector TI han sido las que más aplican los Avisos de Privacidad, seguidos de la Consultoría Legal.

El Sector que menos aplican los Avisos de Privacidad es el de Servicios y Pequeñas Empresas.

La Ley hace exigible y obligatorio, el Aviso de Privacidad para todas las Empresas, y es facultad de las mismas apegarse a los requerimientos que establece la Ley con la finalidad de que el titular tome decisiones informadas con relación a sus datos personales y controle el uso de su información personal.

Uno de los indicadores por el cual las Empresas no cuentan con Aviso de Privacidad, es principalmente el desconocimiento de la Ley, aunado a que los titulares de los datos personales no hacen exigible los derechos que les faculta esta Ley, ante las Empresas que tratan sus datos.

- **Calidad de Datos**

El principio de calidad de datos introduce un criterio de racionalidad y proporcionalidad en el Tratamiento de los datos personales.

Los datos personales en posesión de Empresas deben estar actualizados y reflejar con veracidad la realidad de la información, de tal manera que cualquier inexactitud no afecte la información de los Titulares, encontrándose los datos al día.

Los datos recabados deben ser adecuados, pertinentes y no excesivos, estableciendo que sólo se recopilarán aquellos datos necesarios para la finalidad establecida por el Responsable.

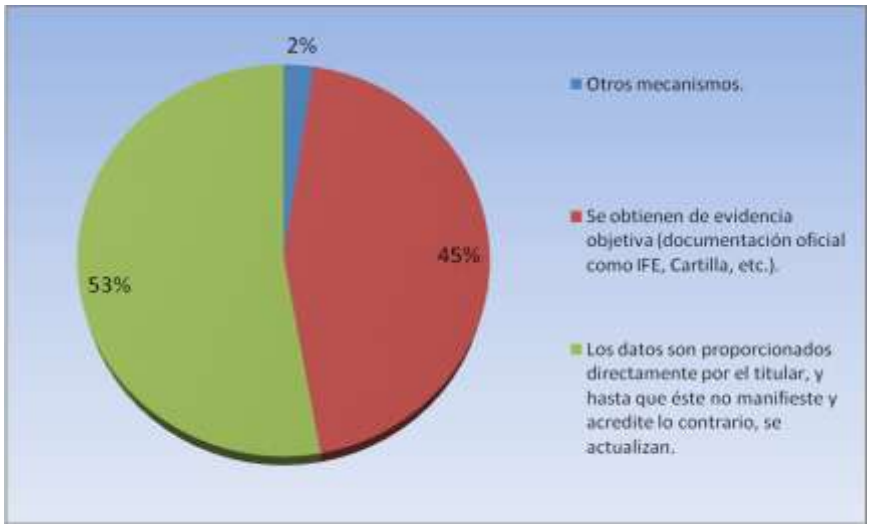
Cuando la finalidad para la cual se proporcionaron los datos deja de existir, el Tratamiento deja de ser necesario y, por lo tanto, las Empresas deben cancelarlos. La Ley establece al Responsable demostrar mediante pruebas que el Responsable han cancelados en su totalidad los datos que obraban en su posesión, de manera que el Responsable no pueda recuperar los datos y utilizarlos de forma ilícita.

Los datos proporcionados conforme a la Ley cuentan con un periodo de resguardo dependiendo del tipo de datos que se trate, contemplando 72 meses para su eliminación definitiva en caso de que los datos ya no sean necesarios para los fines por los que fueron recabados; así mismo para la información de tipo contable el Código Fiscal establece que el periodo mínimo de resguardo será de 5 años.

El principio de calidad permite reducir errores en los datos tratados, considerando que en el caso de ser inexactos se le da la facultad al Titular de corregir sus datos, controlando los Titulares sus datos personales, mejorando la información proporcionada como resultado cumplen los objetivos de la Ley en forma eficaz y eficiente, mejorando la visión que los Titulares tengan de las Empresa ya que les garantizan la confianza de que sus datos se encuentran correctos, actualizados y que únicamente trataran los datos pertinentes y necesarios. Asimismo al Titular le garantiza que sus datos al termino de cumplida la finalidad y tras el periodo de resguardo sus datos serán cancelados y no serán tratados para distintas finalidades de las que fue objeto su recopilación.

En este apartado analizaremos los Mecanismo que adoptan las Empresas encuestadas para asegurar el principio de Calidad de los Datos Personales,

Gráfica 14: Mecanismo que adoptan las Empresas para asegurar el Principio de Calidad de Datos (%)



Mecanismos que adoptan las Empresas para asegurar el Principio de calidad de datos.	%
Los datos son proporcionados directamente por el Titular, y hasta que éste no manifieste y acredite lo contrario, se actualizan.	53%
Se obtienen de evidencia objetiva (documentación oficial como IFE, Cartilla, etc.).	45%
Otros mecanismos.	2%

La **Gráfica 14** muestra los mecanismos que adoptan las Empresas encuestadas para garantizar el principio de Calidad de Datos.

Este principio es de gran utilidad para las Empresas puesto que, al estar establecidas relaciones contractuales entre el Titular y las Empresas, estas últimas tienen interés en proporcionar sus servicios o productos, y quisieran mantener buenas relaciones con los Titulares ya que generarán más negocios en el futuro.

Este principio de la LFPDPPP ya se venía llevando a cabo en las Empresas por motivos estrictamente comerciales y legales.

Con base en lo anterior se tiene del total de las Empresas encuestadas:

- El 53% de las Empresas actualiza los datos proporcionados por el Titular hasta que este no manifieste lo contrario.
- El 45% de las Empresas obtiene evidencia objetiva (documentación oficial como IFE, Cartilla, etc.) de los datos proporcionados.
- El 2% utiliza otros mecanismos para asegurar el principio de Calidad de Datos.

Tabla 14.1: Mecanismos de calidad adoptados por las Empresas que registran evidencias para la obtención de datos con consentimiento del Titular

Mecanismos que adoptan las Empresas para asegurar la calidad de datos personales.	Registran evidencias para la obtención de consentimiento del Titular
	Si
Los datos son proporcionados directamente por el Titular, y hasta que éste no manifieste y acredite lo contrario, se actualizan.	55%
Otros mecanismos.	2%
Se obtienen de evidencia objetiva (documentación oficial como IFE, Cartilla, etc.).	43%

Nota: Esta tabla se basó en el 54% de las Empresas que consideran que cuentan con algún Responsable para establecer Medidas de Seguridad para datos personales y con 51% de la Empresa que registran evidencias objetiva para la obtención de consentimiento del Titular.

La Tabla 14.1 muestra que del 23% de las Empresas que consideran que registran evidencias del consentimiento para la obtención de datos del Titular el 55% (considerando 23% como 100%) son obtenidos directamente del Titular, y hasta que éste no manifieste y acredite lo contrario, se actualizan, él 43% (el 23%

se considera como 100%) considera que obtienen evidencia objetiva (documentación oficial como IFE, Cartilla, etc.), y el 2%(el 23% se considera como 100%) utiliza otros mecanismos

- **Principio de Finalidad**

El Tratamiento de los datos personales únicamente será llevado a cabo en el ámbito de las finalidades señaladas, que de forma clara y concreta se encuentran en el aviso de privacidad; las cuales deberán ser determinadas, explícitas y legítimas relacionadas con las actividades del Responsable.

El objeto de este principio es frenar la oferta de información, regulando a los Responsables de registros o bancos de datos y a los distribuidores (comercializadores) de vender y transferir información que contenga datos personales, sin el consentimiento de los Titulares ya que esta es utilizada para fines distintos a los que originaron la relación entre el Responsable y el Titular. Generando un grado de molestia por parte de los Titulares cuando reciben propagando o llamadas de marketing donde ellos no han proporcionado sus datos.

Este principio obliga al Responsable a cerrar los sistemas de acceso universal y circunscribirlos sólo a aquellas instituciones que evalúen riesgo para el proceso de crédito, los cuales por el ejercicio de sus funciones son regulados por la Ley de Instituciones de Crédito.

En virtud de este principio las Empresas a las cuales se otorga el consentimiento para el Tratamiento de los datos personales, se encuentran obligadas a utilizar los datos únicamente para las finalidades establecidas en el aviso de privacidad, quedándole prohibido su uso para fines distintos.

Así mismo faculta al Titular el derecho de negarse, oponerse o revocar su consentimiento al Tratamiento de sus datos cuando estos sean tratados para finalidades distintas de las que originaron su recopilación.
Para el caso del Tratamiento de datos con finalidades distintas que no resulten compatibles o análogas con las primeras que se hayan establecido en el aviso de privacidad; el reglamento determina que sólo se dará en los casos en que una Ley o reglamento lo permita o el Responsable hubiera solicitado un nuevo consentimiento para el Tratamiento de sus datos con finalidades distintas.

Es necesario que el Responsable elabore un listado del tipo de datos personales que trata en cada actividad y/o procedimiento. Se sugiere que en este ejercicio, el Responsable valore si los datos que trata son los estrictamente necesarios para

alcanzar la finalidad que se persigue, garantizando que los datos solicitados al Titular no sean excesivos, evitándose el Responsable un cúmulo de información innecesaria para las finalidades que persigue.

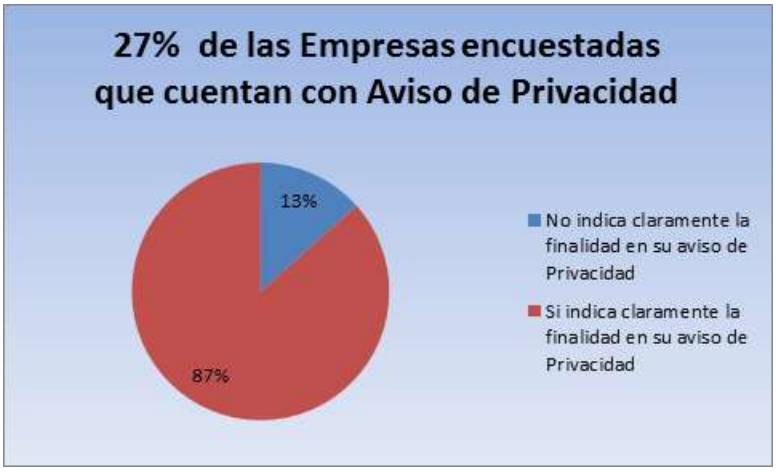
Es muy importante resaltar que en caso de que utilice cookies, web beacons o cualquier otra tecnología o aplicación como fuentes directas para obtener o recabar información personal del Titular es importante lo siguiente:

- Informar al Titular del uso de tal práctica en el aviso de privacidad completo y si el Responsable lo desea puede manifestar las razones que lo conllevan al empleo de estas tecnologías

- Habilitar mecanismos a través de los cuales el Titular, en cualquier momento, tenga la posibilidad de oponerse libremente a que sus comportamientos sean monitoreados por el Responsable.

En este apartado se analizara únicamente al 27% de las Empresas que cuentan con Aviso de Privacidad, para evaluar si sus avisos de Privacidad cumplen con lo que establece la Ley; conforme a la Finalidad del Tratamiento de los datos personales, como lo establecen los Artículos 13 y 14 de la Ley y los Artículos 11 y 27 del Reglamento

Gráfica 15: Principio de Finalidad (%)



La **Gráfica 15**muestra del 27% de las Empresas que cuentan con Aviso de Privacidad, cuales incluyen la Finalidad para la que recaban la información.

De lo anterior se entiende que el 87% de las Empresas que cuentan con Aviso de Privacidad si incluyen la Finalidad en sus avisos; mientras que el 13% restante no lo muestra, por lo cual está incumpliendo con el artículo 16 de la Ley, el cual establece el contenido que debe tener un Aviso de privacidad, siendo la finalidad un requisito indispensable del Aviso; por lo que manifestamos que una de las causas o por lo menos la más lógica del por qué el 13% no muestran la finalidad en su Aviso de Privacidad es porque no se han entendido en su totalidad la Ley.

La **Tabla 15**muestra con base en el 27% de las Empresas que cuentan con Aviso de Privacidad, si la Finalidad que se muestra en su Aviso de Privacidad, indica el tipo de fin Comercio, Publicidad, Mercadotecnia que tendrán los datos recabados.

Tabla 15: Principio de Finalidad (%)

27.15% de las empresas encuestadas que cuentan con Aviso de Privacidad	Indica claramente si el Aviso de Privacidad si su finalidad es Mercadotecnia, Publicidad o Comercial.		
	No	Si	Total general
	6%	21%	27%

El 27% de las empresa que contestaron la encuestas cuentan con aviso de privacidad, de ese 27% solo el 21% su finalidad de almacenar y tratar datos personales está relacionada con Mercadotecnia, Publicidad o Comercial.

El 6% de las empresa que cuentan con aviso de privacidad respondieron que la finalidad con la que almacenan y trata datos personales no está relacionada con Mercadotecnia, Publicidad o Comercial.

En base a lo anterior se puede visualizar que las empresas (Empresa encuestadas) que ya tienen conocimiento sobre la existencia de la ley están procurando cumplir con ella.

En la siguiente tabla se mostrara que porcentaje de empresas no hace mención a la finalidad con la que almacena y trata datos personales en su aviso de privacidad, por lo cual se ha tomado como base el 6% de las empresas que su finalidad de almacenar y tratar datos no está relacionada con Mercadotecnia, Publicidad o Comercial.

Tabla 15.1: Principio de Finalidad (%)

6% de las empresas que en su aviso de privacidad la finalidad es distinta a Mercadotecnia , Publicidad o Comercial	Indica claramente si el Aviso de Privacidad es otra finalidad que no sea Mercadotecnia, Publicidad o Comercial.		
	No	Si	Total general
	4%	2%	6%

La anterior Tabla nos muestra que **el 4 % de las empresas encuestadas que cuentan con aviso de privacidad no indica en su aviso de privacidad la finalidad con la que almacena y trata datos personales.**

Independientemente de las conclusiones obtenidas en los anteriores apartados, podemos concluir conforme a los resultados obtenidos **en este apartado** que solo el 23 % de las empresas encuestadas están cumpliendo con lo que marca la ley

El resto de las empresas encuestadas 77% no cumplen con todo lo que indica la ley, sino solo con algunas partes, la razones principales por la cuales no se cumples son dos, Desconocimiento de la ley, y Falta de entendimiento.

Principio de Lealtad

Lealtad, respetar la expectativa razonable de privacidad.

El principio de lealtad busca garantizar al Titular que el Tratamiento de sus datos será con apego a la Ley y que la información obtenida no será a través de medios engañosos o fraudulentos por parte del Responsable.

El Responsable deberá determinar de manera clara y precisa las finalidades para los cuales recabara los datos personales, ya que de no ser las finalidades informadas en el aviso de privacidad y tratando los datos para finalidades diferentes a las establecidas incurrirá en sanción. Así mismo garantizar que no transferirá los datos personales a persona alguna que no establezca en el aviso de privacidad, avalando la legalidad del Tratamiento.

Una vez que los datos dejan de ser necesarios para los fines recabados los datos deben ser cancelados, dando paso a la eliminación de información relativa a incumplimiento de obligaciones considerándose este el derecho al olvido.

En este apartado analizaremos y verificaremos si las Empresas están aplicando apropiadamente el principio de Lealtad tal y como lo establece el Reglamento en su Artículo 44°

La **Gráfica 16**muestra los Mecanismos utilizados por las Empresas para garantizar el cumplimiento del Principio de Lealtad.

Gráfica 16.- Mecanismos que han implementado las Empresas para garantizar el cumplimiento del Principio de Lealtad (%)

Principio de Lealtad	
Se cuenta con políticas y procedimientos de control interno para la seguridad de datos personales.	64%
Capacitación al personal sobre la Ley y la expectativa de protección y privacidad de los datos personales.	23%
Otra.	13%

De lo anterior se tienen los siguientes Mecanismos que implementan las Empresas encuestadas:

El 64% de las Empresas considera Políticas y Procedimientos de Control Internos para la seguridad de datos personales; considerando a este 64% dentro del cumplimiento de la normativa ya que ha implementado o se encuentra en proceso de implementación de la normativa, lo cual considera una preocupación por la protección de los datos, y garantiza el principio de Lealtad a los titulares de los datos que obran en su posesión, proporcionándoles seguridad y confianza.

El 23% considera Capacitar al personal sobre la Ley y la expectativa de protección y privacidad de los datos personales, este 23% nos muestra un grado de cumplimiento y preocupación por parte de las Empresas al capacitar a su personal en la protección de datos, mecanismo que consideramos fundamental, para el efectivo cumplimiento de la normativa; pues al capacitar a su personal de todos los estratos o por lo menos los más indispensables, es decir aquel personal que de manera directa trate los datos personales de los titulares, se garantiza el cumplimiento de los requerimientos de la Ley y así mismo del principio de Lealtad hacia los titulares de los datos, mostrando un interés por el cumplimiento de la Ley y garantizarle confianza a los Titulares.

El 13% utiliza otros Mecanismos, refiriéndonos como aquellos que cada Empresa considere pertinentes para el cumplimiento de este principio, y que no se

encuentren englobados en las opciones que se dieron en la encuesta, los cuales por políticas de las mismas Empresas, guardan confidencialidad y no se muestran como tales. Mostrando este 13% un escaso grado de interés por el cumplimiento de este principio ante sus Titulares, pues no están considerando como primordiales para el cumplimiento de la Ley, los principales mecanismos para garantizar el principio de Lealtad, pilar básico para ganar la confianza y el prestigio de los Titulares; suponiendo que no hay un grado de comprensión de la Ley por parte de estas Empresas o se encuentren en una falta de interés.

- **Principio de Responsabilidad**

Se entiende como el deber de la entidad o persona Responsable del Tratamiento de los datos, de velar por el cumplimiento de los principios y rendir cuentas al Titular en caso de incumplimiento, independientemente de quién realice el Tratamiento.

El Responsable es el que decide sobre el Tratamiento de los datos, es decir, toma decisiones sobre qué hacer con los mismos, es el Responsable desde que el dato entra a formar parte del sistema de información hasta la eliminación del mismo, es el Responsable durante toda la “vida” del dato.

El Responsable determina, la finalidad, contenido y uso de los datos recabados para cumplir las finalidades que persigue conforme su negocio, para definirlas en el aviso de privacidad.

Además deberá dar respuesta a los ciudadanos cuando éstos ejerciten ante el mismo sus derechos de acceso, rectificación, cancelación y oposición. También deberá adoptar las medidas de seguridad para el Tratamiento de los datos personales que obren en su posesión.

El Responsable garantiza que el aviso de privacidad será respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica, verificando que siempre este actualizado conforme a los establecido en Ley y su Reglamento.

El Responsable establecerá medidas de seguridad que permitan proteger los datos personales contra: Daño, pérdida, alteración, destrucción o el uso, acceso o Tratamiento no autorizado.

Las medidas de seguridad no serán menores a aquellas que mantenga el Responsable para el manejo de su información.

Para la implementación de medidas administrativas técnicas y físicas, el Responsable debe tomar en cuenta:

- El riesgo inherente por el tipo de dato personal
- Las posibles consecuencias para los Titulares
- La sensibilidad de los datos
- El desarrollo tecnológico

Las vulneraciones de seguridad, ocurridas en cualquier fase del Tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los Titulares y serán informadas por el Responsable al Titular de forma inmediata, a fin de que el Titular pueda tomar las medidas correspondientes a la defensa de sus derechos.

Obligaciones del Responsable:

Fase 1. Al momento de recabar los datos personales

1. Dar un uso a los datos personales respetando la ley, desde el momento de su obtención (Principio de licitud).

2. No utilizar medios engañosos o fraudulentos para obtener los datos personales (principio de lealtad).

3. Poner a disposición el aviso de privacidad, de tal manera que el Titular pueda conocer de qué forma serán tratados sus datos personales y cómo podrá ejercer sus derechos ARCO (principio de información).

4. Obtener el consentimiento o autorización del Titular para el Tratamiento de sus datos personales

5. Recabar sólo aquellos datos personales que sean necesarios para las finalidades para las que se obtienen.

Fase 2. Durante el manejo o utilización de los datos personales

1. Utilizar los datos personales respetando la Ley (principio de licitud).

2. Respetar la expectativa razonable de privacidad del Titular, es decir, la confianza que depositó este último en el Responsable, respecto de los datos personales que serán tratados conforme a lo que acordaron y en los términos establecidos por la Ley (principio de lealtad).

3. Limitar el Tratamiento de la información personal al cumplimiento de las finalidades previamente consentidas por el Titular (principio de finalidad).

4. Usar los datos personales que resulten estrictamente necesarios para cumplir con las finalidades para las cuales fueron recabados (principio de proporcionalidad).

5. Mantener los datos personales actualizados y correctos (principio de calidad).

6. Limitar el periodo de conservación de la información personal tratada al mínimo necesario (principio de calidad).

7. Mantener la confidencialidad de los datos personales tratados (deber de confidencialidad).

8. Implementar Medidas de Seguridad de carácter administrativo, físico y técnico que garanticen la confidencialidad e integridad de los datos personales (deber de seguridad).

9. Informar al Titular, sin demora alguna, sobre las vulneraciones de seguridad ocurridas en cualquier fase del Tratamiento que afecten de forma significativa los derechos patrimoniales o morales de éste, en cuanto se confirme la vulneración sucedida (deber de Seguridad).

10. Adoptar las medidas necesarias para cumplir con las obligaciones establecidas en la Ley (principio de Responsabilidad).

11. Rendir cuentas al Titular en caso de algún incumplimiento con relación a la protección de sus datos personales (principio de Responsabilidad).

12. Comunicar los datos personales a terceros nacionales o extranjeros únicamente con la autorización del Titular, salvo las excepciones previstas en la Ley, y hacer del conocimiento de los receptores de los datos personales el aviso de privacidad y las finalidades a las que el Titular sujetó el Tratamiento de su información personal.

Fase 3. Una vez agotadas las finalidades que justificaron el Tratamiento de los datos personales

• Suprimir los datos personales cuando hayan concluido las finalidades que dieron origen al Tratamiento, previo bloqueo (principio de calidad).

• Facilitar el ejercicio de los derechos ARCO. Estos esquemas deberán incluir mecanismos para medir su eficacia con respecto a la protección de los datos personales, así como prever consecuencias y medidas correctivas eficientes en caso de incumplimiento.

La ley establece en su Tercero Transitorio que la asignación del Encargado de Tratamiento se tendrá que hacer efectivo a más tardar un año después de la entrada en vigor de esta. Así, la obligación citada es exigible a partir de julio de 2011, en virtud de que la Ley entró en vigor el 6 de julio de 2010.

Así mismo el Cuarto Transitorio de la Ley establece que la atención de los Derechos ARCO por el Encargado será a partir de enero de 2012, por lo tanto las Empresas deben establecer todos los procedimientos internos para la atención de solicitudes de derechos ARCO entre el 6 de julio de 2011 y enero de 2012, por lo tanto este estudio mide que tanto han implementado las Empresas los procedimientos establecidos.

En este apartado analizaremos sin las Empresa que participaron en la encuesta aplican apropiadamente los Artículos 47 y 48 del Reglamento conforme al Principio de Responsabilidad

Gráfico17: Porcentaje de Medidas que ha implementado el Responsable en la Empresa para garantizar el principio de Responsabilidad%)

Medidas que ha implementado el Responsable	%
Ninguna de las anteriores.	40%
Políticas y programas de privacidad obligatorios	18%
Programa de capacitación y concientización del personal	11%
Revisión de políticas y programas de seguridad	6%
Mecanismos para el cumplimiento de las políticas de privacidad	4%
Procedimientos para recibir y responder dudas y quejas	4%
Destinar recursos para programas de privacidad.	4%
Supervisión y vigilancia interna, auditorías externas	4%
Trazabilidad de los datos personales	3%
Procedimiento tratamiento del riesgo sobre nuevos productos	3%
Acciones técnicas y administrativas que permitan garantizar el cumplimiento con la Ley y el Reglamento.	3%

Tabla 17: Medidas que ha implementado el Responsable en la Empresa para garantizar el principio de Responsabilidad (%)

Medidas que ha implementado el Responsable en la Empresa para garantizar el principio de Responsabilidad	%
Ninguna de las anteriores.	40%
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.	18%
Poner en práctica un programa de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales.	11%
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.	6%
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.	4%
Establecer procedimientos para recibir y responder dudas y quejas de los Titulares de los datos personales.	4%
Destinar recursos para la instrumentación de los programas y políticas de privacidad.	4%
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.	4%
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su Tratamiento.	3%
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.	3%
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al Responsable el cumplimiento de los principios y obligaciones que establece la Ley y el Reglamento.	3%

De lo anterior se tiene que el 40% de las Empresas que cuentan con un Responsable, **no** está aplicando ninguna de las medidas que establece el Artículo 48 del Reglamento, para garantizar el principio de Responsabilidad, mostrando una falta de interés para la protección de datos que obran en su posesión, mientras que el 60% restante (resultante de los porcentajes de cada una de las medidas que por lo menos implementan las Empresas restantes), cuenta con alguna medida implementada para la protección de sus datos, lo cual es positivo debido a que son más las Empresas que muestran interés en la protección de datos personales y se encuentran trabajando en ello, aunque no cuenten con la totalidad de las medidas que establece la Ley.

Tabla 17.1: Medidas que ha implementado las Empresas (Principio de Responsabilidad)

Medidas que ha implementado el Responsable en la Empresa para el principio de responsabilidad	Sin responsable	Persona Interna de la compañía.	Persona moral externa a la compañía.	Responsable
Ninguna de las anteriores.	85%	16%	5%	16%
Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.	5%	22%	30%	29%
Poner en práctica un programa de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales.	0%	18%	15%	19%
Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.	1%	14%	10%	13%
Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.	0%	6%	5%	8%
Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.	2%	5%	0%	8%
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.	1%	5%	15%	3%
Destinar recursos para la instrumentación de los programas y políticas de privacidad.	2%	4%	5%	5%
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento	4%	3%	10%	1%
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	1%	3%	5%	5%
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y el Reglamento	1%	4%	0%	4%

La **Tabla 17.1** muestra que el 85% de las Empresas que no cuentan con un Responsable de Medidas de Seguridad (46%) no están aplicando las medidas que indica el Artículo 48 del Reglamento, por otro lado las Empresas que consideran que si cuentan con algún Responsable para establecer Medidas de Seguridad para datos personales (54%), su tendencia es elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la Empresa

Las principales medidas que deberían tomar la empresa para que los responsables implementen la acción anteriormente mencionada son:

- Debe de haber un compromiso por parte de la Dirección
- Conocimiento y entendimiento de la ley y su reglamento
- Entendimiento sobre la importancia de implementar medidas de seguridad para la protección de datos personales (políticas y capacitación del personal)

Hay que tener claro que cada Empresa tiene una cultura distinta, por tal motivo las medidas que tome la dirección irán de acuerdo al nivel de cultura que se tenga.

El Encargado del Tratamiento

Es la persona física o jurídica que trata los datos personales por cuenta del Responsable, como consecuencia de la existencia de una relación jurídica (contrato de prestación de servicios) que le vincula al Responsable.

Los datos tratados por el Encargado no pueden ser usados para un fin distinto del dispuesto en el contrato, y no pueden ser comunicados a terceros.

Una vez terminada la relación contractual y cumplido los fines para el Tratamiento de los datos, objeto del contrato, el Encargado debe devolver los datos al Responsable o proceder a su destrucción de manera tal que nos los pueda recuperar.

Asignar la protección de datos a un Encargado por cuenta de un Responsable no exime de obligación al Responsable, pues el Responsable estará obligado a responder sobre todo lo relacionado con el desempeño de las funciones asignadas por la Ley al Encargado.

Es indispensable que se formalice la relación con el Encargado mediante un contrato en el que se establezcan las obligaciones de ambos en torno a la protección de datos personales.

Las acciones en materia de privacidad que lleve a cabo el Encargado del Tratamiento de los datos personales coadyuvan a:

- Fortalecer el lazo de confianza entre la Empresa y sus clientes, proveedores, trabajadores, entre otros, al garantizar que la expectativa razonable de privacidad que tienen estas personas sobre su información está siendo respetada por la Empresa, a través de la implementación de prácticas o políticas para tal fin.

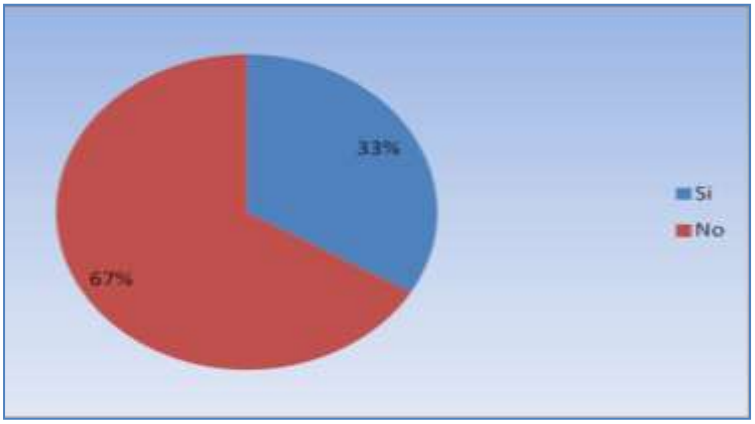
- Dar plusvalía a la calidad del servicio ofrecido, al considerar la privacidad de los clientes o personas como parte de los ejes rectores de sus políticas de servicio y satisfacción.

- Mantener la reputación y posicionamiento de la Empresa en un mercado globalizado.

En este apartado se muestra el porcentaje de Empresas que cuentan con algún prestador de servicios el cual establece la Ley que tendrá la función de Encargado, figura establecida por el Artículo 3 de la Ley, así mismo también

determina sus funciones y obligaciones en los Artículos 49, 50 y 51 del Reglamento

Gráfica 18: Cuenta con prestador de servicios que trate datos personales por cuenta de su Empresa (%)



Cuenta con prestador de servicios que trate datos personales por cuenta de su Empresa.	
Si	33%
No	67%

El 33% de las Empresas cuenta con un prestador de servicios que trata datos personales por cuenta de su Empresa, y el 67% de las Empresa no cuentan con ningún prestador de servicios para tratar los datos personales por cuenta de la Empresa.

Tabla 18.1 Número de Encargados por Empresa (%)

33% de las Empresas que cuentan con algún prestador de servicios que trate datos personales por cuenta de su Empresa.	Cuantos Encargados tratan datos por cuenta de su Empresa		
	1-3	1-5	Más de 5.
	64%	12%	24%

Observamos que del 33% de las Empresas que cuentan con algún Encargado, el 64% tiene de 1 a 3 Encargados, el 12% tiene de 3 a 5 Encargados y el 24% tiene más de 5 Encargados.

3. Tratamiento de Datos Personales en la Nube

Se conoce como “cómputo en la nube” (cloudcomputing en inglés) al modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o software, que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente, de una manera fácil, rápida y con facilidades de servicio a la carta según sean las necesidades del usuario.

Siendo de esta manera un modelo de tecnología que mueve los servicios de computación (software, plataformas o infraestructura) de un medio tradicional (computadora personal, servidores, centros de datos) a internet.

Para el Tratamiento de datos personales en la nube, el Reglamento requiere al proveedor del servicio cumpla con lo siguiente:

a) Cuente con las políticas establecidas por la Ley y su Reglamento para la protección de datos personales

b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio, esto es Conocer la ubicación de la Infraestructura que almacena los datos así como su regulación si se encuentra fuera del país.

c) No condicionar la prestación del servicio a fin de asumir la titularidad o propiedad de la información sobre la que preste el servicio.

d) Garantizar la confidencialidad respecto de los datos personales. Utilizando clausulas claras respecto al uso y confidencialidad de los datos que procesa el Encargado.

e) Contar con mecanismos para dar a conocer cambios en su política de privacidad

f) Permitir al Responsable limitar el tipo de Tratamiento de los datos personales. Asegurándose que el Responsable y el Encargado tengan en claro sus obligaciones.

g) Cuente con medidas de seguridad adecuadas para la protección de los datos. A través de un análisis de riesgos, se puede decidir si el Encargado de Tratamiento mantiene las medidas de seguridad que se requieren.

h) Garantice la supresión de los datos a la conclusión del servicio y garantice que el Responsable no pueda recuperarlos de sus medios.

i) Impedir el acceso a personas ajenas al servicio a los datos personales; Asegurándose el Responsable que sólo él tenga el acceso a sus datos.

El cómputo en la nube representa Ventajas y Desventajas para los Responsables:

Ventajas

Costos: La ventaja más atractiva que presenta el cómputo en la nube al dejar la responsabilidad de la implementación de la infraestructura al proveedor, el cliente no tiene que preocuparse por comprar equipos de cómputo, capacitar personal para la configuración y mantenimiento de éstos, y en algunos casos, por el desarrollo del software.

Competitividad: Las pequeñas Empresas pueden tener acceso a las más nuevas tecnologías a precios a su alcance pagando únicamente por consumo.

Disponibilidad: El proveedor está obligado a garantizar que el servicio siempre esté disponible para el cliente.

Abstracción de la parte técnica: Permite al cliente olvidarse de la implementación, configuración y mantenimiento de equipos; transfiriendo esta responsabilidad al proveedor del servicio.

Acceso desde cualquier punto geográfico: Puede ser accesible desde cualquier equipo de cómputo en el mundo que esté conectado a Internet, incluso desde dispositivos móviles.

Escalabilidad: Las actualizaciones y nuevas funcionalidades son instaladas prácticamente de manera inmediata.

Concentración de esfuerzos en los procesos de negocio: Como resultado de las ventajas antes mencionadas, el cliente pude concentrar más recursos y esfuerzos hacia un aspecto más estratégico y trascendente, que tenga un impacto directo sobre los procesos de negocio de la organización, transfiriendo al proveedor la responsabilidad de la implementación, configuración y mantenimiento de la infraestructura necesaria para que se ejecute la aplicación.

Desventajas

La centralización de las aplicaciones y el almacenamiento de los datos originan una interdependencia de los proveedores de servicios.

La disponibilidad de las aplicaciones está ligada a la disponibilidad de acceso a Internet.

Los datos "sensibles" del negocio no residen en las instalaciones de las Empresas, lo que podría generar un contexto de alta vulnerabilidad para la sustracción o robo de información.

La confiabilidad de los servicios depende de la "salud" tecnológica y financiera de los proveedores de servicios en nube. Empresas emergentes o alianzas entre Empresas podrían crear un ambiente propicio para el monopolio y el crecimiento exagerado en los servicios.

La madurez funcional de las aplicaciones hace que continuamente estén modificando sus interfaces, por lo cual la curva de aprendizaje en Empresas de orientación no tecnológica tenga unas pendientes significativas, así como su consumo automático por aplicaciones.

Seguridad. La información de la Empresa debe recorrer diferentes nodos para llegar a su destino, cada uno de ellos (y sus canales) son un foco de inseguridad. Si se utilizan protocolos seguros, HTTPS por ejemplo, la velocidad total disminuye debido a la sobrecarga que estos requieren.

Una vez establecido lo anterior veremos en qué situación se encuentran las Empresas encuestadas que manejan datos personales en la nube.

Conforme a los datos obtenidos por las encuestas realizadas se obtuvo lo siguiente: El **1.13 %** del total de las Empresas encuestadas manejan computo en la nube por un Encargado, representando un porcentaje muy pequeño, con base en lo anterior analizaremos si cumplen con lo establecido en Ley.

La **Gráfica 19 y Tabla 19** muestran si las Empresas que cuentan con el servicio en la nube o proveen servicios en la nube están cumpliendo adecuadamente con lo que establece el Artículo 52 Fracción I del Reglamento.

Gráfica 19.- Cumplimiento con el Art. 52 del Reglamento de las Empresa que cuentan con servicio en la nube (%)

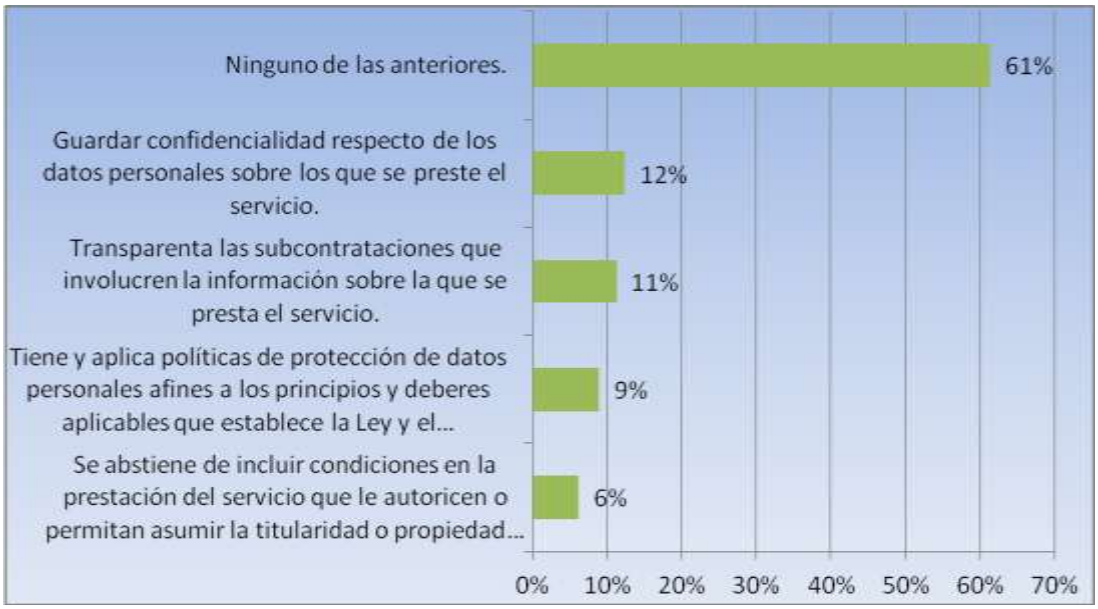


Tabla 19: Cumplimiento con el Art. 52 del Reglamento de las Empresa que cuentan con servicio en la nube (%)

Que controles maneja la Empresa si cuenta con los servicios de la nube su proveedor o la Empresa.	
Ninguno de las anteriores.	61%
Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.	12%
Transparentan las subcontrataciones que involucren la información sobre la que se presta el servicio.	11%
Tiene y aplica políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y el Reglamento.	9%
Se abstiene de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio.	6%

Con base en los datos proyectados por la **Gráfica 19 y la Tabla 19,** se obtiene lo siguiente:

Del **1.13%** del Total de las Empresas encuestadas que cuentan con computo en la nube, el 61% afirma no cumplir con lo que establece el Reglamento en su Artículo 52, para el tratamiento de datos personales en la nube, siendo esta una suposición de las Empresas encuestadas; lo anterior debido a como califican dichas Empresas sus servicios de Computo en la nube; aclarando que no podemos afirmar cierto incumplimiento debido a que no se conocen con certeza, los procedimientos que siguen dichos servicios en la nube, contratados por las Empresas encuestadas. Y es un porcentaje muy pequeño de Empresas las que se presume llegan a cumplir con una o varias obligaciones que establece el Reglamento para el tratamiento de datos en la nube.

Tabla 19.1- Porcentaje de cumplimiento con el Art 52 del Reglamento por Giro de Empresas.

Controles manejados por las Empresas que cuentan o proveen servicios en la nube (De acuerdo a su Giro)	%
Ninguno de las anteriores.	**61%**
Otros Servicios	18%
Pequeña Empresa (imprenta, tintorería, etc.)	13%
Tecnología de la Información	8%
Consultoría de Negocios	7%
Servicios Financieros	3%
Servicios profesionales (médico, dentista, contador)	3%
Consultoría Legal	3%
Comunicaciones y Transporte	2%
Logística	2%
Agropecuaria	2%
Seguros	1%

Salud	1%
Construcción	0%
Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.	**12%**
Tecnología de la Información	6%
Consultoría Legal	1%
Consultoría de Negocios	1%
Otros Servicios	1%
Servicios Financieros	1%
Seguros	0%
Servicios profesionales (médico, dentista, contador)	0%
Salud	0%
Construcción	0%
Pequeña Empresa (imprenta, tintorería, etc.)	0%
Transparentan las subcontrataciones que involucren la información sobre la que se presta el servicio.	**11%**
Tecnología de la Información	6%
Otros Servicios	2%
Servicios Financieros	1%
Seguros	1%
Servicios profesionales (médico, dentista, contador)	0%
Agropecuaria	0%
Comunicaciones y Transporte	0%
Construcción	0%
Consultoría Legal	0%
Tiene y aplica políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y el Reglamento.	**9%**

Tecnología de la Información	5%
Servicios Financieros	2%
Consultoría Legal	1%
Comunicaciones y Transporte	1%
Pequeña Empresa (imprenta, tintorería, etc.)	0%
Otros Servicios	0%
Se abstiene de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio.	**6%**
Tecnología de la Información	3%
Servicios Financieros	2%
Comunicaciones y Transporte	0%
Servicios profesionales (médico, dentista, contador)	0%

En la tabla 19.1 del total de las Empresas encuestadas que cuentan con un proveedor de servicios en la nube, el Giro de Tecnología de Información es el que cuenta con mayor apego a los requerimientos y controles establecidos en el Art. 52 del Reglamento. Reafirmando uno de los supuestos de nuestro estudio en donde se considera que el sector de TI puede proveer servicios como Encargado teniendo mayor cumplimiento y conocimiento de los requerimientos de la Ley.

Los retos más importantes que debe enfrentar la industria ante el cómputo en la nube:

- Estandarización incipiente.- Como resultado de la inmadurez aún no se establecen estándares, ni de facto ni de jure, para la implantación, operación y federación de servicios de cómputo en la nube. Cada proveedor está desarrollando sus propias soluciones, aunque ya hay iniciativas haciendo esfuerzos de estandarización.
- Viabilidad a largo plazo.- ¿Qué pasa si su proveedor de cómputo en la nube es adquirido por otra Empresa, o peor aún, desaparece? Los clientes deberían establecer mecanismos y procesos que les aseguren que sus datos estarán disponibles si eso pasa.

- Portabilidad entre nubes.- Dado que los estándares aún están evolucionando, hoy en día no es tan fácil migrar de una nube a otra en caso de ser necesario.
- Mecanismos de recuperación.- Los planes de recuperación del negocio y de TI, siempre importantes, adquieren mayor relevancia cuando parte de los datos y las aplicaciones están “en algún lugar de la nube”. Es muy importante saber qué previsiones tiene el proveedor para recuperar la operación en caso de fallas en su infraestructura.
- Soporte para análisis forense (técnico y legal).- La investigación de actividades inapropiadas o ilegales puede llegar a ser imposible en un ambiente de cómputo en la nube, tanto por cuestiones técnicas como legales: se requiere que la infraestructura del proveedor permita la vigilancia y recopilación de la posible evidencia, pero también se necesitan mecanismos contractuales y legales que permitan a los clientes el acceso a dicha evidencia
- Legislación inadecuada.- De todos es conocido que la legislación en casi cualquier país suele estar retrasada en lo que tiene que ver con aspectos relacionados a cómputo e Internet. Esto es especialmente notable en el caso del cómputo en la nube, pues se trata de uno de los paradigmas más nuevos.
- Cumplimiento regulatorio y jurisdicción.- Este es un tema fundamental que no debe ser soslayado y que corre el peligro de ser ignorado pues más que una cuestión técnica se trata de un asunto legal. Finalmente los clientes son los responsables de la seguridad y la integridad de sus datos, aún si estos están con un proveedor de servicios, y en un modelo de cómputo en la nube hay dos grandes preocupaciones:
    - ¿Cómo se puede auditar y certificar a un proveedor de servicios de cómputo en la nube, sobre todo de cara al cumplimiento regulatorio?
    - Dado que el cliente puede no saber dónde están sus datos ¿cómo saber si se están infringiendo leyes sin saberlo (por ejemplo, al permitir que los datos del cliente sean almacenados en países en los que las regulaciones legales lo prohíben)?
- Seguridad de la información.- De acuerdo a lo dicho líneas arriba, el mantenimiento de la famosa CIA (confidencialidad, integridad y disponibilidad) de la información es uno de los temas más relevantes: “…los expertos dicen que el modelo de cómputo en la nube sigue siendo inmaduro y tendrá que demostrar un alto nivel de seguridad que satisfaga a la mayoría de los usuarios empresariales” (ComputerWeekly, septiembre 2009). Algunos de los temas que más hay que cuidar al respecto son los siguientes:
    - Acceso privilegiado (Privilegeduseraccess). ¿Cómo se asegura que personal no autorizado, tanto del cliente como de otros clientes y del propio proveedor, no tendrá acceso a los datos?

- Localización de los datos (Data location). Ya se habló de esto en la parte de cumplimiento regulatorio y en resumen la preocupación se centra en cómo lograr que los proveedores mantengan y procesen los datos en jurisdicciones específicas y cómo lograr que acepten el cumplimiento de leyes y regulaciones locales que son de relevancia para sus clientes.
- Segregación de los datos (Data segregation). En ambientes de cómputo en la nube, por su propia naturaleza, los datos de los clientes comparten una infraestructura común. Es por ello que los clientes deberían pedir evidencia de que su información está cifrada y segregada de los datos de otros clientes.
- Falta de estrategia de seguridad.- Como siempre, no todo es responsabilidad de los proveedores. De acuerdo a IDC, más del 30% de las grandes corporaciones en Estados Unidos tienen datos o aplicaciones en la nube, pero dos tercios de ellas no tienen una estrategia de seguridad para el cómputo en la nube.

El cómputo en la nube es una de las principales tendencias del desarrollo de aplicaciones computacionales debido a que permite incrementar el número de servicios que se ofrecen, lo que genera beneficios tanto para los proveedores de aplicaciones como a los consumidores de las mismas, además de que ofrece ventajas únicas como la inmediatez y transparencia en los servicios.

Análisis Comparativo

En la siguiente tabla, se muestra un análisis comparativo sobre el nivel actual de cultura de la LFPDPPP en México, comparado con estudios realizados por INTECO (Instituto Nacional de Tecnologías de la Comunicación) en España.

Aclarando que el nivel deseable se obtuvo haciendo un comparativo entre los resultados obtenidos de la encuesta realizada y los resultados de los estudios consultados de INTECO, realizando un énfasis en que los niveles deseables que se requieren para México dependerán de su nivel de madurez que arrojo la encuesta conforme a su nivel de cultura sobre la Ley.

El nivel deseable se obtuvo tomando como base la madurez actual que presenta México, sobre la cultura de la Ley siendo este muy bajo; por ejemplo Alemania presenta un nivel de cultura superior al de México, considerando el tiempo que tiene implementada la Ley de Privacidad, por tal motivo su nivel deseable de madurez recomendado seria de un 97% considerando que ya cuenta con un nivel de conocimiento y cumplimiento de la Ley más avanzado que en México, por lo cual su nivel deseado debe superar el que tiene actualmente, siendo para Alemania más fácil llegar al 100% tomando en cuenta su nivel de madurez actual sobre la Ley.

Por tal motivo los niveles deseables que se requieren para México son mínimos, no pudiendo exigir un 100% como nivel deseable para México, considerando su bajo nivel de cultura.

Análisis Comparativo		
Aspecto Analizados	**Nivel Actual**	**Nivel Deseable**
Conocimiento y Entendimiento de la Ley	8%	66%
Aviso de Privacidad	27%	65%
Principio de Finalidad	23%	60%
Figuras o Procedimientos definidos		
Las Empresas cuenta con la Figura de Responsable	28%	51%
Procedimiento de Ejercicio de Derecho ARCO	8%	60%
Medidas de Seguridad		
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.	8%	60%
Calidad de Datos		
Los datos son proporcionados directamente por el Titular, y hasta que éste no manifieste y acredite lo contrario, se actualizan.	53%	80%
Principio de Responsabilidad		

Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.	4%	50%
Establecer procedimientos para recibir y responder dudas y quejas de los Titulares de los datos personales.	4%	50%
Destinar recursos para la instrumentación de los programas y políticas de privacidad.	4%	50%
Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.	4%	50%
Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su Tratamiento.	3%	50%
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.	3%	50%
Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al Responsable el cumplimiento de los principios y obligaciones que establece la Ley y el Reglamento.	3%	50%

Debido al bajo nivel de cultura de la Ley, que presentan las Empresas en México se exigen niveles considerables, para escalar un nivel de cultura óptimo para la protección de datos y para poder alcanzar los niveles de los países de la Unión Europea (normativa de la cual México ha tomado las bases para adecuar su Ley de Protección de Datos Personales.)

Justificadamente podemos inferir en que el nivel de cultura en México sea bajo debido a la reciente entrada en vigor de su Ley, lo cual explica su desconocimiento por parte de las Empresas y de los individuos. Aunado a su escaza difusión entre la población.

El IFAI tiene como objeto principal difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana, promover su ejercicio y vigilar por la debida observancia de las disposiciones previstas en la ley y que deriven de la misma; en particular aquellas relacionadas con el cumplimiento de obligaciones por parte de los sujetos regulados por el ordenamiento.

Además se le otorgará como función principal: difundir el conocimiento de las obligaciones en torno a la protección de datos personales entre la iniciativa privada nacional e internacional con actividad comercial en territorio mexicano; y promover las mejores prácticas comerciales en torno a la protección de los datos

personales como insumo de la economía digital y el desarrollo económico nacional en su conjunto.

Como parte de las acciones que el IFAI ha implementado para la difusión y entendimiento de la Ley; en su página de internet ha elaborado guías de ayuda para el conocimiento de la Ley a la población en general, así como para las Empresas, para auxiliarlas en la implementación de la Ley de una forma clara, sencilla y de fácil entendimiento para cualquier tamaño de Empresa.

Así mismo ha difundido en los medios de comunicación comerciales sobre la importancia de cumplir con la Ley, dirigido tanto a Empresas como a la población en general. Lo cual denota la preocupación por parte de este Instituto en difundir la protección de datos, lo cual muestra un avance significativo pero hace falta más interés por parte de Empresas Privadas como de la población en general.

En cuanto a la Ley se denota su estricto nivel de cumplimiento al establecer sanciones a las Empresas en caso de incumplimiento:

En materia de infracciones, la LFPDPPP otorga al IFAI la facultad de imponer sanciones a los particulares que van desde un apercibimiento hasta multas desde los 100 hasta 320,000 días de salario mínimo vigente en el Distrito Federal, con doble imposición para los casos de reincidencia, las cuales pudieran duplicarse en aquellos casos de infracciones relativas a datos personales sensibles.

Por otra parte, la LFPDPPP introduce la tipificación de delitos en materia del tratamiento indebido de datos personales, con penas que podrán ser desde los tres meses hasta los cinco años de prisión.

La LFPDPPP, presenta ciertas contradicciones y lagunas en cuanto a su contenido por lo cual hace falta mucho por legislar en materia de protección de datos.

Por ejemplo presenta contradicciones en cuanto a que **no son definitivas las resoluciones dictadas por el IFAI**, ya que la LFTAIPG que regula las funciones del Instituto, en su artículo 59° determina que *"Las resoluciones del Instituto serán definitivas para las dependencias y entidades. Los particulares podrán impugnarlas ante el Poder Judicial de la Federación."* Mientras que la LFPDPPP en su artículo 56° determina que *"Contra las resoluciones del Instituto los particulares podrán promover el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa."*

Lo cual resulta una decisión desafortunada por parte del legislador, el haber otorgado a un Tribunal Contencioso Administrativo dependiente del Poder Ejecutivo, la facultad de dictaminar en última instancia de aquellos actos que materialmente son jurisdiccionales, no administrativos; como es el caso de las resoluciones emitidas por el IFAI, las cuales se dictan, dada su naturaleza y definición, para resolver las controversias entre particulares respecto al tratamiento de datos personales y no como actos propios de autoridad que pudieran considerarse administrativos.

Para el caso de las Infracciones y sanciones que establece la Ley, no se establece una gradación o clasificación de las infracciones en que se pueden incurrir (leves, graves o muy graves) pero si se establece la forma en la cual el IFAI fundamentará y motivará sus resoluciones tomando como base la naturaleza del dato, la improcedencia de la negativa del Responsable del tratamiento de datos, la intencionalidad de las acciones y omisiones cometidas, las capacidad económica del infractor o su reincidencia, según el procedimiento fijado para tal efecto.

En lo que respecta a la determinación de la cuantía de las sanciones, resultaría más adecuado atender a la naturaleza de los derechos personales que se afecten por alguna omisión o acción, pues el dato en sí mismo no puede ser afectado, sino los derechos de su titular.

De igual forma habría que considerar con independencia del tratamiento que se le haya dado a dichos datos, el beneficio real obtenido por el Responsable a efecto de determinar efectivamente el grado de antijuricidad y de culpabilidad presente en la concreta actuación infractora.

Por contrapartida y en razón de circunstancias que pudieran concurrir en conductas no intencionadas, la autoridad sancionadora debería apreciar una cualificada disminución de la culpabilidad del imputado o de la antijuricidad del hecho, aplicando la escala relativa a la clase de infracciones que preceda en gravedad a aquella en que se integra la considerada en el caso particular.

Para la prescripción de las infracciones cometidas durante el tratamiento de datos personales, falta definir los límites de sanción para el caso de que transcurra determinado tiempo sin que dé comienzo el procedimiento sancionador, pues en el texto legal no se advierte la regulación de las condiciones para que tenga lugar la prescripción de las infracciones a que se hace referencia. Se entiende que la autoridad tiene un plazo indefinido para iniciar procedimientos sancionadores e imponer las penas correspondientes.

Delitos

En materia de delitos relacionados con el uso de las tecnologías de la información, la legislación mexicana ha sido omisa en demasía respecto a su tipificación, pues los que se mencionan se hacen de manera implícita y se contiene en diversas legislaciones sin encontrar una coherencia normativa en su regulación.

Los evidentes progresos globales en materia computacional acompañados con el creciente aumento de la capacidad de almacenamiento y procesamiento de distintas bases de datos, en particular aquellas en posesión de particulares que contienen datos personales ponen en relieve el desarrollo actual de la era de la información.

Por ello se han venido dando una serie de comportamientos antes impensables y en algunos casos difíciles de tipificar conforme a las normas penales tradicionales: la intangibilidad de la información como valor fundamental de la nueva sociedad y bien jurídico a proteger; el desvanecimiento de teorías jurídicas como la relación entre acción tiempo y espacio; el anonimato que protege al delincuente informático; la dificultad de recolectar pruebas de los hechos delictivos de carácter universal del delito informático; las dificultades físicas, lógicas y jurídicas del seguimiento, procesamiento y enjuiciamiento en estos hechos delictivos; la doble cara de la seguridad, como arma de prevención de la delincuencia informática y a su vez como posible barrera en la colaboración con la justicia. Todas ellas son cuestiones que caracterizan a este nuevo tipo de delitos y que requieren respuestas jurídicas.

Dando como resultado que el tratamiento de los datos personales tratados por terceros sea insuficientemente tipificado por la LFPDPPP, pues no va a la par con el desarrollo de las TI, si consideramos que la sola puesta en riesgo o vulneración de las bases de datos que los contengan no constituye una afectación directa al bien jurídico tutelado, ni el simple engaño para su obtención, pues la tipicidad requiere necesariamente de un daño efectivo en los derechos tutelados.

Delitos informáticos en perjuicio de los titulares de los datos personales considerados por la ONU:

Fraudes cometidos mediante manipulación de computadoras:

- Manipulación de los datos de entrada
- Manipulación de programas
- Manipulación de datos de salida
- Fraude efectuado por manipulación informática

Falsificaciones informáticas:

- Utilizando sistemas informáticos como objetos
- Utilizando sistemas informáticos como instrumentos

Daños o modificaciones de programas o datos computarizados:

- Sabotaje informático
- Virus
- Gusanos
- Bomba lógica o cronológica
- Acceso no autorizado a sistemas o servicios
- Piratas informáticos o hackers
- Reproducción no autorizada de programas informáticos con protección legal

Con base a lo anterior la LFPDPPP debería considerar la extraterritorialidad y transnacionalidad de los delitos que se cometen a través de las Tecnologías de la Información instrumentando una protección jurídica adecuada respecto a los datos personales, y no sólo dejar a éstos la responsabilidad penal respecto de un mal tratamiento de los mismos.

Por ello, será muy importante que se conozca el efecto que estas nuevas disposiciones tendrán en la operación de las empresa y aprovechar los plazos que la Ley otorga para su cumplimiento.

Es preciso seguir de cerca el desarrollo y aplicación que la misma tendrá, así como los criterios, observaciones y recomendaciones que el IFAI, con apoyo de la Secretaría de Economía, estime conveniente. Para lo cual se han puesto a disposición los links de las guías que han expedido estos organismos para su mayor conocimiento y que ayuden a fomentar la cultura de la protección de datos en México y exigir su cumplimiento.

Guía práctica para ejercer el derecho a la Protección de Datos Personales: http://inicio.ifai.org.mx/Publicaciones/01GuiaPracticaEjercerelDerecho.pdf

Guía práctica para la atención de las solicitudes de ejercicio de los Derechos ARCO: http://inicio.ifai.org.mx/Publicaciones/02GuiaAtencionSolicitudesARCO.pdf

Guía práctica para generar el Aviso de Privacidad:
http://inicio.ifai.org.mx/Publicaciones/privacidadguia.pdf

Tríptico: Lo que tienes que saber acerca de Ejercicio de los Derechos ARCO: http://inicio.ifai.org.mx/Publicaciones/Tripticoejercicioderechos.pdf

Tríptico: Lo que tienes que saber acerca de La Protección de tus Datos Personales: http://inicio.ifai.org.mx/Publicaciones/TripticoWeb.pdf

Tríptico: Lo que tienes que saber acerca de Aviso de Privacidad: http://inicio.ifai.org.mx/Publicaciones/folletoAviso.pdf

Tríptico: Lo que tienes que saber acerca de La atención de los Derechos ARCO:http://inicio.ifai.org.mx/Publicaciones/Tripticoatencionderechos.pdf

Beneficios para las empresas

Como se mencionó anteriormente la Ley surge para proteger el derecho de autodeterminación informativa de las personas, sin embargo es importante mencionar que beneficios y ventajas obtienen las empresas al Implementar esta Ley.

Beneficios

- Mitiga los riesgos e impactos del incumplimiento de la LFPDPPP y su Reglamento y establecer controles para la protección de datos de carácter personal.

- Proporciona ventaja competitiva como empresa de cara a posibles colaboraciones o trato con terceros.

- Genera confianza a los clientes, proveedores y terceras partes implicadas, asegurando la protección de sus datos personales y, sobre todo, que no se hace uso indebido de los mismos. Lo anterior aporta una imagen de seriedad y profesionalismo que incrementa el valor y la reputación de la organización.

- Reduce el riesgo de pérdida, mal uso, y/o extracción indebida de información.

Ventajas

- Garantiza el pleno ejercicio de los derechos de las personas.
- Compromiso de confidencialidad por parte de los empleados y subcontratistas respecto de los datos que conozcan y traten por motivo de su trabajo, esto es una garantía también para los clientes, proveedores, administraciones y terceras partes implicadas.
- Mejora la imagen y la reputación, y la relación con terceros
- Minimiza los costos al mitigar los riesgos detectados

Conclusiones

A continuación se presentan un concentrado de las principales conclusiones de los apartados tratados anteriormente y que tuvieron mayor relevancia, posteriormente se señalan las barreras que tienen las Empresas Privadas para implementar la Ley, las conclusiones del estudio en general y Recomendaciones.

Perfil del Encuestado:

Con base en las Gráficas y Tablas mostradas en el apartado de **Perfil del Encuestado** se concluye lo siguiente:

De las 221 Empresas que participaron el 52% fueron del Distrito Federal y el 48% Foráneas, en el estudio se muestra que las Empresas que tuvieron mayor participación fueron las Micro Empresas con un 66% de participantes, las Pequeñas con un 19%, las Medianas con un 7% y las Empresas Grandes una participación del 8%. El Giro que mayor partición tuvo en el estudio fue el de Tecnologías de Información con 24% mostrando un porcentaje igual el de Otros Servicios sin embargo este último engloba servicios diferentes a los identificados en la encuesta.

Conforme al cargo que ocupan los encuestados participantes son de la Dirección General presentando un 33% de participación en Entidades Federativas; por parte de las Empresas del Distrito Federal el cargo que tuvo mayor participación fue el de Analista con un 24%. Conforme al total de encuestados tanto Empresas Foráneas como las del Distrito Federal los cargos que presentaron mayor participación en la encuesta son: Dirección General con 26%, Analista con un 20% y la Gerencia con un 19%.

Tipos de datos que manejan las Empresas

El 65 % de las Empresas manejan dos tipos de datos principalmente según la clasificación por Ley siendo estos datos Básicos, Financieros y patrimoniales, el 31% maneja datos Básicos y sólo el 4% de las Empresas trata datos Básicos, Financieros y Patrimoniales, y Sensibles.

Del total de las Empresas encuestadas el 53% almacena sus datos personales en Papel, mientras que el 45% de las Empresas almacena sus datos personales en medios Electrónicos. Por lo anterior es relevante mencionar que aun encontrándonos en una era de avances tecnológicos, la mayoría de las Empresas sigue almacenado los datos personales en medios no automatizados como lo es el Papel, es importante señalar que esta misma tendencia se presenta en países europeos como España.

No se registraron Empresas que manejaran únicamente datos Básicos y Sensibles, como podrían ser los del sector salud.

Figuras o Procedimientos definidos dentro de las Empresas.

El 69% de las Empresa consideran que cuenta con alguna Figura o Procedimiento definido tal y como estable la Ley y solo el 31% consideran que no cuentan con alguna Figura o Procedimiento definido.

Las Principales razones de que el 31% de las Empresas consideren que no cuentan con alguna Figura o Procedimiento definido son las siguientes:

- El 27% de las Empresas es por Desconocimiento de la Ley y su Reglamento.
- El 2.4% de las Empresas es por Falta de Entendimiento de la Ley.
- El 1.3% de las Empresas es por Falta de Compromiso de la Administración.
- El 0.5% de las Empresas es por Otra razón,

Del 52% de las Empresas que consideran que cuenta con alguna Figura o Procedimiento definido (No se incluye a las Empresas que cuentan con la Figura de Titular) solo el 8% consideran que cuentan con el procedimiento de Atención a Derecho ARCO.

Por tal motivo se concluye que solo el8% de las Empresas que tratan datos personales respondieron que consideran lo que establece la Ley y su Reglamento para el ejercicio de derechos ARCO.

El análisis anterior muestra que el giro de Tecnología de Información es el que mayor porcentaje de inclusión de Figuras y Procedimientos tiene conforme a la Ley, no obstante hace falta reforzar sus procedimientos para atención de Derechos ARCO.

Observamos que los únicos giros que cuentan con Listado de exclusión son el de Tecnologías de Información y Consultoría Legal con un 1%, mientras que para la atención de Derechos ARCO el giro de Tecnología de Información se encuentra en el tercer lugar con 1.7 siendo el giro de Consultoría Legal el que se encuentra en primer lugar con 2.91 %, siguiéndole el giro de Servicios Financiero con un 2.26%.

Es importante destacar que en relación a la Figura de Responsable, el giro de Tecnología de Información se encuentra en el primer lugar con 8.81%, en segundo lugar el de Consultoría Legal con 5.01% y en tercer lugar Otros Servicios el de con 3.88%.

Medidas de Seguridad

El 54% de las Empresas encuestadas consideran que desarrollan Medidas de Seguridad conforme a lo establecido en la Ley, de estos el 49% deja esta Responsabilidad a personal interno (incluyendo Responsable), y únicamente el 6% encarga estas medidas a una persona moral externa a la Empresa, destacando que el 46% restante de las Empresas encuestadas no identifica a un Responsable para las Medidas de Seguridad faltando al artículo 19 de la Ley, y al artículo 59 del Reglamento.

El Responsable, el Personal Externo y el Personal Interno de la Empresa tiene una mayor tendencia a tomar acciones como: Elaborar inventarios de datos personales y de los sistemas de Tratamiento.

Asimismo, estos prestan poca atención a capacitar al personal que efectúe el Tratamiento de datos personales. (Responsable 5%, Personal Externo 1% y Personal Interno 7%).

Cabe señalar que mientras el Personal Externo a la Empresa toma interés alto en el Establecer las Medidas de Seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva con 22%, el Responsable muestra un interés del 3% y el Personal Interno 5%.

La conclusión sobre este apartado es que los Responsables carecen de los conocimientos adecuados para aplicar la LFPDPPP.

De las Empresas que cuentan con un Responsable para mantener Medidas de Seguridad se determinó que el 51% considera cuenta con algún procedimiento para notificar que hubo una vulneración de seguridad equivale al 28% del total de Empresas.

Las disposiciones que establece la Ley son desconocidas o no han sido entendidas para la mayor parte de las Empresas, debido a los resultados de la encuesta muestran que el 60% de las Empresas que recaban datos de carácter Básico lo hacen mediante consentimiento expreso y por escrito, cuando por Ley sólo se requiere consentimiento tácito, y en forma contraria para recabar los datos de carácter Sensible la encuesta muestra que el 80% de las Empresas utilizan el consentimiento tácito en lugar del expreso y por escrito como requiere la Ley.

En este apartado de la encuesta los encuestados mostraron un sesgo significativo ya que como veremos más adelante carecen de los avisos de privacidad.

En algunos casos el guardar evidencias han sido debido a los registros de entrada a las instalaciones de las Empresas y a la documentación que deben conservar para para las relaciones contractuales.

Aviso de Privacidad:

El 73% de las Empresas **no cuentan con Aviso de Privacidad**, solo el 27% cuentan con **Aviso de Privacidad.**

Del 27% de las Empresas que tienen Aviso de Privacidad:

- El 30% define la identidad y domicilio del Responsable.
- El 26% tiene la finalidad del Tratamiento de datos.
- Sólo el 2% identifica el procedimiento y medio por el cual el Responsable comunicará a los Titulares de cambios al aviso de privacidad

En relacionado a la forma en que se da a conocer el Aviso de Privacidad:

- El 28% da a conocer el Aviso de Privacidad por medio visuales.
- El 25% da a conocer el Aviso de Privacidad a través de portal o página de internet.
- Sólo el 2% da a conocer el Aviso de Privacidad a través del teléfono viva voz o grabación en la contestadora telefónica (IVR) (medios sonoros).

Estos datos refleja que aun contando con Avisos de Privacidad estos son inadecuados en su gran mayoría.

El 27% de las Empresas que cuentan con Aviso de Privacidad solo el **23% muestra claramente la Finalidad (Publicidad, Mercadotecnia, u Otras) con la que trata su datos Personales en su Aviso de Privacidad.**

El giro que cumple mayormente con el Aviso de Privacidad es el Tecnología de Información con un 11.76%, siguiéndole el de Consultoría Legal y de Negocios con 3.17%.

Barreras que tienen las Empresas Privadas para implementar la Ley

Tal y como se ha mostrado a lo largo de este estudio, la situación de las 221 Empresas encuestadas, tanto Empresas Privadas y las PYME en lo que se refiere al nivel de cultura e implementación de la Ley, aplican inadecuadamente la normativa: De acuerdo a los resultados del apartado de Medidas de Seguridad el 47.5% de las Empresas "No entienden la Ley" y el 27.1% de las Empresas" Desconocen la Ley y su Reglamento

En el presente estudio se analizan las barreras con los que se encuentran las Empresas Privadas en su proceso de adopción a la normativa, así como los beneficios y valor añadido que la implementación aporta al negocio.

Barreras a la adopción

Falta de sensibilidad hacia la necesidad de proteger los datos personales y desconocimiento de la ley.

Las Empresas, no conocen la importancia y necesidad de proteger los datos de carácter personal y no entienden el porqué de una normativa sobre protección de datos. Este hecho hace que desconozcan en gran medida la LFPDPPP y el RLFPDPPP.

En ocasiones, es posible que las Empresas tengan conocimiento de la existencia de una Ley, pero desconocen la obligatoriedad de la misma y/o las consecuencias de su incumplimiento.

Este desconocimiento y falta de sensibilización afecta incluso a la consideración de qué son datos personales y no tienen cierta relevancia, existen Empresas Privadas que, por no conocer el ámbito objetivo de aplicación de la normativa, no se consideran afectadas, olvidando que los principios generales del derecho enuncian: el desconocimiento de la Ley no exime de su cumplimiento.

El Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), y la Secretaría de Economía, se encuentran realizado labores informativas y de sensibilización sobre la protección de datos personales por los distintos medios de comunicación, para su difusión y conocimiento para todo el público en general.

Otras de las circunstancias por la cual México cuenta con una Escasa cultura sobre la Protección de datos personales es el alto índice de Piratería.

La BSA (Business Software Allian) realizo un estudió en donde muestra la piratería de software que hay a nivel mundial, en donde destaca el alto grado de porcentaje de Usuario en la Latinoamérica que acepta comprar Software sin licencias.

Latinoamérica cuenta con un promedio de Piratería en Software entre 2007 a 2011 de un 61% y mientras que la Unión Europea cuentan con un promedio de 33% entre 2007 a 2011.

El 61% de los Usuarios que Hacen uso de Software, lo hacen sin licencia.
Link donde se pude encontrar el Estudio de la BSA en:

http://portal.bsa.org/globalpiracy2011/downloads/translatedstudybrief/2011GlobalPiracy_InBrief_es.pdf

La Unión Europea cuenta con un bajo porcentaje de piratería, lo cual incide en que cuentan con un alto grado de madurez referente a la cultura de protección de datos. El tener un Madurez sobre la Protección de Datos ha ayudado a disminuir el tráfico de datos que se da en la piratería.

El constante cambio tecnológico, muestra el rumbo a los negocios modernos en México y en todo el mundo, aunque las implicaciones y resultados de su impacto sobre el cambio o la reinvención de las empresas, facilitados por la TI, están aún pendientes de demostración científica.

Hay dos variables fundamentales que impactan sobre la sostenibilidad de la privacidad en las empresas. Estas variables son el clima (ambiente) y la cultura de la organización

El clima está más basado en el conocimiento individual (percepciones) y la cultura es ampliamente previa al conocimiento, o más relacionada con valores implícitos, actitudes y creencias.

Existirá congruencia entre la cultura y el clima si los comportamientos clave para la privacidad se combinan con estos dos conceptos clave en todos los niveles empresariales.

Lo anterior ayudará a comprender el tema de la privacidad en todos los niveles organizativos de una Empresa desde los niveles Directivos hasta los últimos niveles, cubriendo todos los niveles de la Empresa, tanto en los contextos académicos como en el sector empresarial.

De este modo, esta característica única acelera la portabilidad y comprensión de los valores, actitudes y percepciones de la privacidad, que pueden implantarse por todos los niveles de clima y cultura de una Empresa.

Rechazo al cambio

Incluso en el caso de conocer la normativa, existe en las Empresas un rechazo a las iniciativas de control. La adaptación a la legislación sobre protección de datos supone un cambio en la organización de la información que afecta a tareas, conceptos, procesos y mecánicas de trabajo. En general, las Empresas que se encuentran en proceso de adaptación a la normativa sobre protección de datos lo perciben como una imposición o una carga y no como algo que aporta valor a su negocio.

Por ello, las medidas de sensibilización a implementar deben tener en cuenta esta circunstancia, haciendo énfasis en el valor añadido que la normativa aporta al negocio y que la adaptación al cambio requiere un esfuerzo inicial que a medio y largo plazo es sencillo de manejar.

Limitación de recursos (económicos, humanos y tiempo)

Puede darse el caso de Empresas que conocen la normativa y no muestran un rechazo frontal al cambio que supone, no obstante, reconocen una limitación de recursos necesarios para su correcta implementación. Se podría decir que, junto con el desconocimiento de la normativa, éste es el motivo que en mayor medida frena a las Empresas a la hora de la adaptación; por otra parte, las Empresas que cuentan con recursos para la implementación de la normativa muestran desinterés en la protección de datos personales derivado de la aparente licitud por parte del las Instituto (IFAI) para la aplicación de sanciones.

Las Empresas por lo general, consideran que el gasto que supone la labor de adaptación (consultoría, si optan por esta opción, y medios materiales como soportes de almacenamiento, control de acceso lógico, cifrado, etc.), es excesivo e innecesario, en tanto en cuanto no les reporta un valor añadido inmediato.

Del mismo modo, al tratarse de algo que consideran complejo, consideran que no disponen de personal con suficientes conocimientos técnicos en la materia, y por tanto se plantean la necesidad de contratar a alguien específico.

Al excesivo costo percibido y la falta de recursos humanos cualificados se une el tiempo de adecuación, que en toda lógica, se desvía de la actividad principal del

negocio para destinarse al cumplimiento de la normativa sobre protección de datos. En general, se percibe como una tarea tediosa que exige desviar recursos de la actividad principal del negocio.

Por ello, es necesario que en la labor difusora del IFAI se tenga en cuenta esta circunstancia, para instruir de forma objetiva acerca de los costos, tiempo y recursos humanos necesarios para la implementación de la Ley, y facilitar pautas para maximizar la efectividad.

Errónea implementación de la normativa

De los casos en los que algunas Empresas han implementado la Ley, ésta se ha llevado acabo de **forma inadecuada**, pues aunque se ha invertido en los medios necesarios para su implementación; y que esto es bueno debido a que muestra compromiso por las Empresas para cumplir con sus obligaciones, no están en situación completamente ajustada a la Ley, la razón más significativa sería su **falta de conocimiento en el tema de privacidad aunado a la escasa interpretación de la Ley**, factores que influyen de manera significativa y que frenan el cumplimiento de la normativa.

De igual forma se denota una falta de conocimiento profundo por algunos prestadores de servicio de consultoría que aprovechan el desconocimiento del tema de las Empresas y venden servicios de implementación de controles parciales. Recomendamos que se evalué a las Empresas que prestan este tipo de servicios para que cuenten con la preparación necesaria y el reconocimiento del Instituto o Autoridad a cargo, a fin de apoyar a las Empresas en la implementación de los controles requeridos conforme a la Ley.

Beneficios derivados de la implementación

Reconociendo la existencia de las barreras anteriormente descritas, e insistiendo en la necesidad de implementar medidas para minimizarlos, es necesario puntualizar que la adopción de la Ley aporta una serie de beneficios que se traducen en un valor añadido para la Empresa. Por ello, las acciones de concienciación y formación deben ir encaminadas a la exposición de las ventajas derivadas de la adopción de la normativa sobre protección de datos.

El valor de los datos

Los datos personales son valiosos en sí mismos. La tendencia actual es a considerarlos un activo más de la Empresa. Los datos son información, y la

información es valiosa. Por ello, es necesario hacer un esfuerzo por proteger los datos para garantizar su confidencialidad e integridad (interna y externa) y evitar posibles incidencias de seguridad: pérdida, fuga o robo de información que puede hacer llegar los datos a personas inadecuadas (Empresas de la competencia, medios de comunicación, empleados malintencionados…). Un incidente de este tipo puede tener consecuencias muy negativas para la Empresa, y en ocasiones los empresarios no se han planteado las consecuencias ante la pérdida de una base de datos de clientes, proveedores o empleados.

Aumento de calidad en las operaciones

La adaptación de las Empresas para el cumplimiento de la Ley contribuye a mejorar los procesos de manejo de la información, ya que proporciona una cultura de calidad en el Tratamiento de los datos y la gestión del negocio que puede trasladarse a otros procesos de la Empresa. Una cuestión tan básica como poner en orden la información contribuye en ocasiones a detectar problemas o carencias del negocio.

Mejora de la imagen corporativa

El cumplimiento de la Ley de protección de datos garantiza la confidencialidad y el derecho a la intimidad de los Titulares de los datos. En este sentido, es una referencia y garantía de seriedad y confianza por parte de las Empresas, principalmente hacia clientes y proveedores, pero también a Empresas de la competencia. Las Empresas privadas se verán en la necesidad de adaptarse a la Ley ante la solicitud de alguno de sus clientes, o ante la petición por parte de otras Empresas pertenecientes a su mismo sector de actividad. Por tal motivo implementar la Ley por parte de las Empresas será beneficioso para la propia imagen y una manifestación de la responsabilidad social corporativa.

Es una garantía individual

La protección de datos es una garantía individual establecida en la Constitución de los Estados Unidos Mexicanos que ampara a todos los ciudadanos, y para garantizar su efectividad las Empresas han de cumplir las disposiciones previstas en la Ley. De lo contrario, pueden verse afectadas por denuncias o sanciones. El IFAI, como órgano competente declarado en la Ley, tiene las atribuciones necesarias para realizar verificaciones y sancionar a los que incumplen la Ley. Las Empresas que disponen de datos de carácter personal pueden verse involucradas en sanciones realizadas bajo denuncias de personas que participan en el negocio ya sea por parte de sus clientes, colaboradores o empleados. Cumplir con la Ley

es una obligación cada día más latente debido en mayor medida a las sanciones, el motivo principal que empuja a las Empresas a cumplir la normativa.

Facilidad en la implementación

El IFAI ha elaborado y puesto a disposición en su portal www.ifai.org.mx Guías para generar aviso de privacidad, para solicitud de derechos ARCO y para solicitud de protección de derechos ARCO (entre otras), con información de interés para aquellas Empresas que estén implementando la Ley de protección de datos personales; así mismo al público en general para que conozcan sus derechos y los hagan exigibles ante las Empresas y el IFAI, sin embargo se requiere mayor difusión sobre las mismas.

Creación de un entorno de seguridad

La implementación de la Ley de protección de datos puede constituir el primer paso para orientar a las Empresas hacia un entorno de seguridad más ambicioso. Así, existen en la actualidad sistemas de gestión de seguridad de la información (SGSI) que persiguen, por un lado, incorporar la seguridad en los sistemas de información de las Empresas como elemento de la mejora de la gestión y de la competitividad y, por otro, ofrecer protección contra los riesgos y pérdidas asociados al creciente uso de tecnologías de la información y de la comunicación en las Empresas.

Conclusiones Generales

La Ley de Protección de Datos Personales en Posesión de Particulares aún es poco conocida en general por la mayoría de las Empresas Privadas, por lo que las pequeñas Empresas se encuentran con desconocimiento de la misma y menos preparadas para hacer frente a las obligaciones previstas por el Reglamento.

El desconocimiento de la Ley, se manifiesta tanto a través de las respuestas de las Empresas encuestadas ante la pregunta directa sobre el conocimiento de la legislación (de acuerdo a las conclusiones del apartado de Medidas de Seguridad el 47.5% de las Empresas No entienden la Ley y el 27.1% de las Empresas Desconocen la Ley y su Reglamento), como mediante los indicios analizados a lo largo del estudio y derivados de las investigaciones cuantitativa y cualitativa. No se puede afirmar, que todas las Empresas se encuentren en un estado similar de desconocimiento de la Ley; ya que nuestro estudio sólo abarco 221 Empresas, y existe un amplio abanico de circunstancias entre las diferentes Empresas encuestadas; desde las que no han oído hablar de la Ley, hasta casos que si bien saben que existe, desconocen la obligatoriedad de su cumplimiento, su ámbito de aplicación, las implicaciones concretas para su negocio, las sanciones a las que se pueden enfrentar en caso de incumplimiento o los plazos de adecuación.

El nivel de desconocimiento es justificado teniendo en cuenta la reciente fecha de entrada en vigor de la Ley y su Reglamento.

Las acciones formativas e informativas llevadas a cabo por IFAI y la Secretaría de Economía, no han alcanzado la efectividad deseada, o no han tenido suficientemente en cuenta las particularidades de los colectivos a la hora de elaborar acciones específicamente dirigidas a ellos.

El nivel de cumplimiento entre las Empresas no es homogéneo, existiendo Empresas que incumplen completamente las disposiciones de la ley, y otras que están parcialmente adaptadas a la normativa. Por tanto, es necesario que el esfuerzo en este sentido sea continuado y sostenido.

Detrás del limitado nivel de adopción se encuentra, aparte de una escasa cultura y concienciación sobre la necesidad de proteger los datos, la consideración por parte de la Empresas que se trata de una obligación legal que implica tareas tediosas y complejas y que no aporta ningún valor añadido a su negocio, el desconocimiento de las consecuencias de incumplimiento, y la limitación de recursos humanos, económicos y técnicos para hacer frente a la adopción. Se

trata, en su mayoría, de barreras declaradas por las propias Empresas que en muchas ocasiones pueden ser fácilmente solventadas con acciones formativas concretas y efectivas.

Actualmente México cuenta con leyes en el tema de la protección de datos personales, pero los avances en este tema son pocos porque los ciudadanos desconocen los derechos que tienen en este aspecto, e incluso los riesgos por no demandar esta protección, como es que los tengan empresas o personas que viven fuera del país, señaló Lina Ornelas Núñez, investigadora del CIDE.

“Cuando se dan datos, ya sea por trámites ante empresas u oficinas de gobierno, estos pueden pasar a formar parte de bases de datos que si no están protegidas pueden ser utilizadas dentro o fuera del país con cualquier finalidad, a través de fugas de información, mientras en las redes sociales o los correos electrónicos, estos datos se encuentran en bases en manos de las empresas donde se contratan estos servicios, algunas en México y otras fuera, y donde cualquier persona puede tener acceso a tales datos”, abundó la investigadora.

Apuntó que aunque hay leyes en materia de protección de datos personales, faltan políticas públicas para avanzar en este tema y tienen que ser muy agresivas para lograr avances rápidos en este tema, pues no solamente se trata de que una persona pueda o no ser contratada para un trabajo por estos datos, sino de que también información sobre sus cuentas bancarias o tarjetas de crédito pueda caer en manos de personas que le quiten sus ahorros, mencionó a manera de ejemplo, al señalar que son muchos los aspectos en los que se requiere trabajar en este tema, pues puntualizó que no se trata solamente de un tema de libertad de expresión, sino también de seguridad para los ciudadanos.[20]

En este contexto, es necesario un esfuerzo de concienciación y difusión por parte de todas las Autoridades implicadas para el cumplimiento de la Ley: las administraciones y autoridades competentes, que han de concientizar a los Titulares y las Empresas sobre la necesidad de adaptarse a la Ley; las Empresas prescriptoras y facilitadoras (asesoras, consultoras), que están en condiciones de realizar un correcto diagnóstico sobre la situación de las Empresas y planificar de forma eficiente su implantación; por último, es importante que si bien la propia inercia del mercado contribuirá a generalizar el cumplimiento de la normativa sobre protección de datos entre las Empresas, a medida que se difunda entre la

[20] Poco avance en protección de datos personales,http://chicotito.com/poco-avance-en-proteccion-de-datos-personales-lina-ornelas/?goback=%2Egde_3786381_member_210887304, Febrero 2013

población el ejercicio de los derechos que la Ley otorga a todo ciudadano, es recomendable:

Que haya más campañas de concientización en todos los medios de comunicación (televisión, radio, periódico, posters en lugares públicos como estaciones de transporte público, entre otros).

Se genere capacitación y certificación a las Empresas que se dedican a ofrecer servicios de implementación, consultoría o auditoría de controles para el cumplimiento con la Ley.

Requerir a los profesionales que participen en Empresas que prestan servicios de consultoría y auditoría certificaciones de reconocimiento internacional como pueden ser las emitidas por ISACA[21].

Las autoridades actúen conforme lo marca la Ley ante las infracciones cometidas por los Responsables y se den a conocer al público en general.

Generar programas de apoyo para las micro y pequeñas Empresas, proveyendo subsidios para la implementación de los controles requeridos para la protección de datos a través de Empresas consultoras.

[21] *Information Systems Audit and Control Association*, www.isaca.org, 2012.

Recomendaciones para Empresas y Administraciones

Con base en el estudio de cultura realizado, los parámetros de medición y los resultados arrojados por el estudio, se realizan las siguientes recomendaciones de actuación para atacar las principales deficiencias que enfrenta la LFPDPPP en México.

Antes de comenzar debemos establecer la diferencia entre la Autoridad Reguladora y la Autoridad Garante ambas facultadas en la LFPDPPP para la protección de los datos personales; para que aunado a las recomendaciones que propondremos colaboren en el ámbito de sus atribuciones a la efectiva implementación de la Ley dentro de las Empresas del Sector Privado.

AUTORIDAD REGULATORIA

Secretaria de Economía

Funciones primordiales conferidas por la Ley:

- Difundir el conocimiento de las obligaciones en torno a la protección de datos personales entre la iniciativa privada nacional e internacional con actividad comercial en territorio mexicano
- Promoverá las mejores prácticas comerciales en torno a la protección de los datos personales como insumo de la economía digital, y el desarrollo económico nacional en su conjunto.

Como sus atribuciones Informativas se encuentran:

- Difundir el conocimiento respecto a la protección de datos personales en el ámbito comercial
- Apoyar la realización de eventos, que contribuyan a la difusión de la protección de los datos personales.
- Fomentar las buenas prácticas comerciales en materia de protección de datos personales

Como sus atribuciones Normativas se encuentran:

- Emitir los lineamientos para el contenido y alcances de los avisos de privacidad en coadyuvancia con el Instituto.
- Emitir, en el ámbito de su competencia, las disposiciones administrativas de carácter general a que se refiere el artículo 40, en coadyuvancia con el Instituto
- Fijar los parámetros para el correcto desarrollo de los mecanismos y medidas de autorregulación a que se refiere el artículo 44 de la Ley, incluido la promoción de Normas Mexicanas o Normas Oficiales Mexicanas, en coadyuvancia con el Instituto
- Diseñar e instrumentar políticas y coordinar la elaboración de estudios para la modernización y operación eficiente del comercio electrónico, así como para promover el desarrollo de la economía digital y las tecnologías de la información en materia de protección de datos personales

Atribuciones de Verificación:

- Llevar a cabo los registros de consumidores en materia de datos personales y verificar su funcionamiento

Atribuciones Resolutorias:

- Acudir a foros comerciales nacionales e internacionales en materia de protección de datos personales, o en aquellos eventos de naturaleza comercial
- Celebrar convenios con cámaras de comercio, asociaciones y organismos empresariales en lo general, en materia de protección de datos personales

AUTORIDAD GARANTE

Instituto Federal de Acceso a la Información y Protección de Datos. (IFAI)

Objeto primordial conferido por la Ley: **Difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana**, **promover su ejercicio y vigilar su cumplimiento** por parte de los sujetos obligados.

Como sus atribuciones Informativas se encuentran:

- Brindar apoyo técnico a los Responsables (Empresas del Sector Privado) que los soliciten para el cumplimiento de las obligaciones que establece la Ley
- Fomentar y difundir análisis estudios e investigaciones en materia de protección de datos
- Brindar capacitación a los sujetos obligados.
- Rendir al Congreso de la Unión un informe anual de actividades.

Como sus atribuciones normativas se encuentran:

- Interpretar en el ámbito administrativo la Ley
- Emitir los criterios y recomendaciones que garanticen la protección de datos personales
- Divulgar estándares y mejores prácticas Internacionales en materia de seguridad de la información

Atribuciones de verificación:

- Supervisión enfocada a vigilar y verificar el cumplimiento de las disposiciones contenidas en la Ley
- Elaborar estudios de impacto sobre la privacidad previos a la puesta en práctica de una nueva modalidad de tratamiento o a la realización de modificaciones sustanciales en tratamientos ya existentes.

Atribuciones Resolutorias:

- Conocer y resolver los procedimientos de protección de derechos y de verificar e imponer las sanciones según corresponda.
- Acudir a foros internacionales y cooperar con otras autoridades de supervisión y organismos nacionales e internacionales, a efecto de coadyuvar en materia de protección de datos.

Atribuciones sancionadoras:

- El IFAI también está facultado para imponer sanciones pecuniarias de acuerdo con la gravedad de las conductas, tomando en cuenta: la naturaleza del dato, la negativa del responsable ante los actos solicitados por el titular, la intencionalidad de la acción u omisión de la infracción, la capacidad económica del Responsable y en su caso la reincidencia.

Como aspectos positivos el IFAI se ha enfocado en:

- ✓ Emisión de regulación secundaria: Lineamientos y recomendaciones
- ✓ Verificaciones a sistemas de datos personales
- ✓ Seguimiento al registro de sistemas de datos (3,034).
- ✓ Notificación de la Guía para la elaboración del documento de seguridad
- ✓ Elaboración de Impacto a la Privacidad (PIA´s): NOM-024 Expediente clínico electrónico y Cédula de Identidad Ciudadana
- ✓ Elaboración de las recomendaciones al proyecto implementación del SNIP y eventual expedición de la Cédula de Identidad
- ✓ Comentarios al Proyecto de reglamento de la Ley Federal de Telecomunicaciones en materia del Registro Nacional de Usuarios de Telefonía Móvil (RENAUT)
- ✓ Difundir en los medios de comunicación, comerciales sobre el aviso de privacidad de manera obligatoria.
- ✓ Difundir a través de los medios visuales: carteles y propagandas colocadas en los sistemas de transporte más comunes y de mayor concurrencia la obligatoriedad de proteger datos personales.

Recomendación para IFAI

Las últimas acciones de difusión, están dedicadas en su mayoría a las Empresas del sector Privado, lo cual es excelente, tratando de imponer la obligatoriedad de cumplir con la Ley a la brevedad posible, pero hacemos hincapié en que aún no se ha elaborado una campaña de difusión para la sociedad, principales actores a quienes protege específicamente la Ley; recomendamos que se haga una **campaña de difusión especializada en los titulares de los datos (la población mexicana)** para darles a conocer este nuevo derecho a la protección de sus datos personales, establecido ya en la Constitución Política de los Estados Unidos Mexicanos como derecho inherente de la población.

La campaña podría establecerse desde el aspecto: del valor intrínseco de los datos, fomentando en la población la protección de sus datos, y dándoles un valor económico en posesión de las Empresas Privadas. Puesto que nuestros datos personales son susceptibles de ser extraídos de instituciones bancarias, crediticias, de servicios como televisión por cable, telefonía celular o fija, e incluso de instituciones gubernamentales o paraestatales. Y no es raro recibir una llamada telefónica con el fin de ofrecernos servicios no requeridos, o llamadas de extorsionadores que parecen tener mucha más información de nosotros. Es por ello que se crea esta Ley para la protección y no divulgación masiva de los datos personales.

Es por ello que basándonos en los resultados obtenidos del Estudio proponemos las siguientes Recomendaciones de actuación, establecidas en 3 ejes de impacto que tienen como finalidad atacar las deficiencias que enfrenta la aplicación de la LFPDPPP y su Reglamento en las Empresas del Sector Privado en México.

1.-Concientizar a la Población Mexicana en los Derechos que les confiere la LFPDPPP y crear un mayor esfuerzo para la concientización de las obligaciones impuestas a las Empresas del sector Privado.

Conforme a los resultados del estudio elaborado, encontramos como principal deficiencia el desconocimiento y entendimiento de la Ley, explicando que aunque nuestro estudio únicamente fue aplicado a Empresas Privadas, es claro determinar que la población en general desconoce este derecho que le confiere la Ley; a la protección de sus datos personales, y es por ello que la sociedad mexicana no ha hecho exigibles sus derechos ante las Empresas, por tal motivo estas han hecho caso omiso a las obligaciones, que tienen frente a los titulares de los que poseen datos.

Podemos inferir que ante el apremio que se imponga a las Empresas del sector Privado, se hará presente su actuación y aplicación de la Ley dentro de las mismas. Siendo así, si la Autoridad garante se encarga de exigir su cumplimiento ante verificaciones constantes y aplicación de sanciones en caso de incumplimiento; las Empresas se encontrarán forzadas para acatar los cumplimientos de la Ley, aunado a esto, si la población conoce y hace exigibles sus derechos ante las mismas, se crearán dos frentes de exigibilidad, lo cual impulsará el cumplimiento de la Ley dentro del sector Privado.

El IFAI ha difundido campañas a manera de obligar a las Empresas Privadas en el cumplimiento de los avisos de Privacidad, pero sus campañas carecen de carácter informativo sobre cómo deben de cumplir, de donde surge este nuevo derecho de protección hacia los datos personales, cuales son las sanciones, y lo más importante que es un aviso de privacidad etc.; difundiendo un único mensaje “sobre aviso no hay engaño” y lo único que establece es un apercibimiento de la Ley por incumplimiento de algo no establecido o definido. Por ello especulamos el no entendimiento de la Ley entre las Empresas Privadas, debido a la falta de información por parte de la autoridad garante en su principal influencia entre la población, que son los medios de comunicación masiva.

.

Recomendaciones:

Nosotros recomendamos una doble vía actuación, por un lado concientizar a las Empresas y por otro lado la concientización de la población ya que a través de su conocimiento, ellos mismos serán capaces de hacer exigibles sus derechos ante las Empresas que recaban sus datos, lo que representaría la actuación inmediata por parte de las Empresas para cumplir con la aplicación de la normativa

Para la concientización en el sector Privado

Dejamos claro que no solo en la difusión de comerciales en los medios de comunicación se genera el conocimiento de esta Ley, el IFAI ha elaborado cursos en su portal de internet y guías prácticas dirigidas a las Empresas; que de manera efectiva, ayudan a cumplir con la Ley, declarando que la información si existe, lo que hace falta es acertar en la manera de propagarla, para crear un conocimiento efectivo en las Empresas para que cumplan con las obligaciones que les señala la Ley.

Se recomienda perfeccionar los comerciales en cuanto a que sean más completos en la información básica y necesaria que deben conocer las Empresas para hacerles saber con lo que deben cumplir haciendo énfasis en que todos los requerimientos ya son exigibles y que de no cumplirlos serán sancionados. Mejorar la estrategia de campaña sobre los medios de comunicación masiva.

Es tarea de las Autoridades determinar la estrategia para generar el impacto, nosotros sólo emitimos recomendaciones sobre lo que hace falta por difundir.

Para la concientización de la Población

La campaña que proponemos al IFAI, se debe establecer con el fin de concientizar a la población del valor de sus datos personales, infundiendo en los titulares el primer filtro de protección; el cual se basa en no proporcionar los mismos a cualquier Empresa, sin que antes le garantice mediante un Aviso de Privacidad que sus datos se encontrarán en las mejores manos, es por ello que se recomienda que en la campaña se abarquen los siguientes puntos como medidas para concientizar a la población:

1. Conocimiento de los Derechos que esta Ley les confiere
   - Protección de datos personales (derecho a la privacidad) establecido en la Constitución Política Mexicana
   - Autodeterminación informativa (el poder que tiene la población para proporcionar los datos que ellos deseen)

2. Explicar a la Población que es un dato personal, bajo esquemas de ejemplos comprensibles, difundiendo en la Población que existe una clasificación por tipo de dato personal y que cada tipo de dato merece medidas especiales de seguridad, así mismo un tipo de consentimiento distinto para poder recabarlo.

3. Establecer el valor de los datos personales de manera económica, en el cuánto vale la información personal para las Empresas, lo cual generará en la población el primer nivel de protección, pues para las Empresas ya no será fácil obtener dato personales sin el consentimiento del titular.
    - Enseñar a la población y principalmente a los jóvenes y menores de edad, ya que son la población más vulnerable de la sociedad, la importancia de proteger sus datos personales, persuadiendo a la población del valor que representan para las Empresas Privadas los datos personales. Proponemos difundir campañas en las Escuelas de estos niveles (básico, medio, medio superior y superior) con el fin de instruir a los alumnos; en la peligrosidad de difundir sus datos personales en las redes sociales, internet, o proporcionarlas a Empresas Privadas, a cambio de un obsequio o promoción.
    - De este modo se ayuda intrínsecamente a la protección de las personas, que hoy en día proporcionan sus datos en internet, haciéndolas susceptibles a diversos tipos de delitos como es el secuestro por citar un ejemplo.

4. Instruir a la población en lo que es un Aviso de Privacidad, sus requisitos mínimos que la Ley les establece a las Empresas, para que den un grado de seguridad a sus datos personales y un grado de confianza en la Empresa que los recaba.

5. Instruir a la población en lo que son los Derechos ARCO, lo que les confiere como derecho al acceso, rectificación, cancelación y oposición de sus datos y como los pueden hacer valer ante las Empresas Privadas que posean sus datos personales.

6. Conocimiento de la Autoridad a las que pueden acudir los titulares en caso de que las Empresas no garanticen sus derechos.

Asimismo consideramos que en las Campañas o capacitaciones a la que haya lugar por parte del IFAI se proporcione un número de atención a la población, que ayude a dilucidar cualquier duda que presente la población acerca del tema.

Resaltamos que nosotros sólo emitimos recomendaciones, y será tarea de las Empresas encargadas de elaborar campañas las formas y los medios que consideren necesarios para elaborar una campaña efectiva y que genere el impacto necesario que se busca; que es generar concienciación y conocimiento del derecho a la protección de datos personales para la Población Mexicana.

Impacto: Conocimiento y entendimiento de la Ley en los dos ámbitos

- **Población mexicana**
- **Empresas del sector Privado**

2.-Implementación de la LFPDPPP en el sector Privado donde se enfocó el estudio (PyME´s)

De acuerdo con el estudio realizado sólo un 54% de las compañías encuestadas afirman estar cumpliendo con las medidas de seguridad existentes, aunque conforme a los demás requerimientos que la Ley les establece se comprobó que es un porcentaje mínimo las que si están implantando medidas para proteger los datos personales en su poder, asimismo tratando de someterse a los requerimientos que la Ley les asigna, mientras que el resto de las compañías que no tienen ni el conocimiento de lo que representa esta Ley y lo deben cumplir, son estas últimas las que representan un foco rojo y ponen en riesgo la protección de los datos personales y la continuidad de los negocios.

Las Empresa privadas no han tomado en cuenta que la Ley ya es exigible para que todas aquellas personas físicas o morales de carácter Privado que traten datos personales cuenten con los procedimiento necesarios para cumplir con la LFPDPPP, y mantengan medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra mal uso o uso no autorizado.

Siendo esta la situación las Empresas Privadas y principalmente las PyME´s no ha considerado que al no implementar las medidas necesarias para cumplir con lo establecido por la Ley podrían ser sancionados con multas que van desde los seis mil a los 38 millones de pesos, lo que representa un riesgo para la permanencia del negocio, incumplimiento que les puede salir muy costoso así como comprometer su libertad.

Así mismo no han hecho énfasis en que independientemente de las multas a las que puedan estar sujetos, existen otros peligros que pueden colocar a la Empresa en situaciones delicadas como el robo de información al que puedan estar sujetos por no contar con medidas de seguridad aplicables a la protección de datos, la afectación a la reputación de la Empresa por no estar sujeta a la Ley, la perdida de contratos con otras Empresas por su incumplimiento, y la desconfianza de sus clientes.

Todo esto presenta un riesgo al sector Privado por no cumplir con la Ley.

A continuación señalaremos los puntos más importantes que exige IFAI frente a una revisión de rutina para la protección de datos personales, para que sea considerado por las Empresas:

- Copia de los documentos donde se recaba el consentimiento expreso cuando se trata de datos sensibles.
- La política de confidencialidad de la empresa según lo que expresa el Artículo 21 de la Ley.
- El "Documento de Seguridad de los Datos Personales" y la forma como se actualiza.
- El aviso de privacidad y la forma en la que se da a conocer a los titulares de los datos.
- La forma en la que se garantiza la confidencialidad de los datos personales, (Procesos, políticas y sistemas).
- Informar si han tenido o sufrido vulnerabilidad a la seguridad de sus sistemas y datos. Así como los reportes de riesgo que puedan prever cualquier contingencia.
- Manifestar qué personal de la organización tiene acceso a los datos personales y de qué manera han sido controlados y concientizados sobre la importancia de los datos que manejan. En este punto solicitan también las responsivas correspondientes.
- Informar sobre las medidas físicas, técnicas o administrativas que ha implementado para tratar los datos personales y en particular los que sean sensibles.

Lo anterior es mostrado para que las Empresas afectadas se enfoquen en lo que les falta por cumplir, así mismo exhortar a las Empresas que no lo han hecho a ponerlo en práctica para su cumplimiento y evitar una sanción por parte de la Autoridad garante.

Lo que buscamos atacar en este eje es generar la divulgación para crear conocimiento, entendimiento y aplicación efectiva de la LFPDPPP y su Reglamento en las Empresas del sector Privado.

Recomendaciones:

Frente a las acciones tomadas por el IFAI para la difusión de la Ley entre las Empresas del sector Privado se encuentran:

- ✓ Las campañas enfocadas a la importancia de cumplir con el Aviso de Privacidad
- ✓ Las guías que se encuentran en su portal de internet para llevar de la mano a la Empresas para el cumplimiento de los requerimiento de Ley
- ✓ Un curso dirigido a las Empresas para inducir el conocimiento de la Ley y que es con lo que debe cumplir.

Aunado a todas estas medidas nosotros exhortamos las siguientes medidas de actuación dirigidas en dos fases para las Empresas:

1. **Capacitar a las Empresas por parte de la Autoridad Garante**

Determinando que capacitar lo entendemos desde el sentido de propagar el conocimiento de esta Ley entre las Empresas. Dejamos a criterio de la Autoridad garante el medio para llevarlo a cabo pudiendo ser a través de campañas internas dentro de las Empresas, realizar campañas más profundas en los medios de comunicación masiva (más completas), a través de más guías enfocadas en los temas que aún no han abordado etc.

Recomendamos capacitar sobre los siguientes temas

- Breve Panorama de la LFPDPPP y su Reglamento, desde el aspecto jurídico en el que la Constitución otorga la protección de derechos personales como una garantía inherente a la población mexicana. Y haciendo énfasis en las obligaciones que se establece la misma a las Empresas Privadas.

- Que es un dato personal, como se clasifican, como recabar los datos dependiendo del tipo de dato a tratar enfocando este punto, en el tipo de consentimiento que se debe obtener conforme a lo establecido en la ley, así como las medidas de seguridad aplicables a cada tipo de dato.

- Perfil que debe cumplir el Responsable de los datos, para que dentro de la Empresa se asigne el personal adecuado para asumir esta responsabilidad de cara a los titulares y ante la Autoridad Garante.
    - □ De acuerdo con la Ley, las Empresas deben designar a una persona o departamento de datos personales que sea responsable de dar trámite y contestación a las posibles solicitudes de derechos ARCO y también de fomentar la protección de datos personales dentro de la organización. Sin embargo, la realidad es que las Empresas no saben cómo actuar ante una solicitud ARCO pues carecen tanto de una metodología para recibirla, como de la tecnología para procesarla y responderla en los términos que

indica la ley (máximo 20 días). De hecho muchas empresas no cuentan ni con la tecnología, ni con el personal suficiente y sobre todo calificado para dar respuesta al número de demandas ARCO, esto tomando en cuenta que dar respuesta a una solicitud ARCO puede ser más complicado de lo que parece a simple vista, dado que los datos personales del solicitante se encuentran dispersos en varios departamentos de la empresa.

- Aviso de Privacidad recomendamos una guía sencilla para su elaboración con los requerimientos mínimos que establece la Ley

- Procedimiento para el Ejercicio de los Derechos ARCO, proponemos elaborar una guía que lleve de la manos a las Empresas para la elaboración de este procedimiento, la cual les muestre los términos de respuesta que la Ley establece. Así como para la elaboración de la solicitud para el ejercicio de los Derechos ARCO.
    - Uno de los principales aspectos de la LFPDPPP es el reconocimiento de los derechos ARCO, es decir, la facultad que cada persona tiene para exigir a una empresa u organización el acceso a sus datos personales que de ella tenga así como para solicitar su rectificación, cancelación e incluso oponerse a su uso. El incumplimiento a una solicitud ARCO puede ser sancionado con multas que pueden llegar a alcanzar hasta los trescientos veinte mil días de salario mínimo (18 millones de pesos según la capacidad de la empresa y la medidas que haya adoptado o no para procurar cumplir con la Ley).

- Recomendaciones sobre las medidas de seguridad mínimas que deben aplicar para el tratamiento de los datos.

- Guía de manera general y sencilla sobre los documentos, procedimientos con que deben cumplir por Ley todas las Empresas para la protección de los datos personales

- Explicar la diferencia entre ceder datos de carácter personal y transferencias.

    - Aquellos terceros deben reflejar su compromiso más allá de los SLA que sólo garantizan, cuando así se cumple, la Continuidad del Servicio, no así el tratamiento de los datos personales. Lo mismo pasa con un convenio de Confidencialidad, que sólo nos dice que “no se divulgará información que se conozca en el transcurso del manejo de la información”, pero no garantiza que se pierda, la roben o extraigan.

Por ello es necesario validar la seguridad de los terceros a los que se comparten datos de carácter personal, a fin de constatar que cuentan con los mecanismos de seguridad mínimos que establece la Ley, y ver que esto se refleje en un documento donde se comparta la responsabilidad en caso de que los datos personales se pierdan.

- Las sanciones a las que se hacen acreedoras las Empresas por el incumplimiento de la Ley de carácter pecuniario y privativo de libertad.

Una vez que las Empresas del sector Privado cuentan el conocimiento suficiente para Implementar la Ley (difundido por IFAI)

- Lo que esta Ley protege (datos personales de los titulares)
- Como les afecta (en el sentido de los controles que deben implantar para cumplir)
- Con lo que deben cumplir (procedimientos que deben generar)
- Las sanciones a las que se hacen acreedores por su incumplimiento
  - ✓ Y como plus: los beneficios que traerá a la Empresa su implementación, e incentivar a las Empresas para cumplir más allá de lo que la norma establece.

Si bien es cierto que en la mayoría de las Empresas consideran y analizan las políticas o herramientas próximas a implementarse antes de usarlas o proponerlas a la Directiva del negocio. Es prioridad cumplir con los requerimientos de la Ley, debido a que ya es obligatoria y exigible y su incumplimiento puede comprometer significativamente al negocio.

Propondremos algunas Recomendaciones para las Empresas

2. Dentro de las Empresas

No debemos olvidar lo más importante en el cumplimiento de la Ley y el Reglamento esto es:

- Verificar que nuestros procesos implantados se encuentren funcionando correctamente
- La concienciación de las personas que tratarán los datos personales dentro de la Empresa (Capacitar al Personal) es la clave para el cumplimiento de la Ley.

En la seguridad de la información, el enemigo más peligroso está en casa y muchas veces se debe a la falta de conocimiento e iniciativas personales, sin identificar los peligros que se invocan cuando actuamos aparentemente en pro de la Empresa.

La mayoría de los fraudes han sido cometidos por empleados internos de las Empresa, por lo que es necesario mantener un control estricto sobre quién y de qué forma se manejan los bancos de datos.

Crear Conciencia en el personal sobre la importancia y riesgo del manejo de datos personales en la labor de cada uno de los que laboran dentro de la empresa y también afuera como titulares, a fin de lograr tener una cultura de protección de datos personales y prever cualquier inconveniente. Recomendamos establecer esta cultura de protección de datos personales como un principio general de la Empresa.

Dar **Capacitación al personal**, ya sea a través de cursos, presentaciones etc. así mismo darle seguimiento a la capacitación, a través de la elaboración de cuestionarios, para conocer el nivel de compresión que se ha sido captado en los empleados y enfocarnos en lo que no fue comprensible para corregirlo de inmediato.

Hacemos hincapié que la capacitación debe realizarse de acuerdo al nivel de importancia del manejo de los datos personales, siendo ésta orientada primeramente en personal que por sus funciones desempeñadas dentro de la Empresa tenga acceso a los datos personales. Recalcando que en ese orden escalado se debe capacitar, permeando todas las áreas de la Empresa, para generar la cultura deseada.

Así mismo la capacitación será en el mismo grado de complejidad, con base al tipo de personal que reciba dicha capacitación. Es importante señalar que el área Directiva es la primera que se debe capacitar, debido a que es de suma importancia que conozca las obligaciones a las que estará sujeta su Empresa ante la Ley.

Debemos recordar que la LFPDPPP fue creada para salvaguardar lo más valioso que tenemos como seres humanos, Nuestra Privacidad, y para ello debemos modificar muchas de las conductas que hemos aprendido y que pasan por alto este derecho. La ley nos dice lo que debemos hacer, el reglamento nos dice bajo que reglas, pero cada uno de nosotros debemos establecer el cómo.

Impacto: Cumplimiento de la Ley por parte de los sujetos obligados el sector Privado, garantizando la Protección de los Datos Personales.

3.- Profesionales de la Seguridad (Consultorías)

Conscientes de que en México la Protección de Datos Personales es un derecho de reciente creación y de carácter obligatorio para las Empresas Privadas, y su implementación es necesaria e inmediata, las Empresas que buscan apegarse a los lineamientos de la Ley pretenden encontrar en las consultorías, profesionales en la materia para ayudarlos a cumplir con la Ley.

La realidad es que existen escasos profesionales en la materia, que no contando con una capacitación dentro del tema de privacidad, se basan en los modelos Europeos donde la protección del derecho a la Privacidad ya lleva aproximadamente 20 años de implantación.

Además existen los falsos Mesías: Consultorías que sin contar con el mínimo conocimiento en la materia, han implementado la Ley en grandes instituciones, y lo han hecho de manera incorrecta, e incompleta, dejando al descubierto su pobreza ante el tema, y demostrando que su implementación no cuenta con el sustento, ni con la capacidad de soportar una verdadera auditoría de protección de datos, lo cual pone el peligro a sus clientes pues no los salva de una multa o incluso de la privación de su libertad.

Recomendaciones:

Proponemos una **Certificación** por parte de la Autoridad garante, en la cual se capacite a las Consultorías que así lo deseen, en el tema de Privacidad, capacitación que cuente con personal calificado en la materia, ya sea mediante convenios con la OCDE o con países que ya cuentan con experiencia en este tema por ejemplo la Unión Europea.

Proponemos la certificación para garantizar que los Consultores realicen bien su trabajo en las Empresas que requieran sus servicios, previo a una capacitación y así mismo se beneficien por encontrarse respaldados por la certificación de una Autoridad competente como lo es IFAI.

A las Consultorías recomendamos lo siguiente

Las Consultorías deben considerar las siguientes recomendaciones, para ejecutar una buena implementación de la Ley:

- Identificar las fuentes y orígenes de datos personales.
- Clasificar los datos, conforme a lo establecido en la Ley
- Hacer un análisis para establecer la finalidad con la que se recaba cada dato personal, recordando que si hay un dato que no nos sirve o no utilizamos, debemos dejar de recabarlo.
- Poner especial atención en los expedientes de recursos humanos de empleados potenciales, actuales y pasados de la organización, así como en los de clientes que sean personas físicas, ya sean prospectos, actuales o pasados.
- Generar y administrar el “Documento de Seguridad de Datos Personales”.

- Realizar un análisis de los riesgos a los que están expuestos los datos personales, considerando las posibles vulneraciones que contempla el Artículo 63 del reglamento.
- Identificar los controles que se requieren para minimizar los riesgos detectados.
- Realizar un análisis de brecha sobre qué controles ya se tienen implementados y establecer un plan de trabajo para implementar los faltantes. Cabe destacar que se tiene hasta junio de 2013 para implementar estos controles.
- Asegurar que se cuenta con un aviso de privacidad que esté alineado a los elementos señalados por el Art. 26 del reglamento y el 16º de la Ley. El aviso de privacidad debe contar con los datos de identificación de la Empresa como responsable de proteger los datos, los datos personales que recabamos (señalando si se trata de datos sensibles y en su caso recabando el consentimiento expreso), así como las finalidades y los tratamientos a los que serán sometidos los datos personales, las organizaciones con las que se comparten datos (transferencias), y las vías de contacto para ejercer los derechos ARCO, para notificar cambios en el aviso de privacidad a los titulares y los medios que se utilizaran para garantizar la confidencialidad de los datos.

También es necesario designar una persona o departamento responsable de la protección de los datos personales al interior de la Empresa.

Recordando que los procedimientos para atender solicitudes de ejercicio de derechos ARCO en los términos del capítulo VII del reglamento ya son exigibles a partir de enero de 2012.

Por último, y no por ello menos importante, capacitar a nuestro personal, tanto al que recaba como al que maneja datos personales, identificando el ciclo de vida de los mismos, desde que son recopilados hasta que son destruidos o cancelados para su uso.

Se identifican las siguientes áreas como críticas donde se tratan datos personales, establecido en la estructura general en una Empresa

- Área R.H.
- Área Jurídica,
- Marketing
- Sistemas

En cada una de ellas se recomienda realizar un assesment detallado sobre el tratamiento que se da actualmente a los datos personales (no sólo de los clientes, sino también de prospectos y, por supuesto, de los propios empleados y colaboradores) para identificar en qué procesos de negocio se recopilan y manipulan estos datos, qué sistemas apoyan dichos procesos y cuáles son los incumplimientos de los mismos respecto de los lineamientos especificados por la norma.

Una vez identificados estos posibles focos de incumplimiento, se deberán definir las modificaciones a realizar en procesos y sistemas, priorizarlas en función de su criticidad,

riesgo y costo asociado y, con esta información, poner en marcha un plan de adecuación en el que uno de los factores de éxito clave será una adecuada gestión del cambio en la organización.

Por todo ello es importante perseguir el dato desde su origen, hasta su final destrucción, a través de los procesos del mismo negocio y no en los servidores y aplicativos.

Nuestra obligación como profesionales de la seguridad ahora no sólo es para con la infraestructura de la Empresa y sus datos, sino también con nuestros usuarios internos y externos y más aún con nuestros Directivos, a los cuales debemos proteger de las sanciones privativas de libertad y que las utilidades se vayan a las arcas del gobierno a través de exorbitantes sanciones

54% afirmaron

Impacto: Implementar la LFPDPPP y su Reglamento de manera correcta en las Empresas Privadas, realizando una Consultoría de calidad.

Todas las recomendaciones anteriores fueron elaboradas en base al estudio previamente realizado, priorizando las deficiencias encontradas, para que sean resueltas oportunamente. Y será facultad de las Autoridades correspondientes encontrar los medios y las formas de cómo será llevado a cabo.

Modelo Incremental

Historia

Propuesto por Mills en 1980. Sugirió el enfoque incremental de implementación como una forma de reducir la repetición del trabajo en el proceso de implantación y dar oportunidad de adquirir experiencia con el sistema. Surge porque en las primeras implantaciones se podía esperar largo tiempo hasta que el sistema estuviese listo.

El modelo incremental combina elementos del modelo lineal secuencial (aplicados repetidamente) con la filosofía interactiva de construcción de prototipos. El modelo incremental aplica secuencias lineales de forma escalonada mientras progresa el tiempo en el calendario. Cada secuencia lineal produce un incremento del proyecto. El proceso se divide en 4 partes: Planear, Diseñar, Ejecutar, Auditar (Ciclo de Deming)

Ciclo de DEMING

El ciclo de Deming, también conocido como círculo PDCA o círculo de Gabo (de Edwards Deming), es una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhart. También se denomina espiral de mejora continua. Utilizado principalmente por los Sistemas de Gestión de Calidad (SGC).

Las siglas PDCA son el acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar).

Los resultados de la implementación de este ciclo permiten a las empresas una mejora integral de la competitividad, de los productos y servicios, mejorando continuamente la calidad, reduciendo los costes, optimizando la productividad, reduciendo los precios, incrementando la participación del mercado y aumentando la rentabilidad de la empresa u organización.

PLAN (Planificar)

Establecer los objetivos y procesos necesarios para obtener el resultado esperado. Al basar las acciones en el resultado esperado, la exactitud y cumplimiento de las especificaciones a lograr se convierten también en un elemento a mejorar. Cuando sea posible conviene realizar pruebas a pequeña escala para probar los resultados.

1. Identificar proceso que se quiere mejorar.
2. Recopilar datos para profundizar en el conocimiento del proceso.
3. Detallar las especificaciones de los resultados esperados
4. Definir los procesos necesarios para conseguir estos objetivos, verificando las especificaciones

DO (Hacer)

Implementar los nuevos procesos, llevar a cabo el plan. Recolectar datos para utilizar en las siguientes etapas. Teniendo el plan bien definido, hay que poner una fecha a la cual se va a desarrollar lo planeado.

CHECK (Verificar)

Pasado un periodo de tiempo previsto de antemano, volver a recopilar datos de control y analizarlos, comparándolos con los objetivos y especificaciones iniciales, para evaluar si se ha producido la mejora.

Monitorear la Implementación y evaluar el plan de ejecución documentando las conclusiones.

ACT (Actuar)

Documentar el ciclo.
Si se han detectado errores parciales en el paso anterior, realizar un nuevo ciclo PDCA con nuevas mejoras.
Si no se han detectado errores relevantes, aplicar a gran escala las modificaciones de los procesos
Si se han detectado errores insalvables, abandonar las modificaciones de los procesos
Ofrecer una Retro-alimentación y/o mejora en la Planificación.

Cuando se utiliza un modelo incremental, el primer incremento a menudo es un producto esencial. Es decir, se afrontan requisitos básicos, pero muchas funciones suplementarias quedan sin extraer. La Empresa utiliza el producto central o sufre la revisión detallada. Como un resultado de utilización y/o de evaluación, se desarrolla un plan para el incremento siguiente. El plan afronta la modificación del producto central a fin de cumplir mejor las necesidades de la Empresa y la entrega de funciones, y características adicionales. Este proceso se repite siguiendo la entrega de cada incremento, hasta que se elabore el producto completo.

El modelo de proceso incremental, como la construcción de prototipos y otros enfoques evolutivos, es iterativo por naturaleza. Se centra en la entrega de un producto operacional con cada incremento. Los primeros incrementos son versiones incompletas del producto final, pero proporcionan al usuario la funcionalidad que precisa y también una plataforma para la evaluación.

Características:

- Las Empresas identifican, a grandes rasgos los servicios que proporcionará el sistema.
- Identifican que servicios son más importantes y cuales menos
- Entonces se definen varios incrementos en donde cada uno proporciona una funcionalidad distinta del sistema.
- Los incrementos que proporcionen servicios con mayor prioridad son desarrollados y entregados primero.
- Una vez que se identifican los incrementos del sistema se definen en detalle los requerimientos para los servicios que se van a entregar en el primer incremento que es inmediatamente desarrollado.
- Durante el desarrollo, se puede llevar a cabo un análisis adicional de requerimientos para los requerimientos posteriores, pero no se aceptan cambios en los requerimientos para el incremento actual.
- Una vez que un incremento se completa y entrega, las Empresas pueden ponerlo en servicio.
- Hay una entrega temprana de partes de la funcionalidad del sistema.

- La Empresa puede experimentar con el sistema, lo que le ayuda a clarificar sus requerimientos para los incrementos posteriores y para las últimas versiones del incremento actual.
- Tan pronto como se completan nuevos incrementos, se integran en los existentes.
- La funcionalidad del sistema mejora con cada incremento entregado.

Ventajas:

1) Las Empresas no tiene que esperar a que se entregue el sistema completo para poder sacarle provecho. El primer incremento satisface los requerimientos más críticos y se puede utilizar inmediatamente.

2) Con un paradigma incremental se reduce el tiempo de implantación inicial, ya que se implementa la funcionalidad parcial.

3) También provee un impacto ventajoso frente a las Empresas, que es la entrega temprana de partes operativas.

4) El modelo proporciona todas las ventajas del modelo en cascada realimentado, reduciendo sus desventajas sólo al ámbito de cada incremento.

5) Permite entregar a la Empresa un sistema más eficiente en comparación del modelo de cascada.

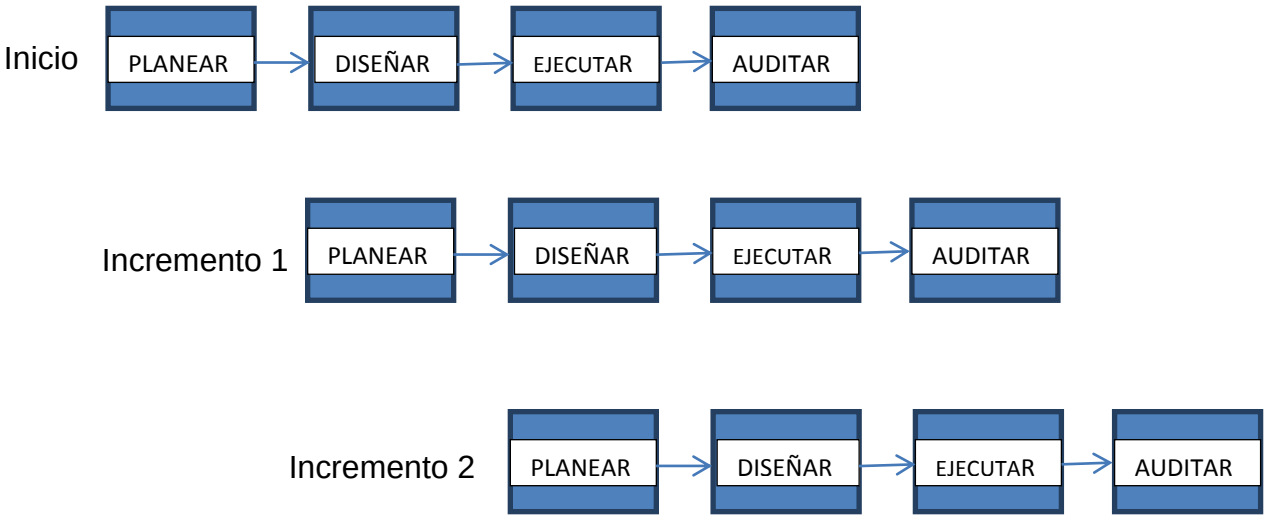
6) Resulta más sencillo acomodar cambios al acotar el tamaño de los incrementos.

7) Por su versatilidad requiere de una planeación cuidadosa tanto a nivel administrativo como técnico.

8) Las Empresas pueden utilizar los incrementos iniciales como prototipos y obtener experiencia sobre los requerimientos de los incrementos posteriores.

9) Existe un bajo riesgo en la falla total del proyecto. Aunque se pueden encontrar problemas en algunos incrementos, lo normal es que el sistema se entregue de manera satisfactoria

Ejemplo de cómo se aplica:



Propuesta de Modelo Incremental para Ciudadanos y Empresas; dirigido a Organismos Reguladores

El modelo propone tres fases recomendables para elevar el Nivel de Cultura sobre la Protección de Datos Personales, entre los Ciudadanos y Empresas atendiendo a las brechas que se han detectado en el presente estudio.

Fase I. "Sensibilización y Concienciación sobre el Conocimiento y Entendimiento de la Ley"

- Elaborar Campañas de Conocimiento y Entendimiento de la Ley dirigidos a los Ciudadanos en el entendido de que será dirigido a personas adultas (mayores de edad).

A través de campañas que conciencien a los ciudadanos para que les muestren el valor de sus datos personales, les simplifiquen el entendimiento de la Ley de una manera más digerible, y hagan hincapié en la exigencia de los Derechos que esta Ley les faculta, ante las Empresas Privadas que posean o puedan poseer sus datos personales.

Con lo anterior se busca extender el entorno del conocimiento de la Ley entre el entorno familiar del Ciudadano; que ya ha sido previamente concienciado, para que esto ayude a permear todas las capas de la sociedad en cuanto a conocimiento de la Ley. Esto es que el Ciudadano con el previo conocimiento que ya tiene sobre la Ley, nos ayudará a fomentar la cultura de la protección de datos inculcándola en su entorno familiar: sobre los niños, jóvenes y adultos mayores, en la medida de sus capacidades promoviendo la importancia de la protección de los datos personales y del valor intrínseco de los mismos. Siendo este uno de los motores que impulse la exigencia de los Derechos de los Titulares (englobando a toda la población, no importando su edad) ante las Empresas del Sector Privado en donde se encuentren sus datos personales.

- Elaborar Campañas de Conocimiento, Entendimiento e Implementación de la Ley dirigido a Empresas del Sector Privado.

Siendo estas campañas de una manera no impositiva y sancionadora esto es que no se infunda miedo sobre el incumplimiento de la Ley; se recomienda que las campañas sean dirigidas de una manera favorecedora para la Empresas, en el entendido que si cumplen con la Ley les puede traer más beneficios como negocio mostrando una imagen de confianza y prestigio ante la población, por estar

apegada a los requerimientos de Ley, al encontrarse siempre actualizada y a la vanguardia.

Fomentar la propagación del: Centro Virtual de FORMACIÓN en Acceso a la Información y Protección de Datos (CEVIFAI) que encontrará en el siguiente link: http://cevifaiprivada.ifai.org.mx/ con el fin de promover la información y capacitación para las Empresas en general (no importando el tamaño) y los Profesionistas independientes.

Fase II. "Ejercicio de Derechos"

.

- Elaborar campañas sobre el conocimiento y entendimiento del Aviso de Privacidad

Para los Ciudadanos difundir a través de los medios de comunicación masiva: campañas sencillas o anuncios que de manera sencilla capten la atención de los titulares, y les sea fácil comprender ¿Qué es un Aviso de Privacidad? el ¿Para que sirve?, su importancia, así como los datos básicos que debe contener.

Así mismo facilitar a los ciudadanos mediante trípticos, guías y preguntas frecuentes, que de manera sencilla ilustren a los mismos, sobre el tema de Aviso de Privacidad, ya sea en portales en internet o mediante trípticos que se entreguen a la población de manera gratuita.

Para el caso de las Empresas Privadas, difundir mediante los medios masivos de comunicación la importancia de tener un Aviso de Privacidad y mediante guías en portales de internet, la forma de cómo elaborar su aviso de privacidad en el caso de que no cuenten con el presupuesto para ser auxiliados por una consultoría, de manera tal que a la medida de sus posibilidades puedan cumplir con el Aviso de Privacidad, pilar básico para la protección de datos personales.

- Elaborar campañas sobre el conocimiento, entendimiento y ejercicio de los Derechos ARCO

Para los Ciudadanos difundir a través de los medios de comunicación masiva: ¿Que son los Derechos ARCO?, el significado de su acrónimo, ¿Para qué sirven? y ¿Ante quiénes los puede ejercer la población? ¿Cuál es el procedimiento para ejercerlo de manera sencilla? etc.; siendo todo esto a través de comerciales que capten la atención de los ciudadanos mediante campañas innovadoras, utilizando un lenguaje claro y sencillo ya que será dirigido a la población en general.

Así mismo poner al alcance de la Población trípticos, guías o preguntas frecuentes en las cuales la población en general pueda tener acceso a esta información sobre

los Derecho ARCO, en un lenguaje claro y sencillo, ya que una vez informado el titular, pueda saber cómo ejercer sus derechos y como elaborar una Solicitud de Derecho ARCO, ante una Empresa que no cuente con un procedimiento definido obligando a esta a apegarse a los requerimiento de Ley y haciendo exigible sus Derechos de una manera previamente informada.

Para las Empresas, difundir a través de los medios de comunicación masiva, la Importancia de contar con un procedimiento para el Ejercicio de los Derechos ARCO el cual como todas las disposiciones de Ley ya es exigible desde enero del 2012. Así mismo poner a disposición de las mismas guías de ayuda para implementar procedimientos sencillos que puedan adoptar las Empresas para la atención de las solicitudes y hacer efectivo el ejercicio de los Derechos ARCO solicitados por los Titulares.

Fase III. "Medidas de Seguridad"

Para los Empresas: Elaborar campañas en medios de difusión que las Empresas consulten más, por el ejercicio de sus funciones, así mismo la SE puede hacerles llegar trípticos o guías que ayuden al conocimiento de estos requerimientos de Ley; esto asegurará que no haya omisiones en el conocimiento de las Medidas de Seguridad que deben implementar de manera general todas las Empresas del Sector Privado.

Estas campañas de difusión serán enfocadas a las Medidas de seguridad con las que deben contar las Empresas, enfatizando las Medidas Físicas y Técnicas como las principales para asegurar la protección de los datos personales.

Propuesta de Modelo Incremental para la Implementación de la LFPDPPP dirigido a Responsables en Empresas del Sector Privado

A modo de desarrollo en fases proponemos las que a continuación se detallan en orden de importancia para que las Empresas puedan aplicar el cumplimiento de la LFPDPPP de forma exitosa y eficiente.

Fase 1)

- Tarea 1) Concienciación a la Dirección, Responsables y resto de personal
- Tarea 2) Asignación de Responsabilidades.
- Tarea 3) Capacitación del Responsable y Encargados

Conocer los organismos que regulan los derechos de los titulares (IFAI).

La privacidad consiste en la habilidad de cada individuo de controlar qué información revela de uno mismo en las empresas, y controlar quién puede acceder a ella.

Dado el valor que tiene esta información, y las repercusiones negativas que puede tener su uso inadecuado, es necesario concienciar a los titulares de la importancia de la privacidad.

El titular debe velar sobre la información que publica o facilita a terceros, valorando la relevancia que puede tener ahora y en un futuro.

Lo aconsejable es pensar antes de publicar. Preguntas como ¿me permite controlar mi información personal, quién puede acceder a ella o cuándo y dónde se publica?, nos ayudarán a ser conscientes de las implicaciones de publicar información personal

Cursos on-line sobre privacidad gratuitos

https://formacion-online.inteco.es/inscripcion/index.php?area=5

Curso de Privacidad: Adecuación y Cumplimiento

Curso introductorio a los diversos aspectos y facetas de la Privacidad, desde el punto de vista de la adecuación y el cumplimiento. Enfocado a pymes, pero dada la generalidad de los conceptos e ideas tratadas, también puede estar dirigido a todo tipo de organizaciones

Privacidad y seguridad para menores. Curso para padres y educadores

Internet es una herramienta muy útil y que los menores utilizan prácticamente para todo. El uso del ordenador es algo natural para ellos, la mayoría han tenido un ordenador en su casa desde que nacieron, por este motivo se les llama nativos digitales. Sin embargo, aunque su conocimiento de las nuevas tecnologías es muy bueno y realizan las cosas de forma prácticamente innata, muchas veces, no son conscientes de los peligros que se pueden encontrar en Internet. En este curso se explica el uso que los menores suelen hacer de Internet, qué peligros pueden entrañar cada una de esas actividades y cómo evitarlos. Este curso también pretende dar soporte a profesores y padres sobre cómo orientar a los menores en la realización del curso análogo para menores (también disponible en esta página), facilitándoles su gestión y seguimiento. Público objetivo del curso: padres/madres y formadores que están preocupados por la seguridad de los menores en Internet

Fase 2)

- Tarea 1) Análisis de Procesos donde se traten Datos Personales
- Terea 2) Documentación de Procesos responsabilidades y Controles existentes
- Tarea 3) Documentación de Sistemas y Soportes que tratan Datos Personales, ciclo de vida de la información de datos personales y personal que trata
- Tarea 4) Elaboración de Avisos de Privacidad y publicación
- Tarea 5) Elaboración de Procesos Gestión de Incidentes y ARCO, asignación de responsabilidades y publicación

En esta Fase es destacable que aquellas organizaciones que cuentan con certificaciones tales como ISO9000 les es natural elaborar estas tareas ya que son inherentes al sistema de gestión, el control documental y de los procesos.

En Europa (donde la aplicación de las normas ISO están muy extendidos) el apoyo al cumplimiento de las Leyes tales como las de Privacidad no constituye un

obstáculo, más bien es un habilitador de la implantación del cumplimiento de las normas y regulaciones.

ISO 9000 es un conjunto de normas sobre calidad y gestión de calidad, establecidas por la Organización Internacional de Normalización (ISO). Se pueden aplicar en cualquier tipo de organización o actividad orientada a la producción de bienes o servicios. Las normas recogen tanto el contenido mínimo como las guías y herramientas específicas de implantación como los métodos de auditoría. El ISO 9000 especifica la manera en que una organización opera sus estándares de calidad, tiempos de entrega y niveles de servicio. Existen más de 20 elementos en los estándares de esta ISO que se relacionan con la manera en que los sistemas operan

Su implantación, aunque supone un duro trabajo, ofrece numerosas ventajas para las empresas, entre las que se cuentan con:

- Estandarizar las actividades del personal que trabaja dentro de la organización por medio de la documentación;
- Incrementar la satisfacción del cliente;
- Medir y monitorizar el desempeño de los procesos;
- Disminuir reprocesar;
- Incrementar la eficacia y/o eficiencia de la organización en el logro de sus objetivos;
- Mejorar continuamente en los procesos, productos, eficacia, etc., entre otros;
- Reducir las incidencias negativas de producción o prestación de servicios

Fase 3)

- Tarea 1) Análisis de Riesgos
- Tarea 2) Análisis de Brechas
- Tarea 3) Propuestas de Planes de Acción
- Tarea 4) Formación y entrenamiento de Controles aplicables a personal que trate Datos Personales

Como base para la implantación de la Privacidad, se debe realizar un análisis de riesgos previo que permitida identificar los activos críticos y el riesgo al que están sometidos.

El Análisis de Riesgos permite identificar y determinar el mapa de riesgos a los que está expuesta la empresa, así como establecer los mecanismos y pasos a dar para el tratamiento de los mismos.

Tras el análisis de Riesgos se aplicarán los análisis de brechas consistentes en evaluar la suficiencia de los controles existentes y los necesarios para la empresa.

Como consecuencia de estos análisis de Riesgos y Brechas y adecuándose a los presupuestos y objetivos empresariales se elaborarán los planes de acción donde se incluyen los planes de capacitación y entrenamiento de los nuevos controles

Fase 4)

- Tarea1) Establecimiento de Controles Periódicos de Verificación
- Tarea2) Elaboración de Sistema documental y de Planes de Auditoría

Los controles como las incidencias y los fallos deben revisarse de forma preventiva para analizar sus causas y mejorar los controles existentes en la empresa.

Como apoyo y parte fundamental se deben registrar todos los documentos tales como políticas, procesos, procedimientos e incidencias.

En el afán de prevenir acciones no deseadas las auditorías nos alertan de las desviaciones y malfuncionamiento de los controles y debilidades en los procesos y procedimientos, ayudándonos a mejorar los sistemas.

Alcanzar los mejores resultados, **no es labor de un día**. Es un proceso progresivo en el que no puede haber retrocesos. Han de cumplirse los objetivos de la empresa, y prepararse para los próximos retos.

Lo deseable es mejorar un poco día a día, y **tomarlo como hábito**, y no dejar las cosas tal como están, teniendo altibajos. Lo peor es un rendimiento irregular. Con estas últimas situaciones, no se pueden predecir los resultados de la organización, porque los datos e información, no son fiables ni homogéneos. Cuando se detecta un problema, la respuesta y solución, ha de ser inmediata. No nos podemos demorar, pues podría originar consecuencias desastrosas.

La mejora continua implica tanto la implantación de un Sistema como el aprendizaje continuo de la organización, el seguimiento de una filosofía de gestión, y la participación activa de todo las personas.

Índice de Gráficos

Bibliografía

1. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Estándares Internacionales sobre Protección de Datos Personales y Privacidad Resolución de Madrid, Madrid, 2009, 36 pp.
2. CEDRIC LAURANT CONSULTING Y PRIVACY INTERNATIONAL, Guida de privacidad para Hispano hablantes 2012 , Hungría, Proyecto realizado en el año 2010 por Privacy International, (EPIC) y el Centro de Medios de Comunicación y Ciencias de la Comunicación (CMCS) de la Central EuropeanUniversity (CEU) de Budapest, 206 pp.
3. CHIRINO A. CARBAJAL, El camino hacia la regulación normativa del Tratamiento de datos personales en Costa Rica, Costa Rica, 2003, [s/p.]
4. COMISIÓN DE GOBERNACIÓN, LXI legislatura de la Cámara de Diputados Dictamen con proyecto de decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforma los artículos 3, fracciones II y VII, y 33, así como la denominación del capítulo II del título segundo de la ley federal de trasparencia y acceso a la información pública gubernamental 25 de marzo 2010
5. CRISTOS VELASCO SAN MARTÍN, Boletín No 1 Política de Informática, Privacidad y protección de datos personales en Internet ¿Es necesario contar con una regulación específica en México?, 2003, 12 pp.
6. EUROPEA COMMISSIO , Comparative study on Differet Approaches to new privacy Challeges, in Particular in the light of TechologicalDevelopmets ,B.1 United States of America, by Chris Hoofnagle f, 2010, LRDP KA TOR Ltd (Leader) In association with Centre for Public Reform, 34 PP.
7. EUROPEA COMMISSIO , Comparative study on Differet Approaches to new privacy Challeges, in Particular in the light of TechologicalDevelopmets ,B.5 JAPAN, by Graham Greenleaf, 2010, LRDP KA TOR Ltd (Leader) In association with Centre for Public Reform, 34 PP.
8. GABRIEL SÁNCHEZ PÉREZ, ISAI ROJAS GONZÁLEZ , Leyes de protección de datos personales en el mundo y la protección de datos biométricos – Parte I, México, 2012, [s /p].

9. GÓMEZ MARCELO M. , Introducción a la Metodología de la investigación Científica, Argentina , 2006 , Editorial Brujas, 189 PP.

10. INSITUTO FEDERAL DEL ACCESO A LA INFORMACIÓN PÚBLICA, La Protección de Datos Personales en México: Una Propuesta para deliberar, México, 2008, 11 pp.

11. ISSA LUNA PLA, Artículo "La Protección de datos personales en el Distrito Federal" En la Biblioteca Jurídica virtual de la UNAM. [s/p.]

12. IRIARTE, E., Estado situacional y perspectiva del Derecho Informático en América latina y el caribe, Cepal, Naciones Unidas

13. JOSÉ ÁLVARO QUIROGA LEÓN, La Ley y la Autoridad Nacional de Protección de Datos Personales en el Perú, OCDE, 8 pp

14. NACIONES UNIDAS, Directrices para la regulación de los archivos de datos personales informatizados, 3 pp.

15. NACIONES UNIDAS ,IRIARTE E., Estado situacional y perspectiva del Derecho Informático en América latina y el caribe, Cepal, [s /p]

16. ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS, Resumen de Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales, París, 2002, 12 pp.

17. TERRAZA HENG MUI KENG, Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico (APEC), Singapur, 2005, 39 pp.

18. VAN HAREN PUBLISHING, ISO/IEC 20000 una Introducción, it SMF España, 2008, Holanda, ITSM LIBRAY, 261 pp.

Artículos de Noticias:

1. CATHERINE GRANIC, Estados Unidos anuncia ley para proteger la privacidad en Internet, 2012, levelup, en la página < http://www.levelup.com/noticias/17918/Estados-Unidos-anuncia-ley-para-proteger-la-privacidad-en-Internet/> [s/p].

2. COMPUTERWORLD, E.U.A. considera que la nube es clave para mejorar la protección de datos, 2012, México [s/p].

3. EQUIPO DE REDACCIÓN, " Ley de protección de datos, ignorada" , 2012 , elempresario.com, <http://elempresario.mx/actualidad/ley-proteccion-datos-ignorada> [s/p].

4. IDG News, China propone normas internacionales para regular internet, 2011, [s/p].

5. PALAZZI P., La transmisión internacional de datos personales y la protección de la privacidad, Argentina, [s./p].

Internet:

1. Antonio Oliveros Dávila, Ley Federal de Protección de Datos Personales en Posesión de Particulares, <http://www.magazcitum.com.mx/?p=1169>, (5/03/2012), [s/p].

2. CANADIAN PRIVACY LAW, de la página, <htpp: //es.wikipedia.org/wiki.> (18 de Junio del 2012), [s/p].

3. CHEN MOK, SUSAN, Privacidad y protección de datos: Un análisis de legislación comparada, http://www.scielo.sa.cr fecha de actualización, (agosto 2010), [s/p].

4. CRISTOS VELASCOS, Ley de Protección de Datos de Costa Rica, México 2012, <http://protecciondatos.mx/2011/09/es-ley-de-proteccin-de-datos-de-costa-rica-encosta-ricas-data-protection-law/> [s/p].

5. ITNEWS, ¿Qué es Cloud Computing?, de la página <http://www.itnews.ec/marco/000035.aspx> (18 de junio de 2012), [s/p].

6. Ley Orgánica 15/99 de Protección de Datos de Carácter Personal (LOPD), España, < http: //protecciónde datos.urjc.es/pd/legislación/index.php> [s/p]

7. PERU CONSUME, Ley Nº 29733, Ley de Protección de Datos Personales, Perú, [s/p].

8. RIASCOS GÓMEZ, LIBARDO ORLANDO, La Visión Constitucional del Habeas Data, <http://www.informatica-juridica.com/trabajos/La_vision_constitucional_del_habeas_data.asp>, (16/06/12)

9. SECRETARIA DE ECONOMÍA, Artículo El reglamento de la Ley de Protección de Datos Personales ya está en Consulta Pública, México,

<http://www.economia.gob.mx/eventos-noticias/sala-de-prensa/comunicados/6598-el-reglamento-de-la-ley-de-proteccion-de-datos-personales-ya-esta-en-consulta-publica>, (12/01/2012), [s/p].

10. MAGAZINE PREMIUM 2010 http://www.magazcitum.com.mx/?p=866

11. REVISTA SEGURIDAD DEFENSA DIGITAL de la Dirección General de Computo y Tecnologías de Información y Comunicación de la UNAM, <http://revista.seguridad.unam.mx/numero-08/c%C3%B3mputo-en-nube-ventajas-y-desventajas> (11/11/2010)

Agencias de Protección de Datos Personales

- http://www.jus.gov.ar/datos-personales.aspx/
- http://www.oipc.ab.ca/pages/home/default.aspx
- http://www.datospersonales.gub.uy/sitio/
- http://www.agpd.es/portalwebAGPD/index-ides-idphp.php

AUREN IBEROAMERICA

WTC, MONTECITO N° 38, PISO 33 – 11, COL. NÁPOLES, C.P 03810

Tel. : 55- 5638 0726