Universidad Michoacana de San Nicolás de Hidalgo

Facultad de Contaduría y Ciencia Administrativas

Tesina:
Análisis de la Legislación para la Protección de Datos Personales en el Estado de Michoacán

Para obtener el Título de:
Licenciado en Informática Administrativa

Immer Izaac Ventura Pérez

Asesor: M.A. Bruno Ramos Ortiz

Morelia Mich. Diciembre 2012

Índice

Dedicatoria

A Dios.

Por haberme permitido llegar hasta este punto y haberme dado salud, sabiduría para lograr mis objetivos, además de su infinita bondad y amor.

A mis padres.

Por el apoyo que me brindaron, los ejemplos de perseverancia y constancia que lo caracterizan y que me ha infundado siempre, por el valor mostrado para salir adelante y por su amor.

A mis familiares.

A mis hermanos por apoyarme moral y económicamente en la carrera.
¡Gracias a ustedes!

A mis maestros.

Bruno Ramos Ortiz por su gran apoyo y motivación para la culminación de Nuestros estudios profesionales y para la elaboración de esta tesina.

Al Lic. Erik Alfaro calderón, Dr. Pedro Chávez Lugo, MC Gustavo Gutiérrez Carreón por su apoyo, su tiempo Compartido y por impulsar el desarrollo de nuestra formación profesional, por apoyarnos en su momento. Y a nuestro padrino de generación MA Alberto Casimiro Andrade.

A la **Universidad Michoacana de San Nicolás de Hidalgo** y en especial a la **Facultad de contaduría y ciencias administrativas** por permitirme ser parte de una generación de triunfadores y gente productiva para el país.

Agradecimientos

Me gustaría que estas líneas sirvieran para expresar mi más profundo y sincero agradecimiento a todas aquellas personas que con su ayuda han colaborado en la realización del presente trabajo.

Un agradecimiento muy especial merece la comprensión, paciencia y el ánimo recibidos de mi familia y mi novia lulú. A todos ellos, muchas gracias.

Introducción

En un mundo con gran despliegue tecnológico y donde la economía gira en torno a la información, es de extrema importancia contar con una legislación que proteja los datos personales. Los sistemas de información se han constituido como una base imprescindible para el desarrollo de cualquier actividad empresarial y gubernamental; estos sistemas han evolucionado de forma extraordinariamente veloz, aumentando la capacidad de gestión y almacenamiento. El crecimiento ha sido constante a lo largo de las últimas décadas, sin embargo, esta evolución tecnológica también ha generado nuevas amenazas y vulnerabilidades para las organizaciones.

Para (wiener n. , 1985) La legislación informática, como una nueva rama del conocimiento jurídico, es una disciplina en continuo desarrollo, las alusiones más específicas sobre ésta, se tienen a partir del año de 1949 , en donde expresa la influencia que ejerce la cibernética respecto a uno de los fenómenos sociales más significativos: el jurídico. Se puede decir que la legislación informática es un conjunto de reglas jurídicas de carácter preventivo y correctivo derivadas del uso de la informática.

Por otra parte, dicha reglamentación deberá contemplar las siguientes problemáticas debidamente identificadas:

- Regulación de los bienes informáticos. Ya que la información como producto informático requiere de un tratamiento jurídico en función de su innegable carácter económico.
- Protección de datos personales. Es decir, el atentado a los derechos fundamentales de las personas provocado por el manejo inapropiado de informaciones nominativas.
- Flujo de datos transfronterizos. Con el favorecimiento o restricción en la circulación de datos a través de las fronteras nacionales.
- Protección de los programas. Como resolución a los problemas provocados por la llamada “piratería” de programas de cómputo.
- Delitos informáticos. Como la comisión de verdaderos actos ilícitos en los que tenga a las computadoras como instrumentos o fin.
- Contratos informáticos. En función de esta categoría contractual sui géneris con evidentes repercusiones fundamentalmente económicos.
- Ergonomía informática. Como aquellos problemas laborales suscitados por la informatización de actividades.

Planteamiento del tema

El avance tecnológico en materia de informática en las últimas décadas ha sido extraordinariamente rápido y cada vez más incide en múltiples facetas de la actividad humana. En los últimos años, esto ha ido extendiéndose de manera importante hasta alcanzar a la población en general. De manera particular, el uso de información a través de sistemas digitales, ha permitido nuevas y más eficientes formas de prestar servicios a la población con elementos como el comercio electrónico, los servicios que ofrecen diferentes instancias del gobierno, sistemas de información y bases de datos, etc.

En cuanto a este tema de la protección de datos personales el estado de Michoacán se encuentra rezagado frente a los demás países y estados ya que no existe una regulación específica. Es cada vez más clara la necesidad de que se brinde al ciudadano una protección adecuada contra el posible mal uso de la información que le concierne, sin que esto implique un intento de limitar o restringir los beneficios que pueden aportar las tecnologías de información. Lo anterior deriva de que las nuevas tecnologías informativas ofrecen nuevas y más flexibles maneras de utilizar la información de manera inadecuada, poco ética y posiblemente perjudicial para el sujeto de la misma. Por ejemplo, los archivos tradicionales hacían muy difícil que pudiera cruzarse información de diferentes documentos, mientras que, estando digitalizada, esto resulta muy sencillo y rápido. Es claro que estas facilidades no son negativas, pero ofrecen a personas maliciosas, posibilidades nuevas, que conviene configurar como delictivas para protección de los individuos que pudieran ser afectados.

Justificación del tema

En el estado de Michoacán no cuenta con una legislación sobre la protección de datos y esto nos lleva a evitar que los datos sean utilizados para una finalidad distinta para la cual la proporcionaste, evitando con ello se afecten otros derechos y libertades, por ejemplo que se utilice de forma incorrecta cierta información de salud lo que podría ocasionar una discriminación laboral, entre otros supuesto es por eso analizaremos países y estados de cómo se está llevando a cabo la protección de datos personales .
Realizaremos una investigación para darnos cuenta de cómo están funcionando la legislación sobre la protección de datos personales en nuestro estado, en la república mexicana y otros países.
Analizaremos hasta qué punto están regulados y Órgano encargado de la protección de Datos Personales. Con esta información se pretende que al final de la investigación podamos determinar las acciones a realizar en nuestro estado y hacer las recomendaciones para actualizarlo en materia protección de datos personales.

Objetivo

General

Brindar un análisis de como el estado de Michoacán está regido por la protección de datos personales que permitirá comprender la situación actual y el nivel de seguridad con que cuenta cada usuario así como en el ámbito público como privado.

Particulares

- Dar a Conocer los términos y conceptos legales vinculados con el derecho informático, tipos de delitos informáticos y sobre que es la protección de datos personales.
- Analizaremos diferente países de cómo están legislada la protección de datos, los diferentes artículos en donde están regidos y algunos fraudes cometidos en esos países.
- Conocer el proceso legislativo para poder implementar una ley en el estado de Michoacán.
- Identificar cada estado de nuestro país si cuenta con la legislación de protección de datos personales.

Cronograma

	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin
1		Inicio de la Tesina	0 días	lun 13/08/12	lun 13/08/12
2		Analisis del Nombre del Tema, Introduccion del Tema, Plantamiento del Tema, Justificacion del tema, Objetivos Y Cronograma	7 días	mar 14/08/12	mié 22/08/12
3		**Capitulo 1 Marco Teorico**	20 días	jue 23/08/12	mié 19/09/12
4		1.1 Derecho	1 día	jue 23/08/12	jue 23/08/12
5		1.2 Cracion del Derecho	1 día	vie 24/08/12	vie 24/08/12
6		1.3 Funciones del Derecho	1 día	lun 27/08/12	lun 27/08/12
7		1.4 Realizaciones del Derecho	1 día	mar 28/08/12	mar 28/08/12
8		1.5 Derecho Informatico	1 día	mié 29/08/12	mié 29/08/12
9		1.6 Clasificacion del Derecho Informatico	1 día	jue 30/08/12	jue 30/08/12
10		1.7 legislacion	1 día	vie 31/08/12	vie 31/08/12
11		1.8 Legislacion Informatica	1 día	lun 03/09/12	lun 03/09/12
12		1.9 Delitos Informaticos	1 día	mar 04/09/12	mar 04/09/12
13		1.10Tipos de Delitos Informaticos	2 días	mié 05/09/12	jue 06/09/12
14		1.11 Definicion de Datos Personales	1 día	vie 07/09/12	vie 07/09/12
15		1.12 Importancia para la Proteccion de Datos Personales	1 día	lun 10/09/12	lun 10/09/12
16		1.13 Definicion del Derecho a la Proteccion de Datos Personales	1 día	mar 11/09/12	mar 11/09/12
17		1.14 Definion de Aviso de Privacidad	1 día	mié 12/09/12	mié 12/09/12
18		1.15 Proposito del aviso de privacidad	1 día	jue 13/09/12	jue 13/09/12
19		1.16 La informacion	1 día	vie 14/09/12	vie 14/09/12
20		1.17 Clientes	1 día	lun 17/09/12	lun 17/09/12
21		1.18 Metodos Usados para Robar Informacion	1 día	mar 18/09/12	mar 18/09/12
22		1.19 Acciones Ilicitas en la red en los ultimos años	1 día	mié 19/09/12	mié 19/09/12
23		**capitulo 2 marco referencial**	11 días	jue 20/09/12	jue 04/10/12
24		2.1 Proteccion de Datos en Europa	1 día	jue 20/09/12	jue 20/09/12
25		2.2 Proteccion de Datos en America Latina	1 día	vie 21/09/12	vie 21/09/12
26		2.3 Alemania	1 día	lun 24/09/12	lun 24/09/12
27		2.4 Austria	1 día	mar 25/09/12	mar 25/09/12
28		2.5 Chile	1 día	mié 26/09/12	mié 26/09/12
29		2.6 China	1 día	jue 27/09/12	jue 27/09/12
30		2.7 España	1 día	vie 28/09/12	vie 28/09/12
31		2.8 Estados Unidos de America	1 día	lun 01/10/12	lun 01/10/12
32		2.9Francia	1 día	mar 02/10/12	mar 02/10/12
33		2.10 Holanda	1 día	mié 03/10/12	mié 03/10/12
34		2.11 Inglaterra	1 día	jue 04/10/12	jue 04/10/12
35		**capitulo 3 Marco Referencial**	4 días	vie 05/10/12	mié 10/10/12
36		3.1 Proceso Legislativo: iniciativa, discusion, aprobacion, sancion, promulgacion,publicidad, iniciativa de vigencia.	4 días	vie 05/10/12	mié 10/10/12
37		**capitulo 4 Caso Practico**	11 días	jue 11/10/12	jue 25/10/12
38		4.1 fraude de proteccion de datos caso sony	1 día	jue 11/10/12	jue 11/10/12
39		4.2 Estados que cuentan con legislacion en materia de proteccion de datos personales	10 días	vie 12/10/12	jue 25/10/12
40		Conclusiones, aportaciones y sugerencias, citas bibliograficas y fuentes de informacion	5 días	jue 25/10/12	mié 31/10/12

Capítulo 1 Marco teórico

1.1 Derecho

Para Juan Carlos Merodeo López (2008). El derecho Es un conjunto de normas jurídicas que forman un sistema hermético al punto que las soluciones hay que buscarlas en las propias normas, criterio válido durante mucho tiempo y que, por lo demás, hay cierta cuota de certeza que ofrece seguridad jurídica a las relaciones sociales, que se desarrollan en ese lugar. En principio, digamos que es un conjunto de normas de carácter general, que se dictan para regir sobre toda la sociedad o sectores preestablecidos por las necesidades de la regulación social, que se imponen de forma obligatoria a los destinatarios, y cuyo incumplimiento debe acarrear una sanción coactiva o la respuesta del Estado a tales acciones.

La palabra derecho proviene del término latino *directum*, que significa “lo que está conforme a la regla”. El derecho se inspira en postulados de justicia y constituye el orden normativo e institucional que regula la conducta humana en sociedad. La base del derecho son las relaciones sociales, las cuales determinan su contenido y carácter. Dicho de otra forma, el derecho es un conjunto de normas que permiten resolver los conflictos en el seno de una sociedad.

1.2 Creación del Derecho

La producción del Derecho es básicamente estatal y es este otro factor que proporciona coherencia a las disposiciones normativas vigentes. Sin ser defensora de posiciones absolutamente normativistas, y aun cuando entre nosotros esta noción ha sido fuertemente criticada no podemos omitir el hecho de que lo cierto es que sólo aceptando que el Derecho es resultado exclusivo del Estado, la prevalencia de la Constitución respecto a todo el ordenamiento jurídico dictado por los órganos competentes, la sumisión del Estado a la ley y el principio de seguridad jurídica ciudadana serán efectivos.

Como resultado de esta aseveración, las lagunas o vacíos normativos son un sin sentido y el operador jurídico o el juez han de ser capaces de encontrar entre las normas la solución del caso que tienen ante si, han de precisar dentro del conjunto armónico, del “sistema” y adoptar la única respuesta posible al caso, como forma de conservar lo más intacta posible la voluntad predominante.

Y si admitimos que el Derecho no es sólo norma, sino una ciencia, que en tanto expresión de una voluntad política predominante, tiene funciones específicas en la sociedad, él ha de garantizar el interés prevaleciente, permitiendo, mandando o limitando, y a su vez ser cauce de lo que se desea obtener. La expresión de intereses aporta unidad a la normativa vigente.

1.3 Funciones del Derecho

Función proviene de la palabra latina "*FONS*" y en sentido figurado se emplea para significar el principio, fundamento u origen de las cosas materiales o intramateriales, en otras palabras es el lugar donde nace, surge o se origina algo, como si nos remontamos al nacimiento de las fuentes de un Río en él.
En este sentido entendemos por fuente del derecho como todo aquello, objeto, actos o hechos que producen, crean u originan el surgimiento, colacimiento del derecho, es decir, de las entrañas o profundidades de la propia sociedad. Ahora bien las fuentes de derecho se clasifican por su estudio en:

- Fuente Histórica*: Son el conjunto de documentos o textos antiguos entre libros, textos o papiros que encierran el contenido de una ley, ejemplo: Código de Hammurabi*
- *Fuente Real*: Conjunto de factores y elementos que determinan el contenido de una ley, ejemplo: Código penal y civil de un estado.

- *Fuente Formal*: Conjunto de actos o hechos que realiza el estado, la sociedad, el individuo para creación de una ley, ejemplo: El poder legislativo federal; esta fuente contiene:
    - Costumbre
    - Doctrina
    - Jurisprudencia
    - Principios generales de estudio
    - Tratados internacionales
    - Legislación o Ley

1.4 Realización del Derecho

Para que una norma pueda ser eficaz, para que se realice, han de crearse, además, los medios e instituciones que propicien la realización de la disposición, y de los derechos y deberes que de tales situaciones resulten. Pero la eficacia de una norma no puede exigirse sólo en el plano normativo, también ha de ser social, material, para que haya correspondencia entre la norma y el hecho o situación, para que refleje la situación existente o que desee crearse, manifestándose así la funcionalidad del Derecho.
Como resultado de lo anterior, será posible, entonces, que la norma obtenga el consenso activo de sus destinatarios, que sea acatada y respetada conscientemente, sin requerir la presión del aparato coercitivo del Estado.
Requisito previo de la validez normativa es la publicidad en el sentido antes expuesto. La publicación de las normas se hace no solo para dar a conocer el nacimiento de la disposición, el inicio de su vida jurídico formal, sino también para declarar la posibilidad de su exigencia y obligatoriedad para el círculo de destinatarios de la normativa. Aún más, si toda disposición normativa se dicta, por regla general, para que tenga vida indeterminada, para que sea vigente y por tanto válida a partir de la fecha de su publicación si ella no establece lo contrario, el acto de la publicación es vital en su nacimiento y acción posterior.

La validez de una norma de Derecho, entonces, y de la disposición que la contiene y expresa, es un elemento importante para la eficacia de la misma, para el logro de su realización en la sociedad, tal y como se previó. Interesan no sólo la observación de los principios, sino también de ciertas reglas relativas a su elaboración racional, a la creación de instituciones para asegurar su cumplimiento, así como la finalidad que con ellas se persigue, a saber: conservar, modificar, legitimar cambios, así como de la observancia de principios básicos que rigen en cada ordenamiento jurídico.
Por tanto, las disposiciones normativas, de cualquier rango, han de ser resultado del análisis previo con el objetivo de conocer los hechos, sus causas y efectos, regulaciones posibles, sus efectos, para poder determinar cuál es la forma precisa que ha de exigirse o propiciarse, o de la Institución jurídica que desea regularse; del cumplimiento de ciertos requisitos formales en su creación y de la observancia de principios técnicos jurídicos que rigen en un ordenamiento jurídico determinado. Han de crearse, además, los medios e instituciones que propicien el cumplimiento de la disposición, y de los derechos y deberes que de tales situaciones resulten, tanto en el orden del condicionamiento social-material, proveniente del régimen socioeconómico y político imperante, de los órganos que hacen falta para su aplicación, como la normativa legal secundaria y necesaria para instrumentar la norma de Derecho.

1.5 Derecho informático

Para Prof. Dr. Wilhelm steinmuller (1970) El derecho informático, ha sido analizado desde diversas perspectivas. Por un lado el Derecho Informático se define como:

- Un conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el Derecho y la informática.
- Es una rama del derecho especializado en el tema de la informática, sus usos, sus aplicaciones y sus implicaciones legales.

El Derecho informático, estudia las transformaciones que se han producido en el Derecho, a partir de la incorporación de las tecnologías de la información y comunicación (tics) en las instituciones jurídicas, en la sociedad, en el Estado, a partir de nuevos principios, normatividades y instituciones que regularan esta particular forma de ver al Derecho.

1.6 Clasificación del Derecho Informático

El Derecho Informático, se clasifica en dos partes:

1.6.1 Informática Jurídica.

En la informática jurídica se estudia a la tecnología como instrumento que beneficia a la ciencia del derecho. Entonces encontramos a la Informática Jurídica Documental, Informática jurídica de Gestión, la Ofimática, La

informática jurídica decisional, la inteligencia artificial, y los sistemas expertos jurídicos.

1.6.2 Derecho de la Informática.

Estudia a la tecnología como objeto, es decir que se preocupa por las transformaciones que esta ha generado en las instituciones jurídicas, y las relaciones contractuales entre los individuos. Encontramos a los contratos informáticos, delitos informáticos, el teletrabajo, protección de datos personales, comercio electrónico, sociedad de la información, biotecnología y derecho, sguridad de la información, documento electrónico y firma digital.

1.7 Legislación.

http://www.definicionabc.com/derecho/legislacion.php (2007) Se denomina legislación al cuerpo de leyes que regularán determinada materia o ciencia o al conjunto de leyes a través del cual se ordena la vida en un país, es decir, lo que popularmente se llama ordenamiento jurídico y que establece aquellas conductas y acciones aceptables o rechazables de un individuo, institución, empresa, entre otras.

1.8 Legislación informática.

Para Israel Barquera (2011). Define como un conjunto de ordenamientos jurídicos creados para regular el tratamiento de la información. Las legislaciones de varios países han promulgado normas jurídicas que se han puesto en vigor dirigidas a proteger la utilización abusiva de la información.

1.9 Delitos informáticos

- Nidia Callegari define al delito informático como “aquel que se da con la ayuda de la informática o de técnicas anexas”. Este concepto tiene la desventaja de solamente considerar como medio de comisión de esta clase de delitos a la informática, olvidándose la autora que también que lo informático puede ser el objeto de la infracción.
- Davara Rodríguez define al Delito informático como, la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.
- Julio Téllez Valdés conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a “las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin” y por las segundas “actitudes ilícitas en que se tienen a las computadoras como instrumento o fin”.
- Parker define a los delitos informáticos como “todo acto intencional asociado de una manera u otra a los computadores; en los cuales la víctima ha o habría podido sufrir una pérdida; y cuyo autor ha o habría podido obtener un beneficio”17, Parker además entrega una tabla en que la que se definen los delitos informáticos de acuerdo a los propósitos que se persiguen:

1. Propósito de investigación de la seguridad: abuso informático es cualquier acto intencional o malicioso que involucre a un computador como objeto, sujeto, instrumento o símbolo donde una víctima sufrió o podría haber sufrido una pérdida y el perpetrador obtuvo o pudo haber obtenido una ganancia (Parker, Nycum and Oura, 1973).
2. Propósito de investigación y acusación: delito informático es cualquier acto ilegal cuya perpetración, investigación o acusación exige poseer conocimientos de tecnología informática (Departamento de Justicia de Estados Unidos).
3. Propósito legal: delito informático es cualquier acto tal como está especificado en una ley sobre delito informático en la jurisdicción en que la norma se aplica.
4. Otros propósitos: abuso informático (sea cual sea su objetivo), es cualquier delito que no puede ser cometido sin computador.

1.10 Tipos de delitos informáticos

1.10.1 Los datos falsos o engañosos (Data diddling).

Conocido también como introducción de datos falsos, es una manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en transacciones de una empresa. Este tipo de fraude informático conocido también como manipulación de datos de entrada, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

1.10.2 Manipulación de programas o los "caballeros de Troya" (Troya Horses).

Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

1.10.3 La técnica del salami (Salami Technique/Rounching Down).

Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra. Y consiste en introducir al programa unas instrucciones para que remita a una determinada cuenta los céntimos de dinero de muchas cuentas corrientes.

1.10.4 Falsificaciones informáticas.

Como objeto: Cuando se alteran datos de los documentos almacenados en forma computarizada. Como instrumentos: Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color basándose en rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer reproducciones de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

1.10.5 Manipulación de los datos de salida.

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían basándose en tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

1.10.6 Pishing.

Es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños.

1.10.7 Spear pishing.

Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes. El robo de identidad es uno de los delitos que más ha aumentado. La mayoría de las víctimas son golpeadas con secuestros de cuentas de tarjetas de crédito, pero para muchas otras la situación es aún peor. En los últimos cinco años 10 millones de personas han sido víctimas de delincuentes que han abierto cuentas de tarjetas de crédito o con empresas de servicio público, o que han solicitado hipotecas con el nombre de las víctimas, todo lo cual ha ocasionado una red fraudulenta que tardará años en poderse desenmarañar. En estos momentos también existe una nueva modalidad de Pishing Dr. Santiago Acurio Del Pino Delitos Informáticos 25 que es el llamado Spear Pishing o Pishing segmentado, el cual ataca a grupos determinados, es decir se busca grupos de personas vulnerables a diferencia de la modalidad anterior.

1.10.8 El sabotaje informático.

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

1.10.8.1 Bombas lógicas (LOGIC BOMBS).

Es una especie de bomba de tiempo que debe producir daños posteriormente. Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

1.10.8.2 Gusanos.

Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

1.10.8.3 Virus informáticos y malware.

son elementos informáticos, que como los microorganismos biológicos, tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian de un sistema a otro, exhiben diversos grados de malignidad y son eventualmente, susceptibles de destrucción con el uso de ciertos antivirus, pero algunos son capaces de desarrollar bastante resistencia a estos.

El malware es otro tipo de ataque informático, que usando las técnicas de los virus informáticos y de los gusanos y las debilidades de los sistemas desactiva los controles informáticos de la máquina atacada y causa que se propaguen los códigos maliciosos.

1.10.8.4 Ciber terrorismo.

Terrorismo informático es el acto de hacer algo para desestabilizar un país o aplicar presión a un gobierno, utilizando métodos clasificados dentro los tipos de delitos informáticos, especialmente los de los de tipo de Sabotaje, sin que esto pueda limitar el uso de otro tipo de delitos informáticos, además lanzar un ataque de terrorismo informático requiere de muchos menos recursos humanos y financiamiento económico que un ataque terrorista común.

1.10.8.5 Ataque de denegación de servicio.

Estos ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a mucho usuarios Ejemplos típicos de este ataque son:

El consumo de memoria de la máquina víctima, hasta que se produce un error general en el sistema por falta de memoria, lo que la deja fuera de servicio, la apertura de cientos o miles de ventanas, con el fin de que se pierda el foco del ratón y del teclado, de manera que la máquina ya no responde a pulsaciones de teclas o de los botones del ratón, siendo así totalmente inutilizada, en máquinas que deban funcionar ininterrumpidamente, cualquier interrupción en su servicio por ataques de este tipo puede acarrear consecuencias desastrosas.

1.10.9 El espionaje informático y el robo o hurto de software.

1.10.9.1 Fuga de datos (data leakege).

También conocida como la divulgación no autorizada de datos reservados, es una variedad del espionaje industrial que sustrae información confidencial de una empresa. A decir de Luis Camacho Loza, "la facilidad de existente para efectuar una copia de un fichero mecanizado es tal magnitud en rapidez y simplicidad que es una forma de delito prácticamente al alcance de cualquiera. La forma más sencilla de proteger la información confidencial es la criptografía.

1.10.9.2 Reproducción no autorizada de programas informáticos de protección legal.

Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, considero, que la reproducción no autorizada de programas informáticos no es un delito informático, debido a que, en primer lugar el bien jurídico protegido es en este caso el derecho de autor, la propiedad intelectual y en segundo lugar que la protección al software es uno de los contenidos específicos del Derecho informático al igual que los delitos informáticos, por tal razón considero que la piratería informática debe ser incluida dentro de la protección penal al software y no estar incluida dentro de las conductas que componen la delincuencia informática.

1.10.10 El robo de servicios

1.10.10.1 hurto del tiempo de la computadora.

Consiste en el hurto del tiempo de uso de las computadoras, un ejemplo de esto es el uso de Internet, en el cual una empresa proveedora de este servicio proporciona una clave de acceso al usuario de Internet, para que con esa clave pueda acceder al uso de la supercarretera de la información, pero sucede que el usuario de ese servicio da esa clave a otra persona que no esta autorizada para usarlo, causándole un perjuicio patrimonial a la empresa proveedora de servicios.

1.10.10.2 Apropiación de informaciones residuales (SCAVENGING).

Es el aprovechamiento de la información abandonada sin ninguna protección como residuo de un trabajo previamente autorizado. To scavenge, se traduce en recoger basura. Puede efectuarse físicamente obteniendo papel de desecho de papeleras o electrónicamente, tomando la información residual que ha quedado en memoria o soportes magnéticos.

1.10.10.3 Parasitismo informático (PIGGYBACKING) y su suplantación de personalidad (IMPERSONATION).

En estos casos, el delincuente utiliza la suplantación de personas para cometer otro delito informático. Para ello se prevale de artimañas y engaños tendientes a obtener, vía suplantación, el acceso a los sistemas o códigos privados de utilización de ciertos programas generalmente reservados a personas en las que se ha depositado un nivel de confianza importante en razón de su capacidad y posición al interior de una organización.

1.10.10.4 Las puertas falsas (TRAP DOORS).

Consiste en la práctica de introducir interrupciones en la lógica de los programas con el objeto de chequear en medio de procesos complejos, si los resultados intermedios son correctos, producir salidas de control con el mismo fin o guardar resultados intermedios en ciertas áreas para comprobarlos más adelante.

1.10.10.5 La llave maestra (SUPERZAPPING).

Es un programa informático que abre cualquier archivo del computador por muy protegido que esté, con el fin de alterar, borrar, copiar, insertar o utilizar, en cualquier forma no permitida, datos almacenados en el computador. Su nombre deriva de un programa utilitario llamado **superzap**, que es un programa de acceso universal, que permite ingresar a un computador por muy protegido que se encuentre, es como una especie de llave que abre cualquier rincón del computador. Mediante esta modalidad es posible alterar los registros de un fichero sin que quede constancia de tal modificación

1.10.10.6 Pinchado de líneas (WIRETAPPING).

Consiste en interferir las líneas telefónicas de transmisión de datos para recuperar la información que circula por ellas, por medio de un radio, un módem y una impresora. Como se señaló anteriormente el método más eficiente para proteger la información que se envía por líneas de comunicaciones es la criptografía que consiste en la aplicación de claves que codifican la información, transformándola en un conjunto de caracteres ininteligibles de letras y números sin sentido aparente, de manera tal que al ser recibida en destino, y por aplicación de las mismas claves, la información se recompone hasta quedar exactamente igual a la que se envió en origen.

1.10.10.7 Piratas informáticos o hackers.

El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias

en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento.

1.11 Definición datos personales

Para **www.ifai.mx** (2012) Los datos personales son cualquier información que refiera a una persona física que pueda ser identificada a través de los mismos, los cuales se pueden expresar en forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, como por ejemplo: nombre, apellidos, CURP, estado civil, lugar y fecha de nacimiento, domicilio, número telefónico, correo electrónico, grado de estudios, sueldo, entre otros. Dentro de los datos personales hay una categoría que se denomina “datos personales sensibles”, que requieren especial protección, ya que refieren a información que pueda revelar aspectos íntimos de una persona o dar lugar a discriminación, como el estado de salud, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, origen racial o étnico y preferencia sexual.

Los dueños de los datos personales son las personas a las que corresponden esos datos. Tu información personal te pertenece, tú eres su titular y quien decide sobre ella.

1.12 importancia para la protección datos personales

Tu información personal es valiosa, por lo que debes cuidarla como lo harías con cualquier otro bien con valor e importancia para ti. En particular, la protección de los datos personales se hace necesaria en la sociedad de la información en la que vivimos, donde el uso de las Tecnologías de la Información (TI) permite comunicar, compartir y utilizar datos personales en cuestión de segundos, de manera masiva y constante, casi ilimitada, y sin mayores complicaciones. Sin duda, las TI han colaborado a mejorar la calidad y condiciones de vida de la sociedad en general. Sin embargo, aunado a sus bondades, su desarrollo lleva implícitos retos para la privacidad, en virtud del uso intensivo que le damos a nuestra información a través de herramientas tecnológicas como el Internet, redes sociales, blogs, teléfonos celulares inteligentes (smartphones), conversaciones en línea, entre otros. Por ejemplo, cuántos de nosotros, de alguna u otra forma, hemos sido objeto de violaciones o amenazas a nuestra privacidad o datos personales, cuando:

- Nos solicitan datos personales a través de páginas “piratas” de Internet.
- Nos envían correos electrónicos no deseados, donde nos ofrecen productos o servicios de diversas empresas.
- Malintencionadamente se apoderan y utilizan tu usuario y contraseña para suplantar tu identidad digital, haciéndose pasar por ti.

- Nos enteramos que nuestros datos personales los tiene una empresa con la que no tenemos contacto alguno.
- Nos llaman para ofrecernos tarjetas bancarias.

1.13 Definición del derecho a la protección de los datos personales

Es probable que se conozca el significado del término “privacidad” o “confidencialidad”, pero ¿sabes a lo que nos referimos cuando hablamos de “protección de datos personales”? La protección de datos personales es un derecho humano que le da a los individuos el poder de controlar la información personal que comparten con terceros, así como el derecho a que ésta se utilice de forma adecuada, para permitir el ejercicio de otros derechos y evitar daños a su titular. Nuestra Constitución Política, en su artículo 16, reconoce el derecho a la protección de datos personales como una garantía individual, al señalar que 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.

1.14 Definición de aviso de privacidad

Para **www.ifai.mx** (2012). Aviso de privacidad es un Documento físico, electrónico o en cualquier otro formato (cómo puede ser visual o sonoro) generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con lo que establece la Ley. El aviso de privacidad es una declaración que informa al titular de los datos personales

- quién recaba (responsable),
- qué recaba (información que se recaba)
- para qué recaba (las finalidades del tratamiento)
- cómo limitar el alcance (uso o divulgación)
- cómo revocar consentimiento
- cómo ejercer derechos ARCO (medios)
- cómo comunica cambios al aviso (procedimiento y medio)
- si se acepta o no que los datos se comuniquen a terceros (transferencias)
- en su caso, si se recaban datos sensibles.

1. 15 Propósito del aviso de privacidad

El aviso de privacidad tiene como propósito principal hacer del conocimiento del titular de los datos personales, primero, que su información personal será recabada y utilizada para ciertos fines, y segundo, las características del tratamiento al que serán sometidos sus datos personales. Lo anterior con el fin legítimo de que el titular tome decisiones informadas con relación a sus datos personales y controle el uso de su información personal. Adicionalmente, el aviso de privacidad permite al responsable del tratamiento de los datos:

- Fortalecer el nivel de confianza entre responsable y titular con relación al tratamiento de su información personal .

- Transparentar al titular las finalidades y transferencias a que son sometidos sus datos personales.
- Informar al titular cómo ejercer los derechos que la ley le otorga.

1.16 La Información

Para Dominic Welsh (1988). La **información** es un conocimiento explícito extraído por seres vivos o sistemas expertos como resultado de interacción con el entorno o percepciones sensibles del mismo entorno. En principio la información, a diferencia de los datos o las percepciones sensibles, tienen estructura útil que modificará las sucesivas interacciones del ente que posee dicha información con su entorno. La naturaleza de la información incide debido a que tiene características distintas de la materia y la energía, que son elementos cuya normatividad es más conocida y de uso general. Entre otros, pueden destacarse los siguientes conceptos relacionados con la información y sus características principales:

- La información no tiene existencia física. Normalmente se le define como el significado de los datos. En términos técnicos, es una comunicación que reduce el grado de incertidumbre de un receptor.
- Los datos a su vez, son el resultado de una observación directa o los resultados de un fenómeno y tampoco tienen una existencia física "per se". Normalmente se reflejan en un soporte físico en el que son representados, como pueden ser: marcas de un lápiz en una hoja de papel, marcas magnéticas en un disco duro de computadora, o impulsos eléctricos enviados por un alambre en una conversación telefónica.
- La información es un recurso. Tiene un valor comercial y un costo de producción. También tiene implicaciones estratégicas, políticas y comerciales importantes.
- La información, a diferencia de otros recursos, puede repetidas veces sin que se desgaste ni se pierda. En su forma electrónica o digital, la información tiene además las características siguientes:

- Puede moverse a grandes distancias a velocidades muy altas y con muy bajos costos. Esto implica que no existan restricciones importantes para su transferencia entre ubicaciones geográficas.

- Puede ser modificada, adaptada, revisada o corregida de manera muy fácil y flexible. Muchas veces estas modificaciones pueden tener impactos importantes y pueden presentarse sin que sea viable o simple poder detectarlas. Esto implica nuevas formas de controlar la exactitud, integridad y confiabilidad de la información.
- Permite que se analice, estructure, y procese de manera rápida, eficiente y con costos muy reducidos. Por lo tanto, ofrece nuevas posibilidades de extraer elementos y conclusiones que de otro modo resultarían muy inconvenientes o no realizables.
- Permite acumular enormes cantidades de datos y recuperarlos con criterio complejos. De este modo, se incrementa de manera importante la posibilidad de localizar datos específicos.

Todo ello ofrece grandes ventajas para un aprovechamiento más amplio, eficiente y efectivo de la información. Sin embargo, si se utiliza con fines negativos, puede representar nuevos riesgos que no deben ser aceptados.

Por otra parte, la información se utiliza en muchos ámbitos diferentes, en los que se tienen condiciones, requisitos de control o confidencialidad y posibles implicaciones muy diversas. A manera de ejemplos, pueden destacarse:

- El ámbito estadístico. La Ley correspondiente prevé que no puedan divulgarse datos que puedan asociarse a un individuo u organización específica. Todos los datos deben darse a conocer en forma agregada, de modo que se preserve la confidencialidad de la información. Este es un ejemplo tradicional de preservación de la privacía.
- El ámbito policial. La información sobre los individuos involucrados en cuestiones criminales debería ser confidencial y accesible solo para los investigadores y funcionarios autorizados. Debe permitir al mismo tiempo hacer correlaciones con los datos de otros individuos que aparentemente no están involucrados con una investigación en proceso y otros accesos que en realidad abren la posibilidad de que se vean los datos de cualquier persona.

La información sobre salud. Los registros médicos generalmente se consideran confidenciales. Sin embargo, deben estar disponibles para cualquier persona del ámbito médico que tenga que ver con el tratamiento de un paciente.

- Los datos que acumulan las instituciones bancarias, financieras y de seguros son necesarios para su operación, pro deben ser confidenciales para evitar perjuicios a los usuarios de estos servicios, pero accesibles a los empleados que los requieren para su trabajo.
- Las empresas en general integran datos sobre personas. En muchas ocasiones estos datos son utilizados más allá del propósito para el que se le solicitan a las personas, llegando a ser empleados para fines comerciales (por ejemplo, para vender direcciones que son usadas luego para envíos de propaganda que puede resultar molesta).
- Los archivos de interés histórico y/o para estudios estadísticos, epidemiológicos o de otros ámbitos científicos, que requieren del manejo de datos en un contexto distinto del que tuvieron originalmente.

1.17 clientes

A continuación se analizará de forma simple la problemática asociada a la gestión de clientes en la empresa; este proceso afecta a todas las organizaciones, por lo que es comúnmente conocido.

La gestión de los clientes aporta a la empresa datos sobre personas físicas, que tienen que ser tratados de acuerdo a la legislación vigente (LOPD – RMS). Los datos del cliente si éste es persona física, o de contactos del cliente, representantes, etc., deben ser recogidos en ficheros, declarados ante la Agencia Española de Protección de Datos y deben serles aplicadas las medidas de seguridad correspondientes, dependiendo del tipo de datos.

De forma habitual, los datos de los clientes pueden llegar a la organización a través de mail, fax, correo, teléfono, y suelen ser recabados por iniciativa del cliente que solicita un servicio.

Es importante informar y solicitar el consentimiento del cliente (si éste es necesario) para llevar a cabo el tratamiento de los datos de carácter personal.

Asimismo, estos datos deben validarse antes de ser introducidos en el sistema de información, ya que el cliente puede existir ya en las bases de datos de la empresa, o puede haber cambiado parte de sus datos.
Una vez capturados los datos, el cliente pasa a formar parte del circuito comercial de la empresa, realizando pedidos a los que se asocian entregas de material y emisión de facturas.

La captura y mecanización de los datos del cliente en el sistema de información, que en la mayor parte de los casos está informatizado y cuyos datos están almacenados en un servidor central, se debe considerar como subproceso de la gestión de cliente. Esta es la casuística que será analizada por ser la más habitual. .

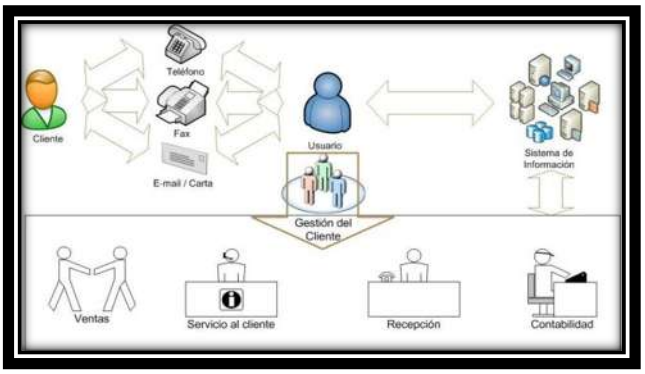


Fig.1 la gestión de los clientes

1.17.1 Análisis de la captura de datos de clientes

Una vez recibida la solicitud de alta del cliente, el personal encargado de su gestión debe realizar una consulta de la base de datos de clientes. Para ello accede a un ordenador, normalmente personal de administración, y utiliza la aplicación de gestión de la empresa que permite acceder a los datos de los clientes o crear nuevos clientes.

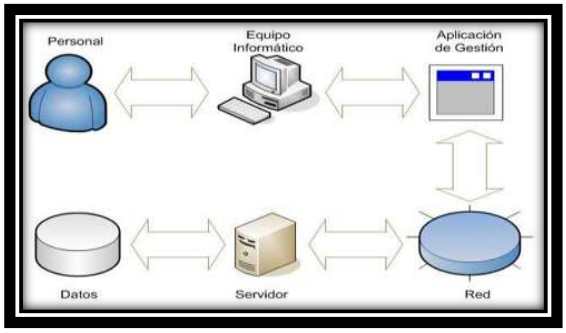


Fig. 2 consulta de la base de datos

Descomponiendo en pasos el proceso anterior, el personal encargado de la gestión de clientes accede a un equipo en el que se ejecuta una aplicación, y a través de las comunicaciones de red realiza la consulta al servidor que contiene los datos. Este análisis permite concluir que son necesarios seis elementos en el istema de información para llevar a cabo las altas y consultas sobre clientes de la empresa, elementos que pueden ser imprescindibles, en mayor o menor medida, en función de la capacidad de ser sustituidos en caso de indisponibilidad. Adicionalmente, se debe considerar que estos elementos dependen a su vez de otros de menor nivel, pero indispensables en el proceso, como son el suministro eléctrico, la red de área local, etc. Todos estos elementos son importantes por dar soporte al proceso general de consulta de clientes.

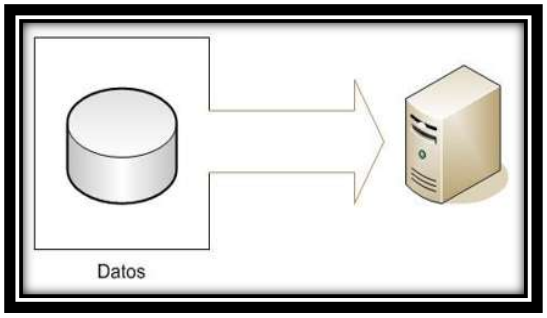


Fig.3 consulta al servidor

En esta imagen se muestra la relación de dependencia que los datos tienen de la disponibilidad del servidor. A su vez, los equipos informáticos dependen de la disponibilidad del suministro eléctrico, del funcionamiento de las comunicaciones y del local en el que están ubicados (cualquier incidente que dañe el local donde estén los equipos podría afectar seriamente la disponibilidad de los equipos en él almacenados). Analizando globalmente el proceso de gestión de un alta de clientes, éste puede quedar reflejado de forma gráfica en el siguiente árbol de dependencias (que muestra de una forma sencilla todos los activos y las relaciones existentes entre ellos).

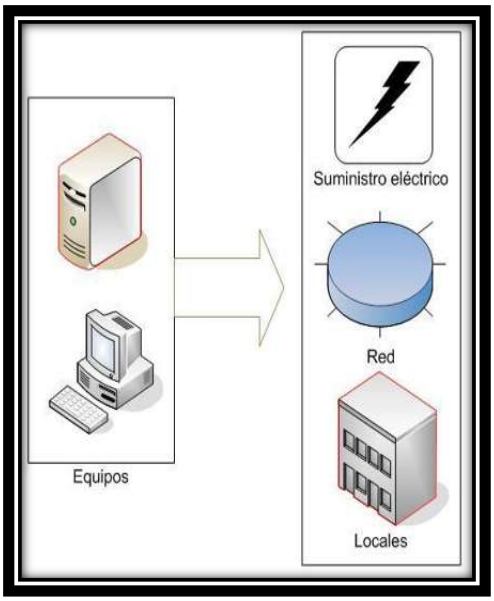


Fig. 4 relaciones de dependencia

Identificación de Activos (Árbol de dependencias) Se puede ver el árbol de dependencias como un castillo, donde el fallo de cualquier elemento de la base genera la caída parcial o total del edificio. Esta forma gráfica evidencia que los fallos en elementos de bajo nivel pueden ser arrastrados y producir paradas en los principales servicios de la empresa. Estas relaciones son las que producen los “efectos bola de nieve o avalancha”, donde un incidente, menor sobre un elemento poco importante, puede tener consecuencias graves en función de la importancia general que tenga el elemento afectado en la continuidad de los procesos de negocio a los que da soporte. Una vez identificados los procesos involucrados en la gestión de clientes, el siguiente paso es identificar las principales amenazas que pueden afectar a los activos de información. Las amenazas pueden tener un origen natural o humano, y pueden ser accidentales o deliberadas.

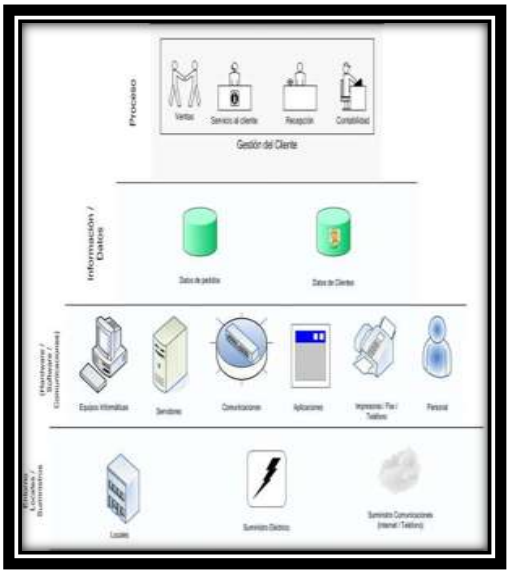


Fig.4 árbol de dependencia.

1.18 Métodos Usados Para Robar Información.

A continuación, se exponen dos de los principales métodos actuales para obtener información personal de usuarios. El primero de ellos, el phishing, hace referencia a la obtención de información confidencial en sitios web, y el segundo, los troyanos bancarios (bankers) refieren a la utilización de códigos maliciosos para el mismo fin.

El phishing es una modalidad de obtención de información llevada a cabo a través de Internet que intenta obtener, de manera completamente involuntaria y fraudulenta, datos personales o sensibles que posibiliten realizar una estafa, utilizando metodologías de Ingeniería Social.

Los primeros casos de phishing a entidades bancarias fueron reportados en Estados Unidos durante el 2003 y desde entonces, esta modalidad delictiva se ha ido diseminando a lo largo del planeta, constituyendo en la actualidad una de las principales amenazas para cualquier sitio que maneje información confidencial.
La mayoría de los casos de ataques de phishing se presentan ante los usuarios en forma de correo electrónico masivo (spam) invitándolo a ingresar a un sitio web similar al de la entidad financiera para solicitarle información confidencial (usuario, contraseña, PIN, número de tarjeta de crédito, etc). Los Códigos Maliciosos: A continuación, se exponen aquellos tipos de ataques de malware más representativos de la actualidad haciendo referencia a su línea evolutiva a largo del tiempo.

BackOriffice dieron origen al robo de información de forma remota. Dichas aplicaciones poseían componentes que permitían interceptar cualquier tipo de información y enviarla al atacante a través de la red. En ese momento, la información relacionada a tarjetas de crédito podía ser parte de los objetivos de las personas malintencionadas que utilizaban estas aplicaciones, para luego usar esos datos para adquirir distintos servicios y/o productos en forma fraudulenta, perjudicando directamente al dueño real de la tarjeta.

Keylogger Estas aplicaciones son troyanos y se caracterizan por poseer la capacidad de capturar y monitorear, de manera oculta, todo aquello que se escribe a través del teclado e incluso con el clic del mouse. Además, existen dispositivos físicos que se acoplan a modo de adaptadores al equipo y cuyas funcionalidades son similares a las de un keylogger de software. Un atacante busca instalar keyloggers en el sistema de la víctima y configurarlo para que le envíe toda la información que haya capturado y almacenado, incluyendo las contraseñas de acceso a diferentes servicios, como por ejemplo el Home Banking13.

Troyanos bancarios (bankers) La evolución de los códigos maliciosos fue dando origen a nuevas estrategias de engaño que permiten obtener información particular de las computadoras comprometidas a través de troyanos. Debido a sus características singulares, algunos de estos códigos maliciosos, reciben el nombre genérico de troyanos bancarios, ya que su objetivo general es obtener información bancaria de los usuarios.

Virus Programas informáticos o secuencias de comandos que intentan propagarse sin el consentimiento, conocimiento del usuario y que realizan alguna acción maliciosa. Entre sus principales características podemos identificar las siguientes: Se presentan como archivos ejecutables, o han

adherido su código malicioso a imágenes, hojas de cálculo o documentos. No pueden reproducirse por sí mismos, es decir para infectar otras computadoras es necesario que el usuario intervenga.

Troyano Programa de computadora que aparenta tener una función útil, pero que contiene código posiblemente malicioso para evadir mecanismos de seguridad, a veces explotando accesos legítimos en un sistema.

Gusanos Son programas que buscan propagarse lo más rápido posible tratando de infectar el mayor número posible de equipos, lo que en ocasiones tiene como consecuencia el colapso de las comunicaciones en la red.

Bot Programa o script que realiza funciones que de otra manera habría que hacer manualmente. También se refiere a una computadora que ha sido comprometida y que ejecuta las instrucciones que el intruso ordena.

Spyware También conocido como programa espía y comúnmente se refiere a aplicaciones que recopilan información sobre una persona u organización, las cuales se instalan y se ejecutan sin el conocimiento del usuario. Adware: Son programas que se instalan en el equipo con o sin intervención del usuario, su objetivo principal es descargar publicidad a la computadora infectada.

Dialers Programas que utilizan el modem14 para realizar llamadas a servicios telefónicos con alto costo. Punto seguridad, defensa digital Número 1, mayo 2009.

Control remoto Esta acción permite a un usuario malicioso tomar control de nuestro equipo, esto le permitiría utilizar nuestros recursos para almacenar más malware o para instalar programas o eliminar datos; aunque también podría utilizarse el equipo para llevar a cabo ataques a otros equipos de Internet.
Ataques de ingeniería social: Existe una nueva tendencia de fabricar malware que tiene por objetivo intimidar, espantar o molestar a los usuarios para que compren ciertos productos (Roberts, 2008). Por ejemplo, existe código malicioso que se hace pasar por un antivirus y alerta a los usuarios de que el equipo está supuestamente infectado y que la única manera de eliminar la infección es adquiriendo un software promocionado por el malware (Garnham, 2009).

1.19 Cibercriminales

1.19.1 Bot-herders: Se trata de criminales que infectan miles de computadoras con programas maliciosos que les permiten tomar el control de éstas y robar información o utilizarlas para realizar sus crímenes.
1.19.2 Carders: Se especializan en el robo de información personal de usuarios de tarjetas de crédito para realizar fraudes bancarios.
1.19.3 Cybergangs: Son grupos de hackers que utilizan las computadoras para realizar crímenes on-line. Estos grupos están establecidos

en países donde las leyes en cuanto a los delitos cibernéticos son ligeras o nulas. Cybermules: Son los miembros de los cybergangs.

1.19.4 Cyberpunk: Son delincuentes que utilizan sus computadoras para irrumpir en redes. El dinero no es su principal objetivo. Hackers y Crackers: Operan de manera individual y su principal objetivo es tener buena reputación entre su comunidad.

1.19.5 Phishers, pharmers, y spammers: Son delincuentes especializados en el robo de información para después venderla a redes criminales. Script kiddy: Se trata de una especie de hacker que no tiene a su disposición mayor tecnología, usualmente son adolescentes, aunque podrían hacer serios daños en algunas computadoras con comandos que obtienen on-line.

1.20 Acciones Ilícitas en la Red en los Últimos Años

1.20.1 Extorsión: Este tipo de ataque afectó tanto a empresas como a usuarios individuales. Los criminales roban la información personal, sobre todo la financiera y entonces pedían dinero a cambio de no utilizarla para cometer robos.

1.20.2 Fraude (phishing, pharming, spoofing, hijacking): Este tipo de ataques se daban a través de correos electrónicos disfrazados de alguna institución bancaria o de algún sitio de entretenimiento que pedía los datos de los usuarios y así robar información sensible. Lavado de dinero: Este tipo de actividad se dio de manera importante durante este año, es sencillo hacerlo a través de Internet. Los criminales utilizaban la banca por Internet, los casinos on-line, y servicios financieros en línea para realizar transacciones.

1.20.3 Spamming: En este tipo de ataques, los delincuentes utilizan los botnets para enviar miles de correos spam y robar información sensible. Robo de información: Los cibercriminales roban información financiera, ya sea de usuarios individuales o empresas. Además roban información de proyectos de empresas para venderlos después A pesar de que a nivel internacional se reforzaron leyes en contra del cibercrimen, señala el informe, la delincuencia cibernética sigue creciendo y los esfuerzos no resultan suficientes, pues los criminales van un paso adelante.

Capítulo 2 Marco referencial

2.1 Protección de datos en Europa

Las primeras formas de protección de la intimidad se encuentran en las prevenciones para evitar la inspección de personas y propiedades sin una autorización judicial. También existen normas penales dirigidas inicialmente a proteger la correspondencia. Estas normas fueron luego ampliadas a otras formas de comunicación.

Un ejemplo son los artículos 13 y 14 (registro personal), 15 (secreto de la correspondencia y de cualquier otra forma de comunicación) de la Constitución italiana de 1947. La Declaración Universal de los Derechos Humanos de 1948 ya recoge expresiones muy claras garantizando que: (artículo 12) “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”. Inmediatamente en Europa la Convención para la Protección de los Derechos Humanos y Libertades Fundamentales de 1950 incluye estos derechos en los artículos 8 y 10.

En Alemania la historia no es tan lineal, pues el pasado del país hace a los alemanes especialmente sensibles con respecto a la información que puede ser manejada por la policía. En la década de los cuarenta los nazis pudieron ejercer el control de la población con los datos del censo y los archivos del gobierno, que fueron utilizados para identificar a los judíos y a otros grupos víctimas de genocidios. Estos hechos motivaron que el derecho de privacidad fuera incluido en la Constitución alemana de la posguerra y que luego las raíces de la teoría europea de protección de datos esté relacionada directamente con estas experiencias horrorosas ocurridas durante la Segunda Guerra Mundial.24 Aun así en 1970, la policía alemana fue pionera en el uso de perfiles computados para capturar a los miembros de la organización terrorista Rote Armee Fraktion. Pero esa forma de investigación generó muchas protestas y fue uno de los argumentos que llevó a Alemania a sancionar probablemente una de las leyes más duras del mundo en materia de protección de datos.

La estrategia para forzar Leyes de Protección más fuertes fue mantenida en la Directiva como la cláusula “de terceros países”. Ajustándose a la Directiva, los Estados miembros deben asegurar que los datos serán “tratados de manera leal y lícita” y sólo recogidos “con fines determinados, explícitos y legítimos”. Los datos deberán ser “adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben” y “exactos”. Serán “conservados... durante un periodo no superior al necesario para los fines para los que fueron recogidos”. La Directiva también contiene protecciones tales como el “derecho de acceso del interesado a los datos”, derecho de oposición al tratamiento y a recurrir judicialmente en caso de violación de esos derechos (responsabilidad y sanciones). Merecen destacarse el concepto de “finalidad” que luego fue recogido por otras legislaciones no europeas, pues es el eje interpretativo de un tratamiento leal y lícito, y la prohibición del tratamiento de datos sensibles,

i.e. aquellos que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como los datos relativos a la salud o a la sexualidad.

El concepto de autodeterminación informativa aparece formalmente en Europa en la sentencia del Tribunal Constitucional alemán del 15 de diciembre de 1983 en relación con la Ley del Censo prohibiendo explícita- mente al gobierno generar "un inventario de datos personales de los individuos por medio de censos gubernamentales de carácter confidencial". Luego de esta decisión el derecho a la privacidad incluye el derecho a controlar la información sobre sí mismo y la capacidad para determinar si esa información puede ser recogida y cómo puede ser usada. La tendencia actual supone el principio de uso mínimo de los datos personales y, consistentes con la finalidad, con preferencia por la anonimización en la recolección y transferencia, cuando sea posible.

2.2 Protección de datos en América latina

En América Latina la protección de datos fue vista como una necesidad resultado de la explosión tecnológica, pero inevitablemente todos los procesos legislativos en la región han sufrido los avatares de una fuerte carga histórica y de la presión de los intereses económicos en la generación de bases de datos.

Las recientes reformas constitucionales en América Latina introdujeron la protección de los datos personales (algunas bajo la forma de habeas data), viz.

- Brasil (1988) artículo 5o.- X, XII y LXXII; artículo 105 I
- Colombia (1991) artículo 15;
- Paraguay (1992) artículos 33, 36 y 135;
- Perú (1993) artículos 2o., 162, 203-3;
- Argentina (1994) artículos 19 y 43; y,
- Ecuador (1998) artículos 23.8, 23.13, 23.24, 94.

Dos textos constitucionales recientes han percibido los riesgos de la informática. Son el caso de la Constitución Política del Perú: "artículo 2o. Derechos fundamentales de la persona. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar"; y de la Constitución de la República Bolivariana de Venezuela: "artículo 60. Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos".

Algunos ejemplos de casos decididos por los más altos tribunales latinoamericanos son:

- En Argentina: Dirección General Impositiva vs. Colegio Público de Abogados de la Capital Federal, 1996 (información personal que figura en los registros, archivos y bancos de datos computarizados).
- Ponzetti de Balbín, Indalia vs. Editorial Atlántida, S.A., 1984 (derecho a la intimidad, personas voluntariamente públicas).

- Granada, Jorge Horacio vs. Diarios y Noticias S.A., 1993 (responsabilidad por datos erróneos).
- Urteaga vs. Es- tado Nacional, 1998 (acceso a la información).
- Ganora vs. Estado Nacional, 1999 (habeas data puede ser usado para todas las bases de datos gubernamentales).
- Lascano Quintana vs. Veraz S.A., 2001 (informacióncrediticia).
- En Chile: Bohme Bascuñán, Manuel vs. Clínica Alemana, 1992 (filmaciones no autorizadas) y CODEPU vs. Gendarmería de Chile, 1995 (micrófonos en cárceles).
- En Costa Rica: C. A., E. vs. Aludel Ltda., 2000 (información crediticia) y M. M., C. vs. Aludel Ltda., 2002 (exactitud de la información).
- En Panamá: Guillermo Cochez vs. ministro de Relaciones Exteriores, 2002 (la planilla de una institución gubernamental no es de carácter reservado) y Aluminio Estructural y otros vs. director general de Ingresos, 2002 (la información acopiada en ejercicio de la función fiscalizadora es de acceso restringido).
- En Venezuela: N. A. y otros, 1998 (datos sensibles, infección VIH), R. C. M. y otros vs. Consejo Nacional Electoral, 2000 (acceso a los padrones electorales) y G. B., X. vs. Juzgado de Protección del Niño y del Adolescente del Estado Lara, 2002 (redacción de sentencias judiciales).

Varios países han sancionado Leyes de Transparencia y Acceso a la Información Gubernamental: Colombia (1985), Perú (2002), Panamá (2002) y México (2002).

2.3 Alemania

En Alemania, para hacer frente a la delincuencia relacionada con la informática, el 15 de mayo de 1986 se adoptó la Segunda Ley contra la Criminalidad Económica. Esta ley reforma el Código Penal (art. 148 del 22 de diciembre de 1987) para contemplar los siguientes delitos:

• Espionaje de datos (202a).

• Estafa informática (263a).

• Falsificación de datos probatorios (269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271, 273).

• Alteración de datos (303a) es ilícito cancelar, inutilizar o alterar datos e inclusive la tentativa es punible.

• Sabotaje informático (303b).

• Destrucción de datos de especial significado por medio de deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.

• Utilización abusiva de cheques o tarjetas de crédito (266b).

• Por lo que se refiere a la estafa informática, el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos o a través de una intervención ilícita. Esta solución fue también adoptada en los Países Escandinavos y en Austria.

2.4 Austria

Según la Ley de reforma del Código Penal del 22 de diciembre de 1987, se contemplan los siguientes delitos:

• Destrucción de datos (art. 126) no solo datos personales sino también los no personales y los programas.

• Estafa informática (art. 148) se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

2.5 Chile

Chile fue el primer país latinoamericano en sancionar una Ley contra Delitos Informáticos.

La ley 19223 publicada en el Diario Oficial (equivalente del Boletín Oficial argentino) el 7 de junio de 1993 señala que la destrucción o inutilización de un sistema de tratamiento de información puede ser castigado con prisión de un año y medio a cinco. Como no se estipula la condición de acceder a ese sistema, puede encuadrarse a los autores de virus. Si esa acción afectara los datos contenidos en el sistema, la prisión se establecería entre los tres y los cinco años.

El hacking, definido como el ingreso en un sistema o su interferencia con el ánimo de apoderarse, usar o conocer de manera indebida la información contenida en éste, también es pasible de condenas de hasta cinco años de cárcel; pero ingresar en ese mismo sistema sin permiso y sin intenciones de ver su contenido no constituye delito. Dar a conocer la información almacenada en un sistema puede ser castigado con prisión de hasta tres años, pero si el que lo hace es el responsable de dicho sistema puede aumentar a cinco años. Esta ley es muy similar a la inglesa aunque agrega la protección a la información privada.

2.6 China

El Tribunal Supremo Chino castigará con la pena de muerte el espionaje desde Internet, según se anunció el 23 de enero de 2001. Todas las personas "implicadas en actividades de espionaje", es decir que "roben, descubran, compren o divulguen secretos de Estado" desde la red podrán ser condenadas con penas que van de diez años de prisión hasta la muerte. ¿Castigo ejemplar?.

La corte determina que hay tres tipos de actividades donde la vigilancia será extrema: secretos de alta seguridad, los secretos estatales y aquella información que dañe seriamente la seguridad estatal y sus intereses. Se consideran actividades ilegales la infiltración de documentos relacionados con el Estado, la defensa, las tecnologías de punta, o la difusión de virus informático. El Tribunal ha hecho especial énfasis al apartado del espionaje desde la red. A los llamados "criminales", además de tener asegurada una severa condena (la muerte), también se les puede... ¡confiscar los bienes!.

2.7 España

Este país quizás sea el que mayor experiencia ha obtenido en casos de delitos informáticos, en Europa. Su actual Ley Orgánica de Protección de Datos de Carácter Personal (LOPDCP) aprobada el 15 de diciembre de 1999, la cual reemplaza una veintena de leyes anteriores de la misma índole, contempla la mayor cantidad de acciones lesivas sobre la información.

Se sanciona en forma detallada la obtención o violación de secretos, el espionaje, la divulgación de datos privados, las estafas electrónicas, el hacking maligno o militar, el phreacking, la introducción de virus, etc.; aplicando pena de prisión y multa, agravándolas cuando existe una intención dolosa o cuando el hecho es cometido por parte de funcionarios públicos. Así mismo su nuevo Código Penal establece castigos de prisión y multas "a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos".

2.8 Estados unidos de América

El primer abuso de una computadora se registró en 1958 mientras que recién en 1966 se llevó adelante el primer proceso por la alteración de datos de un banco de Mineapolis. En la primera mitad de la década del 70, mientras los especialistas y criminólogos discutían si el delito informático era el resultado de una nueva tecnología o un tema específico, los ataques computacionales se hicieron más frecuentes. Para acelerar las comunicaciones, enlazar compañías, centros de investigación y transferir datos, las redes debían (y

deben) ser accesibles, por eso el Pentágono, la OTAN, las universidades, la NASA, los laboratorios industriales y militares se convirtieron en el blanco de los intrusos. Pero en 1976 dos hechos marcaron un punto de inflexión en el tratamiento policial de los casos: el FBI dictó un curso de entrenamiento para sus agentes acerca de delitos informáticos y el Comité de Asuntos del Gobierno de la Cámara presentó dos informes que dieron lugar a la Ley Federal de Protección de Sistemas de 1985 Esta ley fue la base para que Florida, Michigan, Colorado, Rhode Island y Arizona se constituyeran en los primeros estados con legislación específica, anticipándose un año al dictado de la Computer Fraud y Abuse Act de 1986. Este se refiere en su mayor parte a delitos de abuso o fraude contra casas financieras, registros médicos, computadoras de instituciones financieras o involucradas en delitos interestatales.

También especifica penas para el tráfico de claves con intención de cometer fraude y declara ilegal el uso de passwords ajenas o propias en forma inadecuada. Pero sólo es aplicable en casos en los que se verifiquen daños cuyo valor supere el mínimo de mil dólares.

En 1994 se adoptó el Acta Federal de Abuso Computacional (18 U.S.C. Sec 1030), modificando el Acta de 1986. Aquí se contempla la regulación de los virus (computer contaminant) conceptualizándolos aunque no los limita a los comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos. Modificar, destruir, copiar, transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas es considerado delito. Así, esta ley es un acercamiento real al problema, alejado de argumentos técnicos para dar cabida a una nueva era de ataques tecnológicos. El aumento en la cantidad de casos de hacking y la sensación de inseguridad permanente que generaron (fomentada por la difusión de los hechos en programas especiales de televisión y artículos de revistas especializadas), cambiaron la percepción de las 15 º autoridades con respecto a los hackers y sus ataques. Los casos que demostraron ese cambio fueron los del “Cóndor” Kevin Mitnicky y los de “ShadowHawk” Herbert Zinn hijo (ver Anexo II). El FCIC (Federal Computers Investigation Commitee), es la organización más importante e influyente en lo referente a delitos computacionales: los investigadores estatales y locales, los agentes federales, abogados, auditores financieros, programadores de seguridad y policías de la calle trabajan allí comunitariamente.

El FCIC es la entrenadora del resto de las fuerzas policiales en cuanto a delitos informáticos, y el primer organismo establecido en el nivel nacional. Además existe la Asociación Internacional de Especialistas en Investigación Computacional (IACIS), quien investiga nuevas técnicas para dividir un sistema en sus partes sin destruir las evidencias. Sus integrantes son “forenses de las computadoras” y trabajan, además de los Estados Unidos, en el Canadá, Taiwán e Irlanda.

2.9 Francia

Aquí, la Ley 88/19 del 5 de enero de 1988 sobre el fraude informático contempla:

• Acceso fraudulento a un sistema de elaboración de datos. Se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

• Sabotaje Informático. Falsear el funcionamiento de un sistema de tratamiento automático de datos.

• Destrucción de datos. Se sanciona a quien intencionalmente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos, suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión. • Falsificación de documentos informatizados. Se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

2.10 Holanda

Hasta el día 1 de marzo de 1993, día en que entró en vigencia la Ley de Delitos Informáticos, Holanda era un paraíso para los hackers. Esta ley contempla con artículos específicos sobre técnicas de Hacking y Phreacking. El mero hecho de entrar en una computadora en la cual no se tiene acceso legal ya es delito y puede ser castigado hasta con seis meses de cárcel. Si se usó esa computadora hackeada para acceder a otra, la pena sube a cuatro años aunque el crimen, a simple vista, no parece ser peor que el anterior. Copiar archivos de la máquina hackeada o procesar datos en ella también conlleva un castigo de cuatro años en la cárcel. Publicar la información obtenida es ilegal si son datos que debían permanecer en secreto, pero si son de interés público es legal.

El daño a la información o a un sistema de comunicaciones puede ser castigado con cárcel de seis meses a quince años, aunque el máximo está reservado para quienes causaron la muerte de alguien con su accionar. Cambiar, agregar o borrar datos puede ser penalizado hasta con dos años de prisión pero, si se hizo vía remota aumenta a cuatro. Los virus están considerados de manera especial en la ley. Si se distribuyen con la intención de causar problemas, el castigo puede llegar hasta los cuatro años de cárcel; si simplemente se “escapó”, la pena no superará el mes. El usar el servicio telefónico mediante un truco técnico (Phreacking) o pasando señales falsas con el objetivo de no pagarlo puede recibir hasta tres años de prisión. La venta de elementos que permitan el Phreaking se castiga con un año de prisión como tope y si ese comercio es el modo de ganarse la vida del infractor, el máximo

aumenta a tres. La ingeniería social también es castigada con hasta tres años de cárcel. Recibir datos del aire es legal (transmisiones satelitales), siempre y cuando no haga falta un esfuerzo especial para conseguirlos; la declaración protege datos encriptados, como los de ciertos canales de televisión satelital. Falsificar tarjetas de crédito de banca electrónica y usarlas para obtener beneficios o como si fueran las originales está penado con hasta seis años. Aunque... hacerlas y no usarlas parece ser legal.

2.11 Inglaterra

Luego de varios casos de hacking surgieron nuevas leyes sobre delitos informáticos. En agosto de 1990 comenzó a regir la Computer Misuse Act (Ley de Abusos Informáticos) por la cual cualquier intento, exitoso o no de alterar datos informáticos con intención criminal se castiga con hasta cinco años de cárcel o multas sin límite.

El acceso ilegal a una computadora contempla hasta seis meses de prisión o multa de hasta dos mil libras esterlinas. El acta se puede considerar dividida en tres partes:

hackear (ingresar sin permiso en una computadora), hacer algo con la computadora hackeada y realizar alguna modificación no autorizada.

El último apartado se refiere tanto al hacking (por ejemplo, la modificación de un programa para instalar un backdoor), la infección con virus o, yendo al extremo, a la destrucción de datos como la inhabilitación del funcionamiento de la computadora. Bajo esta ley liberar un virus es delito y en enero de 1993 hubo un raid contra el grupo de creadores de virus. Se produjeron varios arrestos en la que fue considerada la primera prueba de la nueva ley en un entorno real.

2.12 México

De acuerdo con el dictamen aprobado queda tipificado como delito de revelación de secretos, “a quien revele divulgue o utilice indebidamente o en perjuicio de otro, información, conversaciones o mensajes de texto, imágenes o archivos de voz, contenidos en sistemas o equipos informáticos” (Artículo 211 Bis).

Al artículo 211 se le agrega un capítulo entero dedicado a definir y sancionar el acceso ilícito a sistemas y equipos de informática (también llamado *cracking*), por el que se establece una pena de entre tres meses y un año de prisión a quien “sin autorización acceda, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática”. La pena se incrementa en dos terceras partes, en caso de que la penetración impida el uso o acceso del sistema afectado.

El *hackeo* (o penetración sin daño a un sistema informático) también está contemplado en el mismo artículo 211 para el que aplica “un año de prisión y de cien a ciento cincuenta días de multa al que sin autorización conozca o copie información contenida en sistemas o equipos de informática no protegidos por algún mecanismo de seguridad”.

Las modificaciones legales establecen también sanciones de hasta tres años de prisión por amenazas e intimidación a través de sistemas digitales (conocido como *cyberbullying*) y el uso de imágenes de otros como forma de chantaje: “al que amenace a otro (...), haciendo uso o empleo de comunicados o mensajes enviados a través de medios o sistemas informáticos o le amenace con divulgar la información, datos o imágenes obtenidos a través del acceso ilícito a dichos medios o sistemas informáticos” (artículo 282 del Código Penal Federal).
Por primera vez se tipifica el acto de contactar víctimas por internet, como ha ocurrido en varias ocasiones: “el empleo de medios informáticos para generar relación de confianza o amistad con la víctima”, según establece la modificación al artículo 205 del Código Penal.
“Hemos tenido buena suerte con esta iniciativa, pues la planteamos en noviembre del año pasado y su dictaminación ha sido rápida, ya que todas las fracciones comprenden que esta ley tendrá efectos positivos para darle identidad a delitos (para) tener una herramienta para juzgar a quienes usan la tecnología para delinquir”, dijo el diputado Pérez-Alonso.
De hecho, la iniciativa se aprobó con 271 votos a favor y nueve en contra. Ahora será enviada a la Cámara de Senadores, donde será revisada.
Todos los delitos informáticos se verían agravados si su propósito es realizar operaciones con recursos de procedencia ilícita, lo que se conoce como lavado de dinero, según lo que establece el apartado 211 Bis 5.

Capítulo 3 Marco metodológico

3.1 El Proceso Legislativo

El proceso legislativo federal se rige por la Constitución Política de los Estados Unidos Mexicanos, la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos y el Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos.

El proceso de elaboración de las leyes federales es el conjunto de etapas sistematizadas y ordenadas por la ley fundamental mexicana, que deberán ser observadas por los Poderes Legislativos y Ejecutivo para incorporar al sistema jurídico aquellas normas jurídicas de aplicación general y obligatoria conocida como leyes.

Este proceso formaliza y distingue al dotar de juridicidad, aquellas normas que oficialmente se conocerán y reconocerán como leyes del sistema de Derecho en México. El proceso de estas normas se constituye por otras cuyo objetivo es la producción jurídica, a estas se identifican como normas sobre la producción jurídica.

Las normas sobre la producción jurídica están reflejadas en los artículos 71 y 72 constitucionales. Este proceso consta de seis etapas. Para que una ley sea considerada como tal se requiere el cumplimiento de formalidades exigidas en un proceso legislativo.

Las formalidades generales también llamadas etapas son:

1. Iniciativa,
2. Discusión,
3. Aprobación,
4. Sanción,
5. Publicación
6. Iniciación de la vigencia.

A contrario sensu, que si el proceso legislativo no se cumple en las etapas generales o en las formalidades particulares el producto obtenido no tiene carácter de ley.

3.1.1 Iniciativa

Constitución Federal:

Artículo 71. *El derecho de iniciar leyes o decretos le compete:*

El Presidente de la República, los Diputados y Senadores al Congreso de la Unión y las Legislaturas de los Estados ejercen su facultad de poner a consideración del Congreso un proyecto de ley.

Cuando el proyecto provenga del ejecutivo o alguna legislatura se turna a una comisión de la cámara respectiva, donde el proyecto adquirirá la forma definitiva en que se presentara para ser debatido.

Comisión o comisiones:

Desarrollan las siguientes actividades:

- Reunión de Trabajo para distribuir la iniciativa entre sus miembros y explicarla.

- Elaboración del programa de Trabajo.
- Recopilación de información especializada respecto a la iniciativa.
- Análisis de la información y antecedentes legales de la materia.
- Celebración de reuniones de Trabajo con representantes de órganos de gobierno y entidades públicas vinculados con la iniciativa.
- Reuniones de Trabajo con especialistas y representantes de los grupos sociales interesados en la misma.
- Celebración de Conferencias con comisiones homologas de otra cámara.
- Integración de la Subcomisión de Redacción.
- Formulación del proyecto de Dictamen.
- Presentación y Exposición del dictamen a los miembros de la comisión explicando y justificando adecuaciones y modificaciones incorporadas.
- Análisis y discusión colegiada de la propuesta de dictamen en la Comisión o Comisiones conjuntas.
- Aprobación y firma del dictamen por la mayoría de los miembros de la comisión y presentación, en su caso, de voto o votos particulares por escrito de quienes disientan del parecer de la mayoría.

Dichas comisiones son grupos de trabajos creados sobre las materias en labor legislativa.

La Cámara ante la cual se inicia un proyecto de ley recibe el nombre de Cámara de origen, la que le sigue recibirá el de cámara Revisora. La Cámara de origen puede ser cualquiera, la de Diputados o Senadores, salvo que el proyecto respectivo se refiera a empréstitos, contribuciones, impuestos o reclutamiento de tropas. En estos casos la cámara de origen será siempre la de Diputados.

3.1.2 Discusión

La discusión del Proceso Legislativo donde los diputados y senadores realizan un ejercicio deliberativo sobre las distintas iniciativas de ley. La discusión se realiza con base a un debate parlamentario. En este los diputados o senadores hacen uso de la tribuna para exponer sus argumentos en pro o en contra de un proyecto de ley

Según el primer párrafo del Artículo 72. *Todo proyecto de ley o decreto, cuya resolución no sea exclusiva de laguna de las Cámaras, se discutirá sucesivamente en ambas, observándose el reglamento de Debates sobre la forma, intervalos y modo de proceder en las discusiones y votaciones.*

3.1.3 Aprobación

Artículo 72. *A) aprobado un proyecto en la cámara de su origen, pasara para su discusión a la otra. Si esta lo aprobare, se remitirá al Ejecutivo, quien si no tuviere observaciones que hacer, lo publicara inmediatamente.*

Una vez que ha sido discutido le sigue la Aprobación. Esta etapa del proceso tiene por objeto la aceptación total o parcial del antedicho proyecto de ley. La aprobación deberá hacerse en la Cámara de origen y luego en la Revisora.

Aprobado por ambas Cámaras, el proyecto se remite al Ejecutivo para que lo sancione y publique.

3.1.4 Sanción

Constitución del Estado de MICHOACAN:

Artículo 71. *Aprobada la ley o decreto se enviara al Gobernador para su publicación. Si éste lo devolviere con observaciones, dentro de diez días volverá a ser examinado... transcurrido aquel termino sin que el Ejecutivo haga observaciones se tendrá por sancionada la ley o decreto.*

La sanción etapa en la que el Presidente de la República acepta o desecha un proyecto de ley. Según la constitución se reputa como sancionado aquel proyecto que no sea devuelto con observaciones a la Cámara de origen dentro de los siguientes diez días útiles, corriendo este termino hubiere el Congreso cerrado o suspendido sus sesiones, en cuyo caso la devolución deberá hacerse el primer día útil en que el Congreso este reunido.

La sanción puede ser total o parcial. El ejecutivo solo podrá rechazar un proyecto de ley en una ocasión. Si las Cámaras insisten el Ejecutivo deberá ordenar su publicación. Esta facultad que posee el Ejecutivo se le llama derecho de veto.

3.1.5 Promulgación, publicación.

Promulgación: acto por el cual el Ejecutivo aprueba con su firma y autoridad que se han cumplido las formalidades anteriores, y ordena su publicación.

Publicación: medio idóneo para el conocimiento de la ley a quienes deban cumplirla.

Medio idóneo en la federación: Diario Oficial de la Federación

Medio idóneo Estatal: Periódico Oficial

La publicación acto formal por medio del cual las leyes aprobadas por el Poder Legislativo y sancionadas por el Ejecutivo son dadas a conocer por este, y de manera indubitable, a la población en general. Para que esta publicación surta sus efectos legales deberá plasmarse en un periódico que el Estado posee llamado Diario Oficial de la Federación. La publicación oficial que de la ley lleva a cabo el poder ejecutivo con las formalidades antes citadas recibe el nombre de promulgación. Esta implica la exigencia de su acatamiento y observancia por parte de los particulares y la autoridad.

La promulgación es la condición para que la ley sea aplicada y pueda hacerse efectivo el principio que señala: La ignorancia de las leyes no excluye a nadie de su cumplimiento.

3.1.6 Iniciación de Vigencia

La última etapa del proceso legislativo se denomina Iniciación de la vigencia. Es la determinación del momento específico en que una ley comenzara a surtir sus efectos. Entre la publicación y la entrada en vigor de toda ley debe mediar un espacio de tiempo, a efecto de que esta será efectivamente conocida por sus destinatarios. A este lapso se le conoce como Vocatio Legis. Existen dos sistemas para que la ley inicie su vigencia el sucesivo y el sincrónico. El sucesivo ordena que la ley entrara en vigor, para los lugares donde se publica el diario oficial, tres días después de su promulgación. En los lugares distintos se conceden otros días en función de la distancia. A los tres primeros días uno más por cada cuarenta kilómetros o fracción que exceda de la mitad.

El sistema sincrónico establece que la ley entrara en vigor, en todas partes, el día preciso que la propia ley fije, siempre y cuando su publicación haya sido anterior.

La jerarquía de las leyes en el sistema jurídico mexicano.

El sistema de derecho mexicano es escrito y que la estructura política del país gira en torno a una Federación, constituida por entidades libres y soberanas.

Existen dos niveles muy claros de legislación, la federal y la local o estatal; la ley de mayor jerarquía es la Constitución Federal, a la cual no podrá contravenir las constituciones de los Estados ni ley alguna.

Capítulo 4 Caso práctico

4.1 El IFAI exige cuentas a Sony por robo de datos a usuarios de PlayStation

PRESIDENCIA
Oficio IFAI/JPM/041-2011

México, D.F. a 03 de mayo de 2011.

"2011, Año del Turismo en México"

Instituto Federal de Acceso a la Información y Protección de Datos

Sr. Hajime Murano
Presidente y Director General de Sony de México, S.A. de C.V.
Av. Santa Fe No. 50, Lomas de Santa Fe,
Álvaro Obregón, México, D.F.
C.P. 01210
PRESENTE

A partir de información obtenida en los medios de comunicación[1], este Instituto Federal de Acceso a la Información y Protección de Datos –en adelante, Instituto- ha tenido conocimiento de que, con fecha 26 de abril de 2011, las empresas *Sony Computer Entertainment* y *Sony Network Entertainment* –en adelante, Sony- advirtieron que ciertos datos personales de 75 millones de usuarios de sus servicios de la Red *PlayStation Network* (PSN) y Qriocity, podrían haber sido sustraídos indebidamente del 17 al 19 de abril de

El Instituto Federal de Acceso a la Información y Protección de Datos se estrenó con Sony por el 'hackeo' a la base de datos de PlayStation

(CNNMéxico) — La irrupción y robo de datos en la red PlayStation Network será el primer caso donde el Instituto Federal de Acceso a la Información (IFAI) pondrá a prueba las atribuciones otorgadas por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares**.**

Esta ley (publicada en el Diario Oficial de la Federación en junio de 2010) determina en su artículo 39 que el IFAI será encargado de proteger la información que empresas tengan de ciudadanos mexicanos.

De hecho, aunque la ley podía ser ejercida luego de su publicación, fue casi un año más tarde cuando el instituto asumió plenamente sus facultades, frente a Sony de México.

En la carta enviada el pasado 3 de mayo por **la** comisionada presidenta del IFAI, Jacqueline Peschard al director general de Sony de México, Hajime Murano (de la cual CNNMexico.com posee una copia), el IFAI pide respuestas a una lista de nueve cuestionamientos, entre las que se encuentra la forma en la que Sony de México trata la información de los usuarios mexicanos de PlayStation Network, así como las medidas de protección y compensación que presentará a los usuarios afectados.

Un portavoz de Sony comentó a CNNExpansión que el presidente y director general de Sony México es Hiroshi Takahashi y no Murano.

La carta enviada a Sony de México no indica tiempo límite para recibir respuesta, pero el artículo 32 de la Ley establece un plazo de alrededor de 20

días más una prórroga adicional de otros 20 para que el IFAI reciba una respuesta de la empresa. Y si Sony de México no quisiera responder o no ofreciera la protección que la ley señala, puede ser multada con hasta 320 mil días de salario mínimo, es decir, 19.1 millones de pesos**.**
Además de la petición realizada por el IFAI, **los** usuarios pueden solicitar de manera individual la ayuda del Instituto para solicitar la protección de su **información**, tanto a través de una sección informativa de su sitio web, del número telefónico 01 800 835 4324 y de la cuenta de Twitter @ifaimexico para recibir peticiones de los ciudadanos.
Mientras tanto, Sony informó en un comunicado que, "actualmente estamos analizando las mejores soluciones para nuestros clientes de Latinoamérica y, una vez que el programa esté listo para ser anunciado, brindaremos los detalles de los servicios específicos disponibles en cada país y explicaremos cómo adherirse al programa"

En seguida clasificaremos los 31 estados y el distrito federal , cómo están protegidos y el tipo de ente en que se rige la ley sobre la protección de datos personales.

Explicare cada punto.

1. Estado.
   Nombre del estado a analizar.
2. Regula la protección de datos personales.
   Tipo de ente que es regulada la protección de datos personales.
3. Órgano encargado de la protección de datos personales.
   Tipo de departamento con que cuenta este estado para el control de la protección de datos personales.
4. Ordenamiento legal que regula la protección de datos personales.
   Nombre de la ley con cuenta este estado para regir la protección de datos personales.
5. Procedimiento o mecanismos que han implementado para cumplir con esta función.
   Tareas que se han implementado para la realización de esta ley sobre la protección de datos personales.

4.2 Estados que cuentan con Legislación en Materia de Protección de Datos Personales en entes Públicos/Privados y Órgano encargado de su protección

No.	Estado	Regula la protección de Datos Personales		Órgano encargado de la protección de Datos Personales		Ordenamiento Legal que regula la protección de Datos Personales		Procedimiento o Mecanismos que han implementado para cumplir con estas funciones	
		En Entes Públicos	En Entes Privados	En Entes Públicos	En Entes Privados	En Entes Públicos	En Entes Privados	En Entes Públicos	En entes Privados
1	Aguascalientes	Si	No	Instituto de Transparencia del Estado de Aguascalientes	no	Ley de ransparencia e Información Pública del Estado de guascalientes	no	No	no
2	Baja California	Si	No	Sujetos Obligados	no	Ley de Acceso a la Información Pública para el Estado de Baja	no	No	no
3	Baja California Sur	Si	no	Instituto de Transparencia y Acceso a la Información Pública del Estado de Baja California Sur	no	Ley de Transparencia y Acceso a la Información Pública para el estado de Baja California Sur	no	1.- Lineamientos generales para la clasificación y desclasificación de la información reservada y confidencial en poder de las entidades gubernamentales y las de interés público a que se refiere la Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California Sur 2.- Lineamientos y políticas generales para el manejo, mantenimiento, seguridad y protección de los datos personales que estén en posesión de las entidades gubernamentales y las de interés público del Estado de	no
4	Campeche	Si	no	Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche	no	Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche	no	1.- Lineamientos que deberán observar los Entes Públicos a que se refiere la fracción IV, del artículo 4, de la Ley, para notificar a la Comisión el Listado de sus sistemas de datos personales; 2.-Lineamientos que deberán observar los Entes Públicos a que se refiere la fracción IV del artículo 4 de Ley, en la recepción, procesamiento, resolución y notificación de las solicitudes de acceso a datos personales que formulen los particulares;	no

No.	Estado	Regula la protección de Datos Personales		Órgano encargado de la protección de Datos Personales		Ordenamiento Legal que regula la protección de Datos Personales		Procedimiento o Mecanismos que han implementado para cumplir con estas funciones	
		En Entes Públicos	En Entes Privados	En Entes Públicos	En Entes Privados	En Entes Públicos	En Entes Privados	En Entes Públicos	En entes Privados
5	Coahuila	Si	No	Instituto Coahuilense de Acceso a la Información Pública	no	Ley de Acceso a la Información Pública y Protección de Datos Personales para el Estado de	no	No	no
6	Colima	Si	Si	Comisión Estatal para el Acceso a la Información Pública de Colima	Comisión Estatal para el Acceso a la Información Pública de Colima	Ley de Protección de Datos Personales del Estado de Colima	Ley de Protección de Datos Personales del Estado de Colima	No	no
7	Chiapas	Si	No	Instituto de Acceso a la Información Pública de la Administración Pública Estatal de Chiapas	no	Ley que Garantiza la Transparencia y el Derecho a la Información Pública para el Estado de Chiapas	no	1.- Lineamientos Generales y Recomendaciones para la Protección de Datos Personales.	no
8	Chihuahua	Si	No	Instituto Chihuahuense para la Transparencia y Acceso a la Información Pública	no	Ley de Transparencia y Acceso a la Información Pública del Estado de Chihuahua	no	1.- Reglamento de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chihuahua; 2.- Lineamientos que regulan la práctica de visitas de inspección periódicas a las unidades de información de los sujetos obligados de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chihuahua. (Según información del Jurídico de Chihuahua, existe un proyecto de Ley de Protección de Datos Personales y Archivos en el Congreso del Estado).	no

No.	Estado	Regula la protección de Datos personales		Órgano encargado de la protección de Dato Personales		Ordenamiento Legal que regula la protección de Datos Personales		Procedimiento o Mecanismos que han implementado para cumplir con estas funciones	
		En Entes Públicos	En Entes Privados	En Entes Públicos	En Entes Privados	En Entes Públicos	En Entes Privados	En Entes Públicos	En entes Privados
9	Durango	Si	no	Instituto Coahuilense de Acceso a la Información Pública	no	Ley de Acceso a la Información Pública del Estado de Durango	no	No	no
10	Distrito Federal	Si	no	Instituto de Acceso a la Información Pública del Distrito Federal	no	Ley de Protección de Datos Personales para el Distrito Federal	no	1.- Reglamento de la Ley de Transparencia y Acceso a la Información Pública del D.F.; 2.- Lineamientos para la protección de datos personales en el D.F.; 3.- Lineamientos para la gestión de solicitudes de información pública y de datos personales a través del Sistema Infomex del D.F.; 4.- Registro Electrónico de Sistemas de Datos Personales.	no
11	Guanajuato	Si	no	Instituto de Acceso a la Información Pública del Estado de Guanajuato	no	Ley de Protección de Datos Personales para el Estado y los Municipios de Guanajuato	no	1.- Lineamientos de la Ley de Protección de datos personales para el Estado y Municipios de Guanajuato. 2.- Asimismo cada sujeto obligado tiene su Reglamento Interior de Protección de datos personales	no
12	Guerrero	Si	no	Comisión para el Acceso a la Información Pública del Estado de Guerrero	no	Ley de Acceso a la Información Pública del Estado de Guerrero	no	1.- Lineamientos y Criterios Generales para la Clasificación y Desclasificación de la Información de los Sujetos Obligados	no
13	Hidalgo	Si	no	Instituto de Acceso a la Información Pública Gubernamental de Hidalgo	no	Ley de Transparencia y Acceso a la Información Publica Gubernamental del Estado de Hidalgo	no	no	no

No.	Estado	Regula la protección de Datos Personales		Órgano encargado de la protección de Datos Personales		Ordenamiento Legal que regula la protección de Datos Personales		Procedimiento o Mecanismos que han implementado para cumplir con estas funciones	
		En Entes Públicos	En Entes Privados	En Entes Públicos	En Entes Privados	En Entes Públicos	En Entes Privados	En Entes Públicos	En entes Privados
14	Jalisco	Si	si	Instituto de Transparencia e Información Pública de Jalisco	El Código Civil no define si algún órgano debe proteger los datos personales	Ley de Transparencia e Información Pública del Estado de Jalisco	Código Civil del Estado de Jalisco (art. 40 bis)	1.- Lineamientos generales para el manejo, mantenimiento, seguridad y protección de la información confidencial. 2.- Lineamientos Generales para la clasificación, desclasificación, custodia de la información reservada y confidencial, que deberán observar los sujetos obligados previstos en el artículo 3 de la Ley de Transparencia e Información Pública del Estado de Jalisco. 3.- Lineamientos generales para la elaboración de versiones públicas respecto de documentos que contengan partes o secciones relativas a información reservada y/o confidencial, que se encuentren en poder de los sujetos obligados previsto por el artículo 3 de la Ley de Transparencia e Información Pública del Estado de Jalisco.	no

No.	Estado	Regula la protección de Datos Personales		Órgano encargado de la protección de Datos Personales		Ordenamiento Legal que regula la protección de Datos personal		Procedimiento o Mecanismos que han implementado para cumplir con estas funciones	
		En Entes Públicos	En Entes Privados	En Entes Públicos	En Entes Privados	En Entes Públicos	En Entes Privados	En Entes Públicos	En entes Privados
15	México	Si	no	Instituto de Transparencia y Acceso a la Información Pública del Estado de México	no	Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios	no	1.- Lineamientos para el manejo, mantenimiento, y seguridad de los datos personales, que se encuentran en posesión del Poder Ejecutivo del Estado de México, las Dependencias y Organismos Auxiliares, los Fideicomisos Públicos y la Procuraduría General de Justicia, como sujetos obligados de la Ley de Transparencia y Acceso a la Información Pública del Estado de México. 2.- Lineamientos para la recepción, trámite y resolución de las solicitudes de acceso a la información pública, acceso, modificación, sustitución, rectificación o supresión parcial o total de datos personales, así como de los recursos de revisión que deberán observar los sujetos obligados por la Ley de Transparencia y Acceso a la Información Pública del Estado de México y municipios. 3.- Lineamientos para vigilar el cumplimiento de las obligaciones de la Ley de Transparencia y Acceso a la Información Pública del Estado de México en el ámbito del Poder Ejecutivo del Estado de México, las dependencias y Organismos Auxiliares, los Fideicomisos Públicos y la Procuraduría General de Justicia del Estado de México.	no

No.	Estado	Regula la protección de Datos Personales		Órgano encargado de la protección de Datos Personales		Ordenamiento Legal queregula la protección de Datos personal		Procedimiento o Mecanismos que han implementado para cumplir con estas funciones	
		En Entes Públicos	En Entes Privados	En Entes Públicos	En Entes Privados	En Entes Públicos	En Entes Privados	En Entes Públicos	En entes Privados
16	Michoacán	Si	no	Instituto para la Transparencia y Acceso a la Información Pública del Estado de	no	Ley de Transparencia y Acceso a la Información Pública del Estado de Michoacán de	no	no	no
17	Morelos	Si	no	Instituto Morelense de Información Pública y Estadística.	no	Ley de Información Pública, Estadística y Protección de Datos Personales del Estado	no	1.- Reglamento sobre la clasificación de la información pública	no
18	Nayarit	Si	no	Instituto de Transparencia y Acceso a la Información Pública del Estado de Nayarit	No	Ley de Transparencia y Acceso a la Información Pública del Estado de Nayarit	no	1.- Acuerdo de Lineamientos para la Clasificación y Desclasificación de la Información en poder de las entidades públicas	no
19	Nuevo León	Si	no	Comisión de Transparencia y Acceso a la Información del Estado de Nuevo León	No	Ley de Transparencia y Acceso a la Información del Estado de Nuevo León	no	no	no
20	Oaxaca	Si	no	Instituto Estatal de Acceso a la Información Pública de Oaxaca	No	Ley de Protección de Datos Personales del Estado de Oaxaca.	no	1.- Implementación del Registro Estatal de Datos Personales. 2.- Manual Protección de Datos Personales Oaxaca. 3.- Lineamientos de Protección de Datos Personales.	no
21	Puebla	Si	no	Instituto Estatal de Acceso a la Información Pública de Oaxaca	No	Ley de Transparencia y Acceso a la Información Pública del Estado de Puebla	no	1.- Lineamientos Generales de Clasificación y Custodia de la información Reservada y Confidencial que deberán observar el Ejecutivo del Estado, las Dependencias y Entidades de la Administración Pública Estatal	no

No.	Estado	Regula la protección de Datos Personales		Órgano encargado de la protección de Datos Personales		Ordenamiento Legal que regula la protección de Datos Personales		Procedimiento o Mecanismos que han implementado para cumplir con estas funciones	
		En Entes Públicos	En Entes Privados	En Entes Públicos	En Entes Privados	En Entes Públicos	En Entes Privados	En Entes Públicos	En entes Privados
22	Querétaro	Si	si	Comisión Estatal de Información Gubernamental de Querétaro	El Código Civil no define si algún órgano debe proteger los datos personales	Ley Estatal de Acceso a la Información Gubernamental en el Estado de Querétaro	Código Civil (Arts. 43 a 47)	no	no
23	Quintana Roo	Si	no	Instituto de Transparencia y Acceso a la Información Pública de Quintana Roo	No	Ley de Transparencia y Acceso a la Información Pública del Estado de Quintana Roo	no	1.- Lineamientos Generales para la clasificación y desclasificación de la información pública de los sujetos obligados de la Ley de Transparencia y Acceso a la Información Pública del Estado de Quintana Roo.	no
24	San Luis Potosí	Si	no	Comisión Estatal de Garantía de Acceso a la Información Pública de San Luis Potosí	No	Ley de Transparencia y Acceso a la Información Pública del Estado de San Luis Potosí	no	1.- Normas para la protección, tratamiento seguridad y resguardo de los datos personales en posesión de los entes obligados. 2.- Registro Estatal de Datos Personales	no
25	Sinaloa	Si	no	Comisión Estatal para el Acceso a la Información Pública del Estado de Sinaloa	No	Ley de Acceso a la Información Pública del Estado de Sinaloa	no	1.- Se utiliza el mismo procedimiento de las solicitudes de información para acceder a los datos personales ya que su ley no lo contempla	no
26	Sonora	Si	no	Sujetos Obligados	No	Ley de Acceso a la Información Pública del Estado de Sonora	no	no	no
27	Tabasco	Si	no	Instituto Tabasqueño de Transparencia y Acceso a la Información Pública	No	Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco	no	1.- Reglamento de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco	no

No.	Estado	Regula la protección de Datos Personales		Órgano encargado de la protección de Datos Personales		Ordenamiento Legal que regula la protección de Datos Personal		Procedimiento o Mecanismos que han implementado para cumplir con estas funciones	
		En Entes Públicos	En Entes Privados	En Entes Públicos	En Entes Privados	En Entes Públicos	En Entes Privados	En Entes Públicos	En entes Privados
28	Tamaulipas	Si	no	Instituto de Transparencia y Acceso a la Información del Estado de Tamaulipas	No	Ley de Información Pública del Estado de Tamaulipas	no	no	no
29	Tlaxcala	Si	si	Comisión de Acceso a la Información Pública y Protección de Datos Personales del Estado de Tlaxcala	Comisión de Acceso a la Información Pública y Protección de Datos Personales del Estado de	Ley de Acceso a la Información Pública y Protección de Datos Personales del Estado de Tlaxcala	Ley de Acceso a la Información Pública y Protección de Datos Personales del Estado	1.- Lineamientos Generales para la clasificación y desclasificación de la información pública y confidencial. 2.- Registro Estatal de Datos Personales.	no
30	Veracruz	Si	No	Instituto Veracruzano de Acceso a la Información	No	Ley de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave	no	1.- Lineamientos Generales para orientar sobre la creación o modificación de ficheros o archivos que contengan datos personales, los que deberán ser acatados por los sujetos obligados por la Ley de Transparencia de Acceso a la Información Pública para el Estado de Veracruz Ignacio de la Llave	no
31	Yucatán	Si	No	Instituto de Acceso a la Información Pública del Estado de Yucatán	No	Ley de Acceso a la Información Pública para el Estado y los Municipios de Yucatán	no	1.- Lineamientos generales para la clasificación y desclasificación de información en posesión de los sujetos obligados.	no
32	Zacatecas	Si	No	Comisión Estatal para el Acceso a la Información Pública de Zacatecas	No	Ley de Acceso a la Información Pública del Estado de Zacatecas	no	1.- Reglamento para la protección de datos personales en el Estado de Zacatecas. 2.- Lineamientos para clasificación de información pública del Estado de Zacatecas	no

Conclusiones

La regulación de la privacidad y protección de datos personales ha sido abordada a nivel Mundial en forma muy particular por cada país. Ello se debe, en gran medida, a los intereses Económicos, políticos y sobre todo responde a las estrategias comerciales de cada país.

El análisis que tenemos sobre el estado de Michoacán sobre la privacidad y los datos de las personas en las relaciones entre empresas y Consumidores no se encuentra regulado. Asimismo, existen otras disposiciones sobre privacidad que se encuentran contenidas en otros ordenamientos jurídicos a nivel federal. En la medida en la que exista una mayor penetración y uso del Internet en Michoacán, se deberá evaluar la posibilidad de crear un marco jurídico más amplio y eficiente que proteja los datos e información que proporcionen los ciudadanos no sólo a los sitios web de las empresas, sino sobre todo a los órganos gubernamentales cuyos servicios se ofrecerán completamente en línea en un futuro no muy lejano.

Por último, insistimos una vez más en la urgente necesidad de que el H. Congreso de la Unión organice una Mesa de Trabajo sobre Privacidad y Protección de Datos Personales, con el objeto de que nuestros legisladores conozcan las opiniones de los sectores interesados de la sociedad.

En el análisis de la tabla obtenemos los siguientes resultados

a) En todos los Estados y el D.F. se regula la Protección de Datos Personales en entes Públicos, ya sea en las mismas Leyes de Transparencia o en Leyes especiales sobre Protección de Datos Personales.

b) En 4 Estados (Colima, D.F., Guanajuato y Oaxaca) existe Ley especial en materia de Protección de Datos Personales (Ley de Datos Personales)

c) En 4 Estados (Colima, Jalisco, Querétaro y Tlaxcala) se regula la Protección de Datos Personales en entes Privados o Particulares.

d) En 2 Estados (Jalisco y Querétaro) se aplica supletoriamente el Código Civil Local para la Protección de Datos Personales en Privados. Cabe señalar que no es claro lo establecido en el Código Civil Local.

e) 21 Estados han emitido Lineamientos, Reglamentos o Manuales en materia de Protección de Datos Personales en entes Públicos (Sujetos Obligados)

f) Sólo 2 Estados (Oaxaca y Tlaxcala) regulan la implementación de un Registro Estatal de Datos Personales.

Aportaciones y sugerencias

Podemos analizar que a nivel nacional los únicos estados que cuentan con una buena protección como en el ámbito público y privado son los siguientes estados.

1.- colima.

Los órganos encargados del ente público y privado es la Comisión Estatal para el Acceso a la Información Pública de Colima y el ordenamiento legal es la Ley de Protección de Datos Personales del Estado de Colima.

2.-jalisco

Los órganos encargados del ente público es el Instituto de Transparencia e Información Pública de Jalisco y el ente El Código Civil no define si algún órgano debe proteger los datos personales y el ordenamiento legal en el ámbito público es Ley de Transparencia e Información Pública del Estado de Jalisco y en el ámbito privado Código Civil del Estado de Jalisco (art. 40 bis).

3.-queretaro

Los órganos encargados del ente público es el Comisión Estatal de Información Gubernamental de Querétaro y el ente privado El Código Civil no define si algún órgano debe proteger los datos personales y el ordenamiento legal en el ámbito público es Ley Estatal de Acceso a la Información Gubernamental en el Estado de Querétaro y en el ámbito privado Código Civil (Arts. 43 a 47).

4.-Tlaxcala

Los órganos encargados del ente público y privado es la Comisión de Acceso a la Información Pública y Protección de Datos Personales del Estado de Tlaxcala y el ordenamiento legal es la Ley de Acceso a la Información Pública y Protección de Datos Personales del Estado de Tlaxcala.

Analizaremos al estado de Michoacán en este estado nada más tenemos implementada Instituto para la Transparencia y Acceso a la Información Pública del Estado de Michoacán que está regido en el ámbito gubernamental.

Ámbito extranjero analizaremos la trayectoria que tubo cada país y el año en que ellos ponen en marcha la ley sobre la protección de datos.

1. **Organización de Naciones Unidas (ONU)**. En 1948, adopta el documento conocido como *Declaración Universal de Derechos Humanos*, en la que el artículo 12 señala que las personas tienen derecho a la protección de la ley de sus datos personales.

2. **Alemania**. En 1970 fue aprobada la primera ley de protección de datos (Datenschutz). En 1977, el Parlamento Federal Alemán aprueba la Ley Federal Bundesdatenschutzgesetz. Estas leyes impiden la transmisión de cualquier dato personal sin la autorización de la persona interesada.

3. **Suecia**. En 1973 fue publicada la que fue una de las primeras leyes de protección de datos en el mundo.

4. **Estados Unidos de Norteamérica**. La protección de datos tiene base en la ley de privacidad de 1974.

5. **Unión Europea**. El primer convenio internacional de protección de datos fue firmado en 1981 por Alemania, Francia, Dinamarca, Austria y Luxemburgo. Es conocido como “Convenio 108” o “Convenio de Estrasburgo”. En los 90’s, se establece una norma común que se denominó Directiva 95/46/CE. La directiva es referente a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

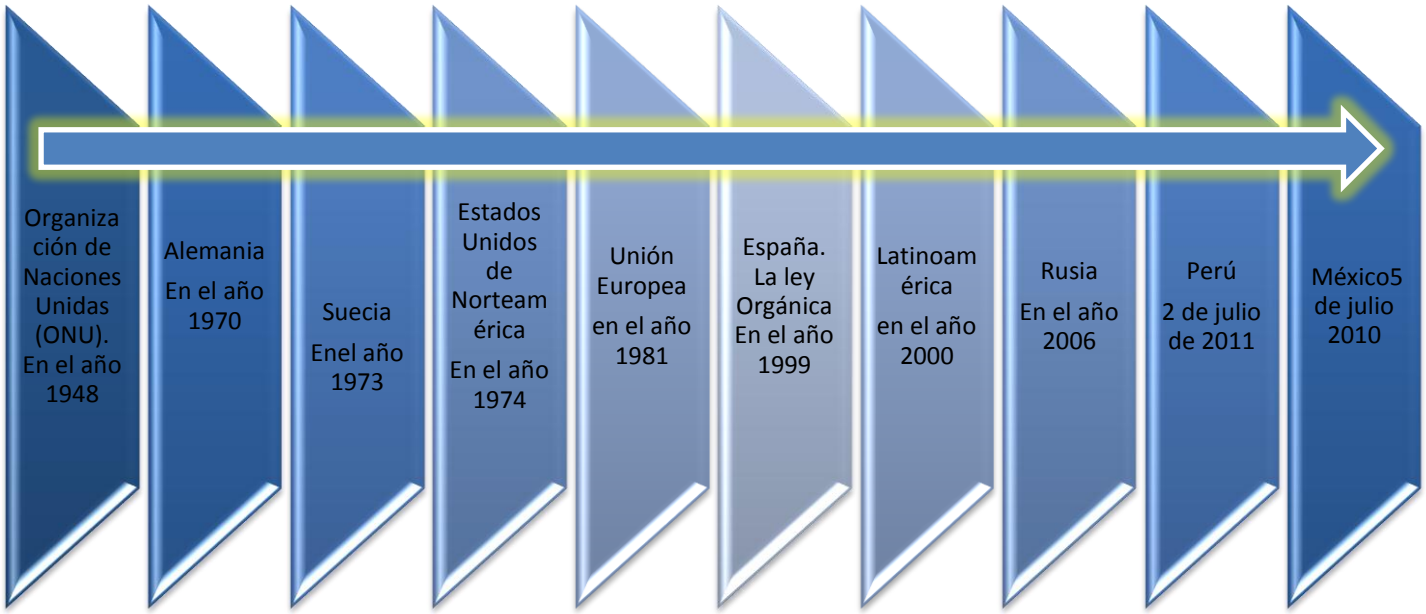
6. **España**. La ley Orgánica 15 de 1999, establece la Protección de Datos de Carácter Personal. Está ley ha sido importante para Latinoamérica porque se ha utilizado como firme referente del modelo europeo.

7. **Latinoamérica**. En América Latina, las leyes de protección de datos personales surgen como una necesidad derivada del incremento del uso de las tecnologías de la información y el aumento de las vulnerabilidades asociadas. En su mayoría, estas leyes se asemejan al modelo europeo: En Argentina la Ley 25.326 (2000), Chile (1999), Panamá (2002), Brasil (1997), Paraguay (2000), Uruguay (2008).

8. **Rusia**. En el año 2006 fue aprobada una exhaustiva ley de protección de datos personales.

9. **Perú**. La ley 29.733 del 2 de julio de 2011 es la más reciente ley de protección de datos personales en el mundo.

10. **México**. La Ley Federal de Protección de Datos Personales en Posesión de Particulares fue publicada en el Diario Oficial de la Federación el 5 de julio de 2010, entró en vigor un día después y tiene efecto a partir de enero del año 2012.



Bibliografía

- *Merodio Lopez Juan Carlos. (2008). Derecho, Editor: SANTILLANA*
- *Velázquez García Arturo Materia de titulación .Instituto tecnológico de Morelia*
- *Dra. Lina Ornelas (2010). Las facultades del ifai avisos de privacidad y autorregulación. Clasificación estadística de delitos*
- *Dr. Santiago Acuario del pino, Profesor de derecho informático de la Puce, Delitos informáticos*
- *Dip. francisco Javier Ramírez acuña, presidente. sen. Carlos Navarrete Ruiz, presidente. Dip. Georgina Trujillo Zentella, secretaria. sen. Renán Cleominio Zoreda novelo, secretario. Rúbricas. (27 de abril de 2010)" ley federal de protección de datos personales en posesión de los particulares, México, D.F.*
- *Juan Carlos oré. (junio 2006). Introducción a la seguridad de la información. juancarlosore@yahoo.com*
- *DR © 2009, instituto de acceso a la información pública del distritofederal. dirección de capacitación y cultura de la transparencia. la morena no. 865, local 1, col. Narvarte poniente, del. Benito Juárez, c. p. 03020, México, distrito federal. "plaza de la transparencia". primera edición, diciembre de 2009. isbn: 978-607-95070-0-8.*
- *Fígoli pacheco, Andrés. (1998). El acceso no autorizado a sistemas informáticos, Uruguay, publicación hecha en internet, www.derecho.org.*
- *merlat, máximo, seguridad informática: los hackers, buenos aires argentina, 1999, publicación hecha en internet. www.monografías.com.*
- *www.dercho.org.pe. Reyna Alfaro Luis miguel, fundamentos para la protección penal de la información como valor económico de la empresa.*
- *c. José María valencia delgado diputado presidente ley de protección de datos personales del estado de colima. 28 de mayo del año 2002.*
- *m. en i.a. miguel Alejandro Orozco malo m. en a.c. Alejandro rubio Pérez la seguridad informática y la ley federal de transparencia y acceso a la información*

- *Eugenio Elorduy Walter , Gobernador del estado (rubrica),Bernardo h. Martínez Aguirre, Secretario general de gobierno (rubrica), Congreso del estado de b.c. Ley de acceso a la información pública para el estado de baja california*

- *http://troya.blogcindario.com/2008/11/00011-legislacion-informatica-concepto-alcances-y-regulacion.html. Israel Barquera lunes, 07 de noviembre de 2011*

- *www.deloitte.com/mx aviso de privacidad atencion@ifai.org.mx. Protección de datos personales http://troya.blogcindario.com/2008/11/00011-legislacion-informatica-concepto-alcances-y-regulacion.html. Definición de legislación. http://www.definicionabc.com/derecho/legislacion.php*

- *http://www.cavaju.net/2007/03/los-mtodos-ms-habituales-para-robar.html. Métodos más usuales para robar información (03/2007).*

- *http://delitosinformaticos.com/legislacion/espana.shtml. Artículos del Código Penal Español referentes a Delitos Informáticos (Ley-Orgánica 10/1995, de 23 de Noviembre/ BOE número 281, de 24 de Noviembre de 1.995)*

- *http://www.ifai.org.mx/nivel2/acceso.html instituto federal de acceso a la información pública. Lineamientos para la clasificación y desclasificación de la información de las dependencias y entidades de la administración pública federal. Diario oficial de la federación. Distrito federal, México. 18 de agosto de 2003.*

- *http://seguridad.internet2.ulsa.mx verónica Bátiz Álvarez, Ulsa Mario Farías Elinos, Ulsa legislación informática en México Juan Carlos ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal.*

- *http://mexico.cnn.com/tecnologia/2012/03/29/legisladores-definen-cuales-son-los-delitos-informaticos-y-su-castigo. Legisladores definen cuáles son los delitos informáticos y su castigo. 29 de marzo de 2012*