UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

"NORMATIVIDAD Y LEGISLACION DIRIGIDA A LA PROTECCION DE DATOS EN TECNOLOGIA DE LA INFORMACION"

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERA EN COMPUTACION

P R E S E N T A:

GRISELDA PEREZ OSORIO

ASESOR: M.C. JAQUELIN LOPEZ BARRIENTOS

MEXICO, D. F. **2003**

A

" Recorri un largo camino
Con muchos obstáculos
Y con ello me fortalecí
Para llegar a ésta etapa de mi vida
Con las fuerzas suficientes
Para seguir adelante."

- DOY GRACIAS A DIOS

- A mi madre por su comprensión y su apoyo en todo este tiempo que me ha llevado a concluir con este maravilloso proyecto.

- A José Ramón por su incansable apoyo y orientación para forjar en mí el espíritu de superación que me ha dado la fuerza para salir adelante.

- A la Universidad Nacional Autónoma de México por todos los conocimientos que en ella obtuve, por ser una hija más de ésta maravillosa casa de estudios de la que me siento orgullosa.

- A todos mis maestros que compartieron sus conocimientos conmigo, por que parte de lo que soy se lo debo a ellos.

- A la maestra M.C. Jaquelin López Barrientos por su maravilloso esfuerzo y su tiempo, así como su ahínco para terminar este hermoso trabajo.

- A mi familia.

C

ÍNDICE *PÁG.*

CAPÍTULO III

SEGURIDAD DE LA INFORMACIÓN

CAPÍTULO IV

ADMINISTRACIÓN DE LA SEGURIDAD

CAPÍTULO V

PROPUESTAS

CAPÍTULO VI

ÉTICA INFORMÁTICA

PRÓLOGO

En la actualidad las computadoras se utilizan no solo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio para obtener y conseguir información, tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos.

Las más diversas ramas del conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporadas a sistemas informáticos que, en la práctica cotidiana, de hecho sin limitaciones, entrega con facilidad a quien lo desee un conjunto de datos que hasta hace unos años sólo podían ubicarse luego de largas búsquedas y selecciones en que el hombre jugaba un papel determinante.

Las facultades que el fenómeno científico - tecnológico pone a disposición de Gobiernos y de particulares, con rapidez y ahorro de tiempo y energía, configuran un cuadro de realidades de aplicación y de posibilidades de juegos lícito e ilícito, en donde es necesario el derecho para regular los múltiples efectos de una situación nueva y de tantas potencialidades en el medio social.

El desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales.

Si se tiene en cuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias y de identificación de las personas. Y si a ello se agrega que existen bancos de datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas; se comprenderá que están en juego o podrían llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico - institucional debe proteger.

No es la amenaza potencial de la computadora sobre el individuo lo que provoca desvelo, sino la utilización real por el hombre de los sistemas de información con fines de espionaje.

No son los grandes sistemas de información los que afectan la vida privada sino la manipulación o el consentimiento de ello, por parte de individuos poco conscientes e irresponsables de los datos que dichos sistemas contienen.

La humanidad no está frente al peligro de la informática sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en daño de las personas. Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

La protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial, e incluso de derecho administrativo. Estas distintas medidas de protección no tienen porque ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas.

Por eso, dadas las características de esta problemática sólo a través de una protección global, del ordenamiento jurídico, es posible alcanzar una defensa de los ataques a los sistemas informáticos.

Las personas que cometen los "Delitos Informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informáticos, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

La delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes, aunque no es el único medio. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente; conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

Se puede señalar que dado el carácter transnacional de los delitos cometidos mediante el uso de las computadoras, es conveniente establecer tratados de extradición o acuerdos de ayuda mutua entre los países, que permitan fijar mecanismos sincronizados de cooperación internacional para contrarrestar eficazmente la incidencia de la criminalidad informática.

Asimismo, la problemática jurídica de los sistemas informáticos debe considerar la tecnología de la información en su conjunto (chips, inteligencia artificial, redes, etc.), evitando que la norma jurídica quede desfasada del contexto en el cual se debe aplicar.

Por lo que en el ***capítulo I*** se darán los antecedentes tanto nacionales como internacionales; respecto a este tema la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), establece en 1998 una ley llamada Ley

Modelo sobre Comercio Electrónico junto con su Guía de Implementación, con el propósito de dar valor jurídico a los mensajes electrónicos, para aumentar el uso de las comunicaciones que operan sin el uso del papel y que sea aceptable en aquellos Estados que tengan sistemas jurídicos, sociales y económicos diferentes para contribuir de manera significativa al establecimiento de relaciones económicas internacionales comunes.

Ya que el apresuramiento de la actividad en el avance de la tecnología y la interdependencia mundial junto con los cambios en nuestro país, el gobierno de México decidió reorientar la política informática fomentando un mejor uso y aprovechamiento de las tecnologías de la información, tanto en la Administración Pública Federal como en la sociedad en general, y fomentando el desarrollo informático nacional en las actividades de la comunidad en torno a algunos proyectos para tener una industria informática competitiva en áreas con posibilidades de participación en los mercados globales, incorporando la informática en los procesos productivos, enriqueciendo los servicios, obteniendo el máximo provecho de la tecnología, para ello será necesario saber incorporar conocimiento y experiencia, en la medida que se pueda desarrollar e incorporar a nuestra cultura. Esto dependerá de la capacidad de adecuar los cambios que está sufriendo el mundo y las oportunidades que brinda esta tecnología a nuestra idiosincrasia.

Por ello el Instituto Nacional de Estadística, Geografía e Informática (INEGI) menciona que en la Administración Pública Federal existen diversas instituciones con atribuciones que directa e indirectamente inciden en el ámbito de la informática, Secretaría de Gobernación, Secretaría de Relaciones Exteriores, Secretaría de Hacienda y Crédito Público, Secretaría de Comercio y Fomento Industrial, Secretaría de Comunicaciones y Transportes, Secretaría de la Función Pública, Secretaría de Educación Pública, Comisión Federal de Telecomunicaciones y el Consejo Nacional de Ciencia y Tecnología cuya participación es necesaria para promover el desarrollo nacional en la materia.

Asimismo el INEGI ha contemplado ya la importancia de la normatividad en informática y para ello da a conocer las diferentes leyes que forman parte esencial de la norma informática mexicana. Ley Federal del Derecho de Autor, Ley de la Propiedad Industrial, Ley Federal de Telecomunicaciones, Ley de INEGI y la Ley del Código Penal Federal.

También se han realizado Foros de Consulta sobre Derecho e Informática con el cual los sectores académico, empresarial y público involucrados en esta nueva tecnología, han tenido la oportunidad de expresar libremente sus puntos de vista en las reuniones realizadas en diferentes Estados de la República Mexicana (D.F.; Veracruz; Guadalajara, Jalisco; Monterrey, Nuevo León; y Tijuana, Baja California), en la que los comentarios giraron en torno a los derechos de los ciudadanos a la confidencialidad de la información personal almacenada en base de datos, tipificación de delitos cometidos

con el uso de herramientas informáticas, protección de derechos de propiedad industrial entre otros.

Igualmente a nivel internacional existen países que han avanzado en crear una legislación en el campo de la informática entre los que se encuentran Portugal, en cuya Constitución aparecen algunos lineamientos en la materia; Suecia, por su Ley de Datos; la Ley Alemana de Protección de Datos; la Ley de Privacidad de Estados Unidos; la Ley Relativa a la Informática, los Archivos y las Libertades, de Francia, así como la Ley Francesa del Soporte Técnico; el Convenio para la Protección de las Personas en Relación con el Tratamiento Automatizado de Datos de Carácter Personal, de Estrasburgo; y la Ley Orgánica de Regulación de Tratamiento Automatizado de los Datos de Carácter Personal, de España, entre otros.

Según un estudio publicado en el Manual de las Naciones Unidas en la prevención y control de delitos informáticos (Nros. 43 y 44), el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada. Asimismo, otro reciente estudio realizado en América del Norte y Europa indicó que el 73% eran atribuibles a fuentes interiores y solo el 23% a la actividad delictiva externa.

Así como también existen en la Declaración de los Derechos Humanos y la Declaración Americana de los Derechos y Deberes del Hombre artículos en que las personas tienen derecho a un recurso efectivo, ante los tribunales nacionales, como nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Por todo esto es necesario que el régimen jurídico mexicano sobre comercio electrónico debería ser compatible con el derecho internacional en materia de comercio electrónico, logrando así mayor seguridad y certeza en las transacciones electrónicas tanto nacionales como internacionales.

En términos generales la legislación actual no reconoce el uso de los medios electrónicos de manera universal, y en caso de un litigio el juez o tribunal tendrán que allegarse de medios de prueba indirectos para determinar que una operación realizada por medios electrónicos es o no válida. Esta situación ha originado que empresas frenen sus inversiones orientadas a realizar transacciones por medios electrónicos, debido a la incertidumbre legal en caso de controversias.

En el ***capítulo 2*** se verá el análisis y el diagnóstico de la problemática, como consecuencia de estos antecedentes y las propuestas de los foros de Consulta sobre Derecho e Informática a la Honorable Cámara de Diputados se lograron reformar y adicionar diversas disposiciones del Código Civil para el Distrito Federal, en Materia Común y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley de Protección al

Consumidor el 29 de mayo del año 2000 tomando como base la adopción de los principios de la Ley Modelo de la Comisión de Naciones Unidas para el Derecho Mercantil Internacional, facilitando el uso del comercio electrónico entre México y los distintos países del orbe, considerando también que los principios de la Ley Modelo sobre Comercio Electrónico no contravienen nuestra legislación nacional y por el contrario contribuyen a la uniformidad de la legislación interna de los Estados sobre la materia.

Haciendo un diagnóstico a la problemática, la humanidad no está frente al peligro de la informática, sino frente a la posibilidad real de individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles (otorgar o adjudicar), la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento (daño o perjuicio) de las personas. Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

Por eso, dadas las características de esta problemática sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

Este tipo de acciones presentan las siguientes características principales: Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas. Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se encuentra trabajando. Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico. Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan. Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse. Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho. Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico. En su mayoría son imprudencia les y no necesariamente se cometen con intención, por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Así mismo se clasifican estos delitos de acuerdo a dos criterios: como *instrumento o medio* en las que se encuentran las conductas criminales que se valen de las computadoras como medio para falsificar documentos, variación de los activos y pasivos en la situación contable de las empresas, entre otros, y como *fin u objetivo* que son los delitos dirigidos a las computadoras, accesorios o programas.

Por lo que Hoy en día existe a nivel mundial una preocupación generalizada de mejorar la eficiencia de los servicios gubernamentales mediante el uso de las modernas tecnologías de la información. Sin embargo, sólo algunos países se han preocupado

por revisar su normatividad para adecuarla al nuevo contexto que impone el avance tecnológico.

Por otra parte, se requieren ir desarrollando las condiciones para que la población que quiera hacer uso de medios electrónicos y no tenga una infraestructura propia, pueda acceder a éstos. Para ello es conveniente analizar proyectos que se están llevando en otros países como los denominados "kioscos electrónicos públicos", donde la población puede utilizar computadoras conectadas a redes para acceder a servicios públicos y privados.

Estos planteamientos, permiten concluir que hay mucho por trabajar. Los medios electrónicos pueden representar una gran oportunidad para el desarrollo de nuestro país, si contamos con el marco normativo - administrativo adecuado para aprovechar las posibilidades que ofrecen.

Por lo que debido a la difusión de las tecnologías de la información, la mayoría de las organizaciones actuales están expuestas a una serie de riesgos derivados de una protección inadecuada o inapropiada de la información, lo que las hace vulnerables a muy diversos tipos de ataques desde amenazas físicas, como cortes eléctricos, hasta errores no intencionados de los usuarios, pasando por los virus informáticos o el robo, destrucción o modificación de la información, por lo que se plantean retos importantes a la seguridad de la información.

En el ***capítulo 3*** se verá la Seguridad de la Información que se refiere a la protección de sistemas de información contra el descubrimiento no autorizado o la modificación de información o la modificación de ésta igualmente de manera ilícita, ya sea que encuentre en una fase de almacenamiento, procesamiento o tránsito. También protege la negación de servicios a usuarios no autorizados incluyendo las medidas necesarias para detectar, documentar, y contrarrestar tales amenazas. La cual considera tres aspectos: *Amenazas* la cual cuenta con cuatro categorías generales (interrupción, intercepción, modificación, suplantación) a su vez existen ataques pasivos (no alteran la información) y ataques activos (implican algún tipo de modificación del flujo de datos transmitido). Los *Servicios de Seguridad* proporcionan una clasificación útil de los diferentes tipos de seguridad que se pueden requerir en cualquier sistema, producto, mecanismo o servicio relacionado con la tecnología de la información, dichos servicios son confidencialidad, autenticidad, integridad, no repudio, control de acceso y disponibilidad. Los *Mecanismos de Seguridad* son una combinación de elementos que en su conjunto permiten funcionar de manera confiable y segura al dispositivo o sistema al cual hayan sido incorporados, pero a la vez considerando que no se contempla un único mecanismo capaz de proveer todos los servicios antes mencionados y que la mayoría de ellos hacen uso de técnicas criptográficas para proporcionar la seguridad requerida. Entre los más importantes destacan los siguientes: Intercambio de autenticación, Cifrado, Integridad de datos, Firma digital, Control de acceso, lo que nos permite asegurar nuestra información transmitida por las redes.

Asimismo es importante notar que los sistemas requieren administrar la seguridad, por lo que se mencionan en el ***capítulo IV*** los dos campos que comprende esta administración:

Seguridad en la generación (procesamiento), localización (almacenamiento) y distribución (tránsito) de la información secreta, de modo que sólo pueda ser accedida por aquellas entidades autorizadas.

La política de los servicios y mecanismos de seguridad para detectar infracciones de seguridad y emprender acciones correctivas.

Cualquier objeto (usuario, administrador, programa, sistema, etc.) debe tener los privilegios necesarios para desarrollar su tarea y ninguno más. Esto quiere decir, cualquier usuario debe acceder a los recursos que necesite, para realizar las tareas que tenga encomendadas y sólo durante el tiempo necesario, también un sistema no es seguro escondiendo sus defectos o vulnerabilidades, debemos conocerlos y corregirlos, estableciendo las medidas de seguridad adecuadas. Manteniendo los errores o vulnerabilidades en secreto no evita que existan, y por lo tanto evita que se corrijan; cuando diseñemos una política de seguridad o establezcamos los mecanismos necesarios para ponerla en práctica, debemos contemplar todas las vulnerabilidades y amenazas, no basta establecer mecanismos muy fuertes y complejos en algún punto en concreto, sino que hay que proteger todos los posibles puntos de ataque.

Por lo que la seguridad de nuestro sistema no debe depender de un solo mecanismo por muy fuerte que éste sea, es necesario establecer varios mecanismos sucesivos, de manera que cualquier atacante tendrá que superar varias barreras para acceder a nuestro sistema.

Las medidas de seguridad que pueden establecerse en un sistema informático son de cuatro tipos fundamentales: lógicas, físicas, administrativas y legales, por lo que debemos considerar los riesgos, hay daños de menores consecuencias, siendo los errores y omisiones las causas más frecuentes, normalmente de poco impacto pero frecuencia muy alta, y otras el acceso indebido a los datos (a veces a través de redes), la cesión no autorizada de soportes magnéticos con información crítica (algunos dicen "sensible"), los daños por fuego, por agua (del exterior como puede ser una inundación, o una tubería interior), la variación no autorizada de programas, su copia indebida, persiguiendo el propio beneficio o el causar un daño, a veces por venganza, como las medidas tienen un costo, a veces los directivos se preguntan ¿cuál es el riesgo máximo que podría soportar su entidad? la respuesta no es fácil, depende de su dependencia respecto a la información y del impacto que su no disponibilidad pudiera tener en la entidad.

Como consecuencia de cualquier incidencia se pueden producir pérdidas, que pueden ser no sólo directas (y éstas las pueden cubrir los seguros), sino también indirectas,

como la no recuperación al perder los datos, o no poder tomar las decisiones adecuadas en el momento oportuno por carecer de información.

Por todos estos antecedentes internacionales y a nivel nacional, por la lucha de una legislación internacional como interna en nuestro país para lograr acuerdos contra las amenazas a los sistemas, y la inquietud de que estamos en un nuevo cambio, el presente trabajo de tesis tiene por objeto comentar algunas de las legislaciones que se han promulgado en diversos países y que las normas jurídicas que se han puesto en vigor están dirigidas a proteger la utilización abusiva de la información reunida y procesada mediante el uso de computadoras, e incluso en algunas de ellas se ha previsto formar órganos especializados que protejan los derechos de los ciudadanos amenazados por los ordenadores.

Desde hace aproximadamente diez años la mayoría de los países europeos han hecho todo lo posible para incluir dentro de la ley, la conducta que incurre en una falta penalmente, como el acceso ilegal a sistemas de computo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos.

En la mayoría de las naciones occidentales existen normas similares a los países europeos. Todos estos enfoques están inspirados por la misma preocupación de contar con comunicaciones electrónicas, transacciones e intercambios tan confiables y seguros como sea posible.

Las personas que cometen los "Delitos Informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informáticos, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que "ingresa" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Por lo que es necesario distinguir entre los diferentes crímenes informáticos, legislando los datos en Tecnología de la Información en la Constitución de los Estados Unidos

Mexicanos y estableciendo acuerdos globales y cooperación mutua a nivel mundial para la extradición de aquellos perpetradores y poder presentarlos ante los tribunales correspondientes, los cuales dictarán su sentencia de culpabilidad, aunado a que las empresas, instituciones, dependencias gubernamentales, etc., establezcan Normas, Procedimientos y Políticas que conlleven a la seguridad de sus equipos, datos, control de acceso, software y hardware por lo que en el ***capítulo V*** presento mi propuesta ante la Honorable Cámara de Diputados sobre reformas a la Ley que Establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública, contando con un marco jurídico que permita que la falta de apego a las políticas, normas y procedimientos cubran a la Federación, los Estados, el Distrito Federal y los Municipios de las acciones fraudulentas, espionaje, violaciones, falta de honradez, etc., que pongan en riesgo la integridad, la confidencialidad y la confiabilidad de la información de la institución como parte primordial de su patrimonio.

Para poder lograr el objetivo es necesario contar con una ética en informática que se verá en el ***capítulo VI*** es muy importante considerar el tema ya que nos habla del impacto que ha tenido la tecnología de información en la sociedad y del papel que juega en las empresas. La tarea ética frente a las empresas es una continua tarea de rehumanización que puede realizarse a través de legislación, siempre empujada por una especial visión ética de la sociedad.

Finalmente en las conclusiones escribo mi inquietud por saber que avances hay en Legislación sobre la protección de Datos en Tecnología de la Información, y que camino nos falta por recorrer, así como mis experiencias durante el proceso de elaboración de ésta Tesis.

CAPÍTULO I

ANTECEDENTES

PAGINACION

DISCONTINUA

1.1 LEY MODELO SOBRE COMERCIO ELECTRÓNICO

La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI ó más conocida por su acrónimo en ingles UNCITRAL[1]) es el órgano jurídico central del sistema de las Naciones Unidas en el ámbito del derecho mercantil internacional. La Asamblea General encomendó a la CNUDMI la labor de fomentar la armonía y unificación progresiva del derecho mercantil internacional y de tener presente, a ese respecto, el interés de todos los Estados[2].

La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) fue establecida por la Asamblea General en 1966 (resolución 2205(XXI) del 17 diciembre de 1966); en la que se vinieron preparando, desde los años 90 una especie de normas que se aprobaron por la Comisión en su 29° periodo de sesiones, celebrado en 1996, y complementada por un nuevo artículo 5 bis aprobado por la Comisión en su 31° periodo de sesiones, celebrado en 1998 llama la Ley Modelo sobre Comercio Electrónico junto con su Guía de implementación.

Esta Ley Modelo, tiene por objeto facilitar el uso de medios modernos de comunicación y de almacenamiento de información, por ejemplo el intercambio electrónico de datos (EDI)[3], el correo electrónico y la telecopia[4]. La Ley Modelo, proporciona los criterios para apreciar el valor jurídico de los mensajes electrónicos, será muy importante para aumentar el uso de las comunicaciones que se operan sin el uso del papel. Lo que trata esta ley es darle vigencia legal o valor legal a todo acuerdo que se hace dentro de un ambiente electrónico y que sea aceptable en aquellos Estados que tengan sistemas jurídicos, sociales y económicos diferentes para contribuir de manera significativa al establecimiento de relaciones económicas internacionales comunes.

La Ley Modelo consta de dos partes, la primera parte está constituida por 3 capítulos y la segunda parte por dos artículos. En la primera parte se establecen los principios generales, con el fin de dar un soporte legal al comercio electrónico en aquellos países donde se promulguen las leyes modelos. En la segunda parte del proyecto de Ley, compuesto de dos artículos, se refieren al transporte de mercancías en general, y una Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Comercio Electrónico.

El Capítulo 1°, se refiere a las disposiciones generales como el ámbito de aplicación, definiciones, interpretación y modificación mediante acuerdos. La característica

[1] UNCITRAL.- United Nations Commission on International Trade Law.
[2] Ver Anexo I.
[3] EDI (Intercambio Electrónico de Datos.- Se entenderá la transmisión electrónica de una computadora a otra, estando estructurada la información conforme a la norma ISO 9735, EDI esta amparada por la Organización de las Naciones Unidas.
[4] Telecopia.- correo electrónico o Telefacsimil.

principal de este articulado general, es que introduce el término "mensaje de datos[5]", es un término jurídico que se quiso utilizar para identificar lo que es un mensaje en un ambiente electrónico, se ha podido manejar únicamente la palabra mensaje o la palabra aviso, pero bueno, a lo mejor no hubiera tenido el contexto, y no se hubiera entendido su significado.

La modificación mediante acuerdo, está diseñada para facilitar la libertad del contrato, la interpretación para incitar a los eventuales usuarios e intérpretes de la Ley Modelo, para que tenga una mente amplia en su aplicación e interpretación, dado su origen internacional.

Otro punto interesante es lo que se ha llamado la equivalencia funcional. ¿Qué es la equivalencia funcional? es realmente tratar de poner dentro del ambiente electrónico, dentro de estos mensajes de datos, una equivalencia que sea igual a las funciones que se producen o que se logran con el documento de papel.

El Capítulo 2° se refiere a la aplicación de los requisitos legales de los mensajes de datos, comenzando por su reconocimiento jurídico, al señalar que no se negarán efectos jurídicos, validez o fuerza probatoria al mensaje de datos, por la sola razón de que está siendo conformada por un mensaje de datos. Este reconocimiento evidentemente es necesario y si queremos darle una base y un soporte legal a este comercio electrónico, tenemos que darle un soporte legal al mensaje de datos, no se puede admitir que se niegue validez, estamos hablando que se niegue ante un Tribunal, ante una Corte de Justicia o ante las partes, no pueden negar la existencia de un contrato por el simple hecho de que el contrato está evidenciado en un mensaje de datos.

El Capítulo 3° se refiere a la formación y validez de los contratos a través de los mensajes de datos, su reconocimiento por las partes, su atribución, su acuse de recibo y su tiempo y lugar de envío y recepción. Estos artículos no establecen normas directas, pero son útiles para definir los derechos y responsabilidades que nacen de los mensajes de datos.

La segunda parte de la Ley Modelo, está dirigida a la regulación del comercio electrónico en áreas específicas en los artículos 16 y 17.

En el artículo 16 se describen y especifican los diversos actos relacionados con los contratos de transporte de mercancía como por ejemplo indicación de las marcas, el número, la cantidad o el peso de las mercancías, declaración de la índole o el valor de las mercancías etc..

[5] Mensaje de datos.- Se entenderá por la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudiera ser entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el telex o el telefax.

En el artículo 17 se establece el principio de la singularidad del mensaje de datos, esto es muy importante, porque para que funcione el comercio electrónico y se pueda dar validez a los mensajes de datos, conformando por ejemplo un contrato de transporte, específicamente un conocimiento de embarque electrónico, es necesario que ese documento de embarque sea único, de ahí la condición de singularidad, que no pueda ser modificado, salvo por supuesto para hacer una transferencia o una cesión de los derechos, un endoso, este sistema es parte de la aplicación de la teoría de la equivalencia funcional.

La finalidad de la **Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Comercio Electrónico** es orientar a los Estados poco familiarizados con las técnicas de comunicación como a los estudiosos en la materia, de los medios electrónicos en los aspectos jurídicos de su empleo, para la incorporación de su régimen al derecho interno. En la información presentada en esta Guía se explica cómo las disposiciones incluidas en la Ley Modelo enuncian los rasgos mínimos esenciales a toda norma legal destinada a lograr los objetivos de la Ley Modelo. Esta información también puede ayudar a los Estados a determinar si existe alguna disposición de la ley que tal vez convenga modificar en razón de alguna circunstancia nacional en particular.

La Ley Modelo ha sido redactada en seis idiomas (Árabe, Chino, Español Francés, Ingles y Ruso), es un texto por el cual se pueda lograr la admisión legal del comercio.

Nuestras leyes exigen que los conocimientos de embarque sean firmados, y en este sentido las preguntas que surgen son ¿quién los firma? y ¿cómo los firma?. Esto ha ocasionado el surgimiento de las firmas digitales eso parece muy fácil, pero para ello se requiere de los sistemas criptográficos[6], pero entonces, como todo en la vida, se ha desatado una gran competencia entre las grandes empresas de computación, para que el patrón de firma sea de su propia empresa. Por lo que han acudido empresas apoyadas por estados para que hagan una Ley sobre los patrones de firmas digitales, que no es ninguna ley, sino sencillamente es una forma de que el programa que ellos tienen en esa empresa, sea el que acoja la comunidad internacional.

Esto ha ocasionado una enorme guerra entre empresas de computación, porque imagínense el negocio de que admitan un patrón de una firma determinada como firma digital, ese es un negocio que hay ahí inmenso.

La Comisión en su 34° periodo de sesiones del 25 de junio al 13 de julio de 2001 aprobó la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas por lo que:

[6] Criptografía.- (Kryptós = escondido, oculto; graphé = grafía, escritura): el arte o ciencia de escribir en cifra o en código, de tal forma que permita que sólo el destinatario lo descifre y comprenda

" La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional

Consiente de la gran utilidad de las nuevas tecnologías de identificación personal utilizadas en el comercio electrónico, generalmente conocidas como 'firmas electrónicas',

Deseosa de desarrollar los principios fundamentales enunciados en el artículo 7 de la ley modelo de la CNUDMI sobre Comercio Electrónico reglamentando el cumplimiento de la función de la firma en las operaciones de comercio electrónico,

Convencida de que la Ley Modelo de la CNUDMI sobre Firmas Electrónicas ayudará considerablemente a los Estados a formular una legislación que regule la utilización de técnicas modernas de autenticación y a mejorar la legislación ya existente.

Convencida que la armonización tecnológicamente neutral de ciertas normas relativas al reconocimiento jurídico de las firmas electrónicas dará una mayor certeza jurídica al comercio electrónico,

Considerando que la elaboración de una legislación modelo que facilite la utilización de las firmas electrónicas de forma que sea aceptable por Estados con distintos ordenamientos jurídicos, sociales y económicos podría contribuir al fomento de relaciones económicas armoniosas en el plano internacional,

Aprueba la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas, que figuran en el anexo II (consultar pagina 6 de este documento) del informe de la comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre la labor realizada en su 34° periodo de sesiones, junto con la Guía para la incorporación de la Ley Modelo al derecho interno.

Pide que se transmita a los gobiernos y a otros órganos interesados el texto de la Ley Modelo de la CNUDMI sobre Firmas Electrónicas, junto con la Guía para la incorporación de la Ley Modelo al derecho interno,

Recomienda a todos los Estados que, al formular o revisar su legislación, tengan presente esta nueva ley Modelo de la CNUDMI sobre Firmas Electrónicas, junto con la Ley Modelo de la CNUDMI sobre Comercio Electrónico, habida cuenta de la necesidad de unificar el derecho aplicable a las formas de comunicación, almacenamiento y autenticación de información sin soporte de papel.

1.1.1 ANEXO I

UNCITRAL está representada por 36 Estados (en su 34° período de sesiones el 25 del junio de 2001, Actualmente la Comisión está integrada por los miembros elegidos el 24 de noviembre de 1997 y el 16 de octubre de 2000;) cuyos mandatos expiran el día anterior al comienzo del período de sesiones anual de la Comisión correspondiente al año indicado entre paréntesis:

Alemania (2007), Austria (2004), Benin (2007), Brasil (2007), Burkina Faso (2004), Camerún (2007), Canadá (2007), China (2007), Colombia (2004), España (2004), Estados Unidos de América (2004), Federación de Rusia (2007), Fiji (2004), Francia (2007), Honduras (2004), Hungría (2004), India (2004), Irán (República Islámica del) (2004), Italia (2004), Japón (2007), Kenya (2004), la ex República Yugoslava de Macedonia (2007), Lituania (2004), Marruecos (2007), México (2007), Paraguay (2004), Reino Unido de Gran Bretaña e Irlanda del Norte (2007), Rumania (2004), Rwanda (2007), Sierra Leona (2007), Singapur (2007), Sudán (2004), Suecia (2007), Tailandia (2004), Uganda (2004) y Uruguay (2004, que alterna anualmente con la Argentina). Asistieron al período de sesiones observadores de los siguientes Estados: Arabia Saudita, Argentina, Australia, Azerbaiyán, Bélgica, Bulgaria, Chipre, Croacia, Cuba, Ecuador, Egipto, Eslovaquia, Eslovenia, Filipinas, Finlandia, Grecia, Guatemala, Indonesia, Iraq, Irlanda, Jamahiriya Árabe Libia, Kuwait, Líbano, Luxemburgo, Malawi, Malasia, Nigeria, Panamá, Perú, Polonia, Portugal, Qatar, República Checa, República de Corea, República Popular Democrática de Corea, Suiza, Turquía, Ucrania, Venezuela, Viet Nam, Yugoslavia y Zimbabwe.

También asistieron al período de sesiones observadores de las siguientes organizaciones internacionales:

a) Sistema de las Naciones Unidas: Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, Fondo Monetario Internacional.

b) Organizaciones Intergubernamentales: Agencia Espacial Europea, Banco Europeo de Reconstrucción y Desarrollo, Centro Europeo para la Paz y el Desarrollo, Corte Permanente de Arbitraje, Instituto Internacional para la Unificación del Derecho Privado, Organización Consultiva Jurídica Asiático – Africana, Organización de Cooperación y Desarrollo Económicos, Organización Intergubernamental para Transporte Internacional por Ferrocarril, Southeast European Cooperative Intiative.

c) Organizaciones no Gubernamentales Internacionales Invitadas por la Comisión: Asociación de Derecho Internacional, Asociación Europea de Estudiantes de Derecho, Asociación Internacional de Jóvenes Abogados, Association of the Bar of the City of New York, Cámara de Comercio Internacional, Centro Europeo para la Paz y El Desarrollo, Centro Nacional de Arbitraje Mercantil Internacional de el Cairo, Chartered Institute of Arbitratos, Comité Marítimo Internacional, Commercial Finance Association, Factors Chain Internacioanl, Federación Europea de Asociaciones de Factoring, Instituto de Información Jurídica Internacional, International Swaps, and Derivatives Association, Moot Alumni Association, Moot Alumni Association, Siciedad Árabe de Contadores Públicos, Unión de Abogados Europeos, Universidad de las Indias Occidentales.

1.1.2 ANEXO II

Ley Modelo de la CNUDMI sobre Firmas Electrónicas (2001)

Artículo 1 . - Ámbito de aplicación.

Artículo 2 .- Definiciones.

Artículo 3 .- Igualdad de tratamiento de las tecnologías para la firma.

Artículo 4 .- Interpretación.

Artículo 5 .- Modificación mediante acuerdos.

Artículo 6 .- Cumplimiento del requisito de firma.

Artículo 7 .- Cumplimiento de lo dispuesto en el artículo 6.

Artículo 8 .- Proceder del firmante.

Artículo 9 .- Proceder del prestador de servicios de certificación.

Artículo 10 .- Fiabilidad.

Artículo 11 .- Proceder de la parte que confía en el certificado.

Artículo 12 .- Reconocimiento de certificados extranjeros y de firmas electrónicas extranjeras.

BIBLIOGRAFÍA

Ley Modelo Sobre Comercio Electrónico.
http://www.biztob.com/images/es/legislacion_b2b.pdf

Comisión De Las Naciones Unidas Para El Derecho Mercantil Internacional (CNUDMI).
Http://www.un.org

Comisión De Las Naciones Unidas Para El Derecho Mercantil Internacional (CNUDMI).
http://www.uncitral.org/sp-index.htm

Ley Modelo Sobre Comercio Electrónico.
http://members.tripod.com/~DMaritimo/Cova.htm

Ley Modelo de la CNUDMI.
http://www.arkaios.com/ecommerce/leymodelo.htm

Historia y Antecedentes sobre CNUDMI.
http//www.mincomex.gov.co/ecommerce/foros/CNUDMI.asp

Lex Mercatoria.
http://www.inter-mediacion.com/arbleymercatoria.htm

Créditos Documentarios/Cartas de Crédito.
http:/www.bbv.es/BBV/europyme/mpcredoc.htm

Intercambio electrónico de Datos (EDI)
http//ciberconta.unizar.es/LECCION/EDI/205.HTM

1.2 ANTECEDENTES EN MÉXICO

1.2.1 Marco general

El apresuramiento de la actividad en el avance de la tecnología y la interdependencia mundial, junto con los cambios nacionales, dio un nuevo marco a la política informática. Además se derivaron diversas acciones con efectos sustanciales para el sector informático: la globalización de la economía, la apertura de fronteras al mercado de cómputo, la reorientación de la política y el mercado de telecomunicaciones, la privatización de los bancos, la desincorporación de empresas paraestatales y la redefinición del papel rector del Estado. Dentro de este contexto, el gobierno de México decidió reorientar sus acciones hacia una política informática concertada y de fomento.

1.2.1.1. Reorientación de la Política Informática

La política informática nacional se reorientó hacia dos vertientes principales: fomento de un mejor uso y aprovechamiento de las tecnologías de la información, tanto en la Administración Pública Federal como en la sociedad en general, y fomento del desarrollo informático nacional.

Tres componentes estructurales adquirieron relevancia dentro de esta política.

El primero de ellos se basó en una visión de largo plazo para planear un desarrollo sostenido y armónico de la informática nacional e identificar las metas y los programas que permitieran garantizar un sano crecimiento del mercado local y, sobre todo, un mayor aprovechamiento de la tecnología para los propósitos generales de modernización del país y en particular del Estado.

En segundo lugar, la consolidación de los cuerpos colegiados existentes[7] y la institución de aquellos que hacían falta, con la finalidad de garantizar continuidad en la perspectiva, representatividad en las opiniones y contrapeso en las acciones.

Por último, la instalación de un sistema de información oportuno y objetivo sobre informática y de monitoreo tecnológico a disposición de toda la comunidad para poder percibir con claridad la situación, orientar la actividad y corregir las acciones.

Además la política se fundamentó en una concentración de las actividades de la comunidad en torno a algunos proyectos y áreas estratégicas que permitieron agrupar las voluntades y los esfuerzos hacia acciones concretas, así como garantizar la

[7] (CIAPEM) Comité de Informática de la Administración Pública Estatal y Municipal y en la Administración Pública Federal desde 1971 el Comité Técnico Consultivo de Unidades de Informática (CTCUI) posteriormente llamado Comité de Autoridades de Informática de la Administración Pública (CAIAP) , como órgano asesor del Estado en materia de informática en la Administración Pública.

seguridad de los programas de cómputo manejados en cualquier medio electrónico, óptico o de cualquier otra tecnología.

En la Administración Pública Federal existen diversas instituciones con atribuciones que directa e indirectamente inciden en el ámbito de la informática, cuya participación es necesaria para promover el desarrollo nacional en la materia.

1.2.2 Según el INEGI las Instituciones de la Administración Pública Federal con Atribuciones Vinculadas con la Informática son:

Secretaría De Gobernación.- Vigilar el cumplimiento de los preceptos constitucionales por parte de las autoridades del país, especialmente a lo que se refiere a las garantías individuales, y dictar las medidas administrativas que requiere ese cumplimiento.

Secretaria de Relaciones Exteriores.- Promover, propiciar y asegurar la coordinación de acciones en el exterior de las dependencias y entidades de la Administración Pública Federal; y sin afectar el ejercicio de las atribuciones que a cada una de ellas corresponda, conducir la política exterior para la cual intervendrá en toda clase de tratos, acuerdos y convenciones en los que el país sea parte.

Secretaría de Hacienda y Crédito Público.- Proyectar y calcular los egresos del Gobierno Federal y de la administración pública paraestatal, haciéndolos compatibles con las disponibilidades de recursos y en atención a las necesidades y políticas del desarrollo nacional. Evaluar y autorizar los programas de inversión así como normar y coordinar los servicios de informática de las dependencias y entidades de la Administración Pública Federal.

Secretaría de Comercio y Fomento Industrial .- Formular y conducir las políticas generales de industria, comercio exterior, abasto y precios del país, con excepción de los precios de bienes y servicios de la Administración Pública Federal. Estudiar y determinar mediante reglas generales, conforme a los montos globales establecidos por la Secretaría de Hacienda y Crédito Público, los estímulos fiscales necesarios para el fomento industrial, el comercio interior y exterior y el abasto, incluyendo los subsidios sobre impuestos de importación, y administrar su aplicación, así como vigilar y evaluar sus resultados. Normar y registrar la propiedad industrial y mercantil, así como regular y orientar la inversión extranjera y la transferencia de tecnología, promover, orientar fomentar y estimular la industria nacional.

Secretaría de Comunicaciones y Transportes.- Formular y conducir las políticas y programas para el desarrollo del transporte y las comunicaciones de acuerdo a las necesidades del país. Otorgar concesiones y permisos previa opinión de la Secretaría de Gobernación para establecer y explotar sistemas de servicios telegráficos, teléfonos, sistemas y servicios de comunicación inalámbrica por telecomunicaciones y satélites,

de servicio público de procesamiento remoto de datos, estaciones de radio experimentales, culturales y de aficionados y estaciones de radiodifusión comerciales y culturales; así como vigilar el aspecto técnico del funcionamiento de tales sistemas, servicios y estaciones.

Secretaría de la Función Pública.- Vigilar el cumplimiento, por parte de las dependencias y entidades de la Administración Pública Federal, de las disposiciones en materia de planeación, presupuestación, ingresos, financiamiento, inversión, deuda, patrimonio, fondos y valores.

Secretaría de Educación Pública .- Organizar, controlar y mantener al corriente el registro de la propiedad literaria y artística. Vigilar con auxilio de las asociaciones de profesionistas, el correcto ejercicio de las profesiones.

Comisión Federal de Telecomunicaciones .- Expedir las disposiciones administrativas y las normas oficiales mexicanas en materia de telecomunicaciones, así como elaborar y administrar los planes técnicos fundamentales. Realizar estudios e investigación en materia de telecomunicaciones y elaborar anteproyectos de adecuación, modificación y actualización de las disposiciones legales y reglamentarias que resulten pertinentes. Establecer los procedimientos para la adecuada homologación de equipos, así como otorgar la certificación correspondiente o autorizar a terceros para que emitan dicha certificación, unidades de verificación, organismo de certificación y laboratorios de prueba en materia de telecomunicaciones, y acreditar peritos en dicha materia. Dar seguimiento a los compromisos adquiridos por México ante organismos y otras entidades internacionales en el ámbito de competencia de la Comisión.

Consejo Nacional de Ciencia y Tecnología .- Fungir como asesor del Ejecutivo Federal en la planeación, programación, coordinación, orientación, sistematización, promoción y encausamiento de las actividades relacionadas con la ciencia y la tecnología, su vinculación al desarrollo nacional y sus relaciones con el exterior.

Asimismo el INEGI ha contemplado ya la importancia de la normatividad en informática y para ello da a conocer las diferentes leyes que forman parte esencial de la norma informática mexicana.

1.2.3 Normatividad En Informática

Ley Federal del Derecho de Autor .- Esta Ley, reglamentaria del artículo 28 constitucional, tiene por objeto la salvaguardia y promoción del acervo cultural del la Nación; protección de los derechos de los autores, de los artistas interpretes o ejecutantes, así como de los editores, de los productores y de los organismos de radiodifusión, en relación con sus obras literarias programas de computación o

artísticas en todas sus manifestaciones, sus interpretaciones o ejecuciones, sus ediciones, sus fonogramas o videogramas, sus emisiones, así como de los otros derechos de propiedad intelectual.

Ley de la Propiedad Industrial .- Esta Ley tiene por objeto proteger la propiedad industrial mediante la regulación y otorgamiento de patentes de invención; registros de modelos de utilidad, diseños industriales, marcas y avisos comerciales; publicación de nombres comerciales; declaración de protección de denominaciones de origen, y regulación de secretos industriales.

Ley Federal de Telecomunicaciones .- Esta Ley es de orden público y tiene por objeto regular el uso, aprovechamiento y explotación del espectro radioeléctrico, de las redes de telecomunicaciones, de la comunicación vía satélite. Corresponde al Estado la rectoría en materia de telecomunicaciones, a cuyo efecto protegerá la seguridad y la soberanía de la Nación. En todo momento el Estado mantendrá el dominio sobre el espectro radioeléctrico y las posiciones orbitales asignadas al país.

Ley de INEGI .- La presente Ley es de orden público e interés social y sus disposiciones rigen a la información estadística y geográfica del país que son elementos consustanciales de la soberanía nacional, a la utilización que de la informática se requiera para los fines de aquéllas en las dependencias y entidades de la Administración Pública Federal.

Como institución responsable de la formulación de la política nacional en informática, a emprender en coordinación con otras dependencias de la Administración Pública y con distintos grupos sociales, una revisión profunda de las situación nacional que permita la planeación de las acciones requeridas para garantizar un desarrollo sostenido y armónico de la informática.

Ley del Código Penal Federal .- Sanciona a toda persona que sin autorización modifique, destruya, provoque perdidas, así como conozca o copie información o aquellas que estando autorizadas indebidamente modifique, destruya, provoque perdidas, así como conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, así como información del Estado o instituciones que integran el sistema financiero. (Artículo 211 del Libro segundo, Título noveno, Capitulo dos). Revelación de secretos (Artículo 210). Sanciones al robo simple o daño en propiedad ajena (Articulo 370). Daño en propiedad ajena (artículo 399).

1.2.4 Foros De Consulta

La Cámara de Diputados y el INEGI realizaron Foros de Consulta sobre Derecho e Informática[8], del 18 de septiembre al 4 de octubre de 1996 en el cual los sectores académico, empresarial y público involucrados en esta nueva tecnología, han tenido la oportunidad de expresar libremente sus puntos de vista en las reuniones realizadas en diferentes Estados de la República Mexicana (D.F.; Veracruz; Guadalajara, Jalisco; Monterrey, Nuevo León; y Tijuana, Baja California), en la que los comentarios más importantes de este evento giraron en torno a los siguientes aspectos:

Los derechos de los ciudadanos a la confidencialidad de la información personal almacenada en bases de datos.

Protección jurídica que deben recibir las bases de datos de carácter estratégico.

Tipificación de delitos cometidos con el uso de herramientas informáticas.

Valor probatorio del documento electrónico en procesos administrativos y judiciales.

Protección a los derechos de autor.

Protección de derechos de propiedad industrial.

Mecanismos de fomento al desarrollo y uso de la informática.

Condiciones de competencia entre los proveedores.

Prestación de servicios telemáticos, así como las condiciones de acceso universal a la infraestructura tecnológica y a la información.

Por lo anterior, los trabajos y conclusiones presentados en el Foro de Consulta sobre Derecho e Informática, serán analizados con detenimiento por la Honorable Cámara de Diputados y el INEGI, así como por los grupos de trabajo que sobre los distintos temas se integrarán, para llegar a propuestas específicas en torno al marco normativo que rige la actividad informática en nuestro país.

La oportunidad está abierta y de nuestra respuesta como comunidad organizada depende ahora el éxito de los objetivos que nos hemos planteado. Ante la sociedad de la información y próximos al nuevo milenio, hagamos que la informática se convierta en el instrumento de apoyo para el logro de mayores niveles de bienestar para todos los mexicanos.

[8] http://info.cddhcu.gob.mx

1.3 ANTECEDENTES INTERNACIONALES

En el mundo son pocos los países que han avanzado en crear una legislación en el campo de la informática. Destacan Portugal, en cuya Constitución aparecen algunos lineamientos en la materia; Suecia, por su Ley de Datos; la Ley Alemana de Protección de Datos; la Ley de Privacidad de Estados Unidos; la Ley Relativa a la Informática, los Archivos y las Libertades, de Francia, la Ley Francesa del Soporte Lógico; el Convenio para la Protección de las Personas en Relación con el Tratamiento Automatizado de Datos de Carácter Personal, de Estrasburgo; y la Ley Orgánica de Regulación de Tratamiento Automatizado de los Datos de Carácter Personal, de España, entre otros.

1.3.1 Antecedentes Externos

El Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos señala que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada. Asimismo, la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.

Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.

Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.

No-armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.

Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.

Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

Al respecto, según un estudio publicado en el Manual de las Naciones Unidas en la prevención y control de delitos informáticos (Nros. 43 y 44), el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada. Asimismo, otro reciente estudio realizado en América del Norte y Europa indicó que el 73% eran atribuibles a fuentes interiores y solo el 23% a la actividad delictiva externa.[9]

[9] Legislación Sobre Delitos Informáticos.- http://www.monografias.com/trabajos/legisdelinf/legisdelinf.shtml

En el orden internacional destacan como antecedentes de la protección de la intimidad y el honor de la persona en el tratamiento de sus datos:

1.3.1.1 La Declaración Universal de los Derechos Humanos[10]

* En su artículo 8 dice que "Toda persona tiene derecho a un recurso efectivo, ante los tribunales nacionales, que la ampare contra actos que violen sus derechos fundamentales reconocidos por la Constitución o la ley".

* El artículo 12 prescribe: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

1.3.1.2 La Declaración Americana de los Derechos y Deberes del Hombre [11]

* El artículo 5 declara que "Toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar".

* El artículo 18 proclama que "Toda persona puede recurrir a los tribunales para hacer valer sus derechos. Asimismo debe disponer de un procedimiento sencillo y breve por el cual la justicia la ampare contra actos de la autoridad que violen, en perjuicio suyo, alguno de los derechos fundamentales consagrados constitucionalmente".

Incluso, cabe destacar el **Proyecto de Convención Americana sobre Autodeterminación informativa** de 1997, compuesto de 21 artículos en los que se propone una regulación para la protección y movimiento internacional de datos, y el cual aborda temas importantes como el derecho a la información en la recolección de los datos, el consentimiento del afectado, la calidad, categorías, seguridad y cesión de los datos, los derechos y las garantías de las personas, el *habeas data*, las sanciones, los recursos, la agencia de protección de datos y el registro de datos.

[10] Declaración Universal De Derechos Humanos.- http://www.carbonell.com.ar/espa.htm
[11] Declaración Americana De Los Derechos Y Deberes Del Hombre.- http://www.nuncamas.org/document/internac/declamdh/declamdh_01.htm

1.3.1.3 En Europa

En Alemania

El 7 de abril de 1970, el Parlamento del estado alemán de Hesse, promulga su normativa de protección de datos *Datenshutz* convirtiéndose en el primer territorio con una norma dirigida a la protección de datos.
Después, el 27 de febrero de 1977, el Parlamento Federal de Alemania aprueba la *Datenshutz* Federal. En estos casos, se crea un Comisario Federal para la Protección de Datos *(Bundesbeauftragter fur den Datenshutz).*

En Francia

En 1978 se establece la Comisión Nacional de la Informática y de las Libertades, un organismo colegiado que tiene por objeto establecer un registro de bancos de datos de consulta ciudadana.

En España

Desde 1978, la Constitución, en su artículo 18, apartado 4, dice: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos... "

Relacionada con esta disposición constitucional, en España se ha publicado la Ley Orgánica 5/1992, de 29 de octubre, de regulación de tratamiento automatizado de los datos de carácter personal que tiene como objeto básico la protección de la intimidad y el honor de las personas.

1.3.1.4 En América Latina

En los Estados Unidos de América

El 31 de diciembre de 1974, el Congreso expide el *"Privacy Act* (literalmente acto de retiro)", con el objeto de proteger a los individuos en sus libertades y derechos fundamentales frente a la recolección y tratamiento automatizado de datos personales por parte de las agencias federales.

En Brasil

En 1988 la Constitución brasileña, en su artículo 5, numeral LXXII, se refiere al "conocimiento de informaciones relativas a la persona de la impetrante..." y a la rectificación de datos.
Aproximadamente 10 años más tarde, en Brasil se expide la Ley número 9.507, de 12 de noviembre de 1997 que reglamenta la disposición constitucional, con base en 23 artículos.

En Colombia

A partir de 1991, el artículo 15 de la Constitución de este país reconoce al habeas data como un derecho fundamental aún no reglamentado.

En Paraguay

Es a partir de 1992, teniendo como antecedente los registros obrantes en poder de la Policía Nacional, que la Constitución, en su artículo 135 reconoce el derecho de las personas para acceder a la información que le corresponda en archivos públicos y privados, para conocer la finalidad de esos registros y para actualizar, rectificar o destruir los mismos datos.

En Perú

Desde 1993, el artículo 200, inciso 3, de la Constitución establece de manera expresa el habeas data con los objetivos de que el interesado pueda acceder a la información pública, con ciertas limitantes, y evitar la difamación de la persona por la difusión o suministro a terceros de informaciones que afecten la intimidad personal y familiar.

En Ecuador

El artículo 30 de la Constitución vigente establece el habeas data con los objetos de acceder a los registros, bancos o bases de datos, conocer su uso y finalidad, así como para solicitar la rectificación, actualización, eliminación o anulación de los datos, en caso de que éstos sean erróneos o afecten ilegítimamente los derechos de las personas.

La ley de Control Constitucional de 1997 ya ha reglamentado la acción de habeas data.

En Argentina

La nueva Constitución de 1994, en su artículo 43, en su párrafo tercero, establece el habeas data como un amparo especial.

Sin embargo, pese a la gran demanda porque se regulara en ley secundaria el habeas data, es hasta el año 2000 que se expide la Ley 25326 de Protección de los Datos Personales, publicada en el Boletín Oficial correspondiente al 2 de noviembre del año mencionado.

En Argentina, el habeas data ha tenido gran recepción, y muestra de ello es que las provincias de Buenos Aires (artículo 20, inciso c de la Constitución local), Córdoba (artículo 50 de su Constitución), Chubut (artículo 56 de su Ley primaria) y Jujuy (artículo 23, inciso 6, de su Constitución), entre otras, prevén el habeas data.

En México, no obstante la gran tradición y entramado constitucional que se posee, no se ha otorgado a los gobernados la garantía procesal del habeas data. México no puede quedarse atrás de los países europeos y latinoamericanos, máxime si se toma en cuenta que los países que ya regulan el habeas data limitan el movimiento internacional de datos con aquellos países que no brinden condiciones equivalentes de seguridad a las propias, de donde se sigue que México, en alguna medida, se encontraría marginado de este movimiento internacional de datos en diferentes materias en las que pueden incluirse la comercial y económica.

BIBLIOGRAFIA

INEGI
http://www.inegi.gob.mx/informatia/espanol/pim/evolución.html

Memorias del Foro de Consulta Sobre Derecho e Informática
http://info.cddhcu.gob.mx

Jurisprudencia y Legislación Internacional
http://www.informatica-juridica.com/jurisprudencia.asp
http://www.informatica-juridica.com/legislacion.asp

La Ley de Habeas Data
http//www.peype.com/habeas.htm

Habeas Data
http//www.ulpiano.com/Pablopalazzicv.htm

Delitos_Informaticos2
http://www.stj-sin.gob.mx/Delitos_Informaticos2.htm

Declaración Universal De Derechos Humanos
http://www.carbonell.com.ar/espa.htm

Declaración Americana de los Derechos y Deberes del Hombre
http://www.nuncamas.org/document/internac/declamdh/declamdh_01.htm

CAPÍTULO II

DIAGNÓSTICO DE LA PROBLEMÁTICA Y ANÁLISIS

2.1 DIAGNÓSTICO DE LA PROBLEMÁTICA

2.1.1 Introducción

La humanidad no está frente al peligro de la informática, sino frente a la posibilidad real de individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas. Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

La protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial, e incluso de derecho administrativo. Estas distintas medidas de protección no tienen porque ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas.

Por eso, dadas las características de esta problemática sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los "delitos informáticos", los estudiosos en la materia los han catalogado como "delitos de cuello blanco" término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943.

2.1.2 Algunos Antecedentes Sobre Legislación Informática

Este tipo de acciones presentan las siguientes características principales:

Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.

Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.

Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.

Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.

Son muy sofisticados y relativamente frecuentes en el ámbito militar.

Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

En su mayoría son imprudenciales y no necesariamente se cometen con intención.

Ofrecen facilidades para su comisión a los menores de edad.

Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Asimismo, se clasifica a estos delitos, de acuerdo a dos criterios:

2.1.2.1 Como instrumento o medio.

En esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)

Variación de los activos y pasivos en la situación contable de las empresas.

Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)

Lectura, sustracción o copiado de información confidencial.

Modificación de datos tanto en la entrada como en la salida.

Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.

Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.

Uso no autorizado de programas de cómputo.

Incorporación de instrucciones que provocan "interrupciones" en la lógica interna de los programas.

Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.

Obtención de información residual impresa en papel luego de la ejecución de trabajos.

Acceso a áreas informatizadas en forma no autorizada.

Intervención en las líneas de comunicación de datos o teleproceso.

2.1.2.2 Como fin u objetivo.

En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

Programación de instrucciones que producen un bloqueo total al sistema.

Destrucción de programas por cualquier método.

Daño a la memoria.

Atentado físico contra la máquina o sus accesorios.

Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.

Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

Por otra parte, existen diversos tipos de delito que pueden ser cometidos y que se encuentran ligados directamente a acciones efectuadas contra los propios sistemas como son:

Acceso no autorizado: Uso ilegítimo de passwords y la entrada de un sistema informático sin la autorización del propietario.

Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.

Infracción al copyright de bases de datos: Uso no autorizado de información almacenada en una base de datos.

Interceptación de e-mail: : Lectura de un mensaje electrónico ajeno.

Estafas electrónicas: A través de compras realizadas haciendo uso de la red.

Transferencias de fondos: Engaños en la realización de este tipo de transacciones.

Por otro lado, la red Internet permite dar soporte para la comisión de otro tipo de delitos:

Espionaje: Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.

Terrorismo: Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.

Narcotráfico: Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

Otros delitos: Las mismas ventajas que encuentran en la Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

2.1.3 Así Mismo En Las Memorias De Los Foros De Consulta Sobre Derecho E Informática En La Ponencia No. 7 "Un Marco Normativo - Administrativo Que Favorezca La Prestación De Servicios Gubernamentales Por Medio De Redes Informáticas".
Por el Act. Carlos Jaso García Coordinador General de Información Pública de la Gestión Gubernamental.
Secretaría de Contraloría y Desarrollo Administrativo[12].

En resumen de su Ponencia comento lo siguiente:

Los avances de la tecnología de los últimos años hacen posible realizar un sinnúmero de actividades por medio de redes informáticas. La comunicación electrónica y la transferencia electrónica de documentos, en particular, permiten la prestación de servicios telemáticos públicos y privados; esto significa una oportunidad sin precedentes para simplificar y mejorar los servicios gubernamentales al evitar la necesidad de desplazamientos de los ciudadanos para la realización de trámites administrativos y, más aún, la posibilidad de brindar atención remota a comunidades lejanas y marginadas.

Para poder aprovechar el potencial de aplicación de las tecnologías de la información en la prestación de servicios públicos, México requiere contar con un marco normativo - administrativo que favorezca su desarrollo. En especial se requiere revisar la normatividad que incide en el sector público y en su interacción con la ciudadanía, a fin de posibilitar además de los procedimientos tradicionales, el uso de los medios electrónicos para la notificación y entrega de documentación.

Las adecuaciones normativas, deben apoyarse además en lineamientos administrativos que definan los estándares y medidas de seguridad indispensables para el uso de medios electrónicos.

Finalmente se requieren garantizar los derechos de los ciudadanos en cuanto a igualdad de acceso para la utilización de estos medios y la protección requerida en cuanto a confidencialidad de la información contenida o transmitida por medios electrónicos.

En este documento se analiza la problemática que se enfrenta en este contexto y se presentan algunas propuestas para resolver esta situación.

Problemática y propuestas

Hoy en día existe a nivel mundial una preocupación generalizada de mejorar la eficiencia de los servicios gubernamentales mediante el uso de las modernas tecnologías de la información. Sin embargo, sólo algunos países se han preocupado

[12] http://info.cddhcu.gob.mx

por revisar su normatividad para adecuarla al nuevo contexto que impone el avance tecnológico.

A nivel general, el uso de la tecnología en la Administración Pública enfrenta cuatro problemas principales:

1. El primero de ellos se relaciona con la normatividad administrativa y aun con aspectos de cultura tecnológica en cuanto al manejo de documentos por parte de las autoridades gubernamentales.

Al reemplazar los documentos tradicionales por sus equivalentes en medio digital, surgen preguntas como qué se entiende por un documento electrónico, cómo autentificar quién es el autor del mismo, cómo garantizar que un documento no ha sido alterado y cuáles son las reglas para su envío y recepción.

Para luchar con este problema resulta una condición básica, poder asumir que el documento electrónico provee la misma evidencia que el documento en papel y que el documento puede ligarse a su autor, de la misma forma que la firma autógrafa lo permite. Esta condición puede ser resuelta con las técnicas de criptografía y de firma electrónica.

Sin embargo, es claro que deben establecerse ciertos lineamientos como cuándo se requiere la firma electrónica, cuál es el tiempo de resguardo de información en línea, bajo qué condiciones debe almacenarse la información, cómo contender ante los riesgos de pérdida o violación de información, qué medidas de seguridad deben establecerse, qué protocolos de comunicación hay que utilizar y qué estándares deben establecerse para la transmisión electrónica de datos.

2. El segundo problema se relaciona más específicamente con la normatividad existente en diversos ámbitos.

La legislación mexicana que incide en los diversos procesos administrativos y judiciales, señala explícitamente la necesidad de entrega de documentos en medio tradicional, la notificación personal o por escrito y la firma autógrafa, entre otros aspectos.

Por ello, es necesario analizar las diversas disposiciones normativas y proponer las modificaciones que permitan utilizar además de los procedimientos tradicionales, los métodos electrónicos.

Es decir, el gobierno y la iniciativa privada deben ser autorizados a utilizar documentos electrónicos, emitirlos y recibirlos de las empresas y los particulares, siempre y cuando cumplan con ciertos requisitos relacionados con la obligación de asegurar que el uso de medios electrónicos está sustentado con las condiciones de seguridad requeridas

para autentificar los documentos, para evitar la pérdida de información y el acceso no autorizado a datos.

Asimismo, los particulares deben tener claros sus derechos en cuanto a la realización de trámites con el uso de estos medios y se requiere prever como dirimir en una controversia.

Así como existen peritos en los medios tradicionales, la legislación debe considerar figuras similares para el caso de los medios electrónicos. En otros países, existen ya auditores, peritos y notarios en informática. En México empiezan a surgir y es necesario que la normatividad defina su actuación.

3. Un tercer problema, se refiere a la necesidad de garantizar igualdad de acceso de la población a las nuevas facilidades que brinda la tecnología.

En este sentido, debe considerarse que la falta de una infraestructura adecuada de telecomunicaciones e informática y la limitada cultura tecnológica de la población en general, impediría en un principio que toda la población tuviera una igualdad en el acceso a los nuevos servicios.

Por ello, es necesario trabajar en dos aspectos: por una parte, que la normatividad permita la convivencia del uso de métodos tradicionales y métodos electrónicos y garantice una equidad en el trato a la ciudadanía independientemente del medio utilizado.

Por otra parte, se requieren ir desarrollando las condiciones para que la población que quiera hacer uso de medios electrónicos y no tenga una infraestructura propia, pueda acceder a los medios electrónicos. Para ello es conveniente analizar proyectos que se están llevando en otros países como los denominados "kioscos electrónicos públicos", donde la población puede utilizar computadoras conectadas a redes para acceder a servicios públicos y privados.

4. El cuarto problema radica en que la legislación vigente no establece garantías a los ciudadanos en cuanto al uso de datos personales contenidos o transmitidos por medios electrónicos. Es común ya en nuestros días que los datos proporcionados para determinados fines, sean comercializados sin ningún control. También estos datos pueden ser utilizados para favorecer actos de corrupción y discriminación.

Todos estos planteamientos, permiten concluir que hay mucho por trabajar. Los medios electrónicos pueden representar una gran oportunidad para el desarrollo de nuestro país, si contamos con el marco normativo - administrativo adecuado para aprovechar plenamente las posibilidades que ofrecen.

BIBLIOGRAFÍA

Memorias del Foro de Consulta Sobre Derecho e Informática
http://info.cddhcu.gob.mx

Julio Téllez Valdez
Legislación sobre Delitos Informáticos

2.2 ANÁLISIS

2.2.1 Introducción

El régimen jurídico mexicano sobre comercio electrónico debería ser compatible con el derecho internacional en materia de comercio electrónico, logrando así mayor seguridad y certeza en las transacciones electrónicas tanto nacionales como internacionales.

El comercio electrónico es un elemento que permitirá al sector productivo de nuestro país aprovechar la revolución informática actual pues representa una poderosa estrategia para impulsar la competitividad y eficiencia de las empresas mexicanas de todos tamaños; sin embargo, también constituye un enorme reto para el sector empresarial mexicano, el competir exitosamente en los mercados globales, utilizando las herramientas tecnológicas más convenientes.

Aspectos tales como la firma electrónica, que representa el consentimiento de las partes para la celebración de un acto jurídico determinado, no se considera pertinente legislar sobre sus características técnicas, en virtud de que se estaría contraviniendo el principio de neutralidad en que se basa la Ley Modelo de la CNUDMI, al comprometerse la legislación con una tecnología determinada, lo cual en su caso debería ser normado de manera temporal mediante la emisión de una Norma Oficial Mexicana.

En términos generales la legislación actual no reconoce el uso de los medios electrónicos de manera universal, y en caso de un litigio el juez o tribunal tendrán que allegarse de medios de prueba indirectos para determinar que una operación realizada por medios electrónicos es o no válida. Esta situación ha originado que empresas frenen sus inversiones orientadas a realizar transacciones por medios electrónicos, debido a la incertidumbre legal en caso de controversias.

Por lo anterior se mencionan las siguientes consideraciones:

2.2.2 Consideraciones

Es clara la necesidad de regular de manera específica lo que es la interacción a distancia, o aquella en que las partes no están físicamente presentes, la cual se ha convertido en una parte indispensable de las relaciones interpersonales, es gran parte de lo que hacemos hoy en día.

El sistema jurídico mexicano debe incluir las menciones necesarias para aprovechar los avances logrados no sólo en el ámbito comercial, sino también en otros campos como la protección de sistemas informáticos entre otros.

La adopción de los principios de la Ley Modelo de la Comisión de Naciones Unidas para el Derecho Mercantil Internacional, facilitaría el uso del comercio electrónico entre México y los distintos países del orbe; estos principios no contravienen nuestra legislación nacional y por el contrario contribuyen a la uniformidad de la legislación interna de los Estados sobre la materia.

La finalidad de la Ley Modelo es la de ofrecer al legislador nacional un conjunto de reglas aceptables en el ámbito internacional que le permitan eliminar algunos de esos obstáculos jurídicos con miras a crear un marco jurídico que permita un desarrollo más seguro de las vías electrónicas de negociación designadas por el nombre de "comercio electrónico".

La ausencia de un régimen general del comercio electrónico puede resultar en la incertidumbre para el sano y seguro desarrollo del comercio.

La adopción del criterio del equivalente funcional no debe dar lugar a que se impongan normas de seguridad más estrictas a los usuarios del comercio electrónico que las aplicables a la documentación consignada sobre papel.

La adopción de los principios de la Ley Modelo de la CNUDMI constituye lo que se conoce como legislación mínima, en virtud de que enuncia los rasgos mínimos esenciales referentes al tema del comercio electrónico. Así, "La Ley Modelo tiene por objeto enunciar los procedimientos y principios básicos para facilitar el empleo de las técnicas modernas de la comunicación para consignar y comunicar información en diversos tipos de circunstancias."

Por lo que la Ley Modelo fue considerada en los Foros de Consulta sobre Derecho e Informática que se llevo a cabo en diferentes Estados de la República Mexicana lo que dio como resultado propuestas a las Reformas de Ley, las cuales fueron emitidas en el Diario Oficial de la Federación el día 29 de mayo de 2000.

En materia de **Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal**, resulta necesario reconocer la posibilidad de que las partes puedan externar su voluntad o solicitar algún bien o servicio mediante el uso de medios electrónicos, e incluso dar validez jurídica al uso de medios de identificación electrónica.

En el Código Federal de Procedimientos Civiles se introducen reformas por virtud de las cuales se reconocen efectos jurídicos, validez y fuerza probatoria de los mensajes de datos. Se atiende igualmente al reconocimiento de los requisitos de

autenticidad[13], integridad[14] y confiabilidad[15] de la información, generada, comunicada o archivada a través de Mensajes de Datos.

En lo que se refiere al **Código de Comercio** se conseguirá una legislación mercantil innovadora y al día en aspectos informáticos, con ello se concederá la posibilidad de que los comerciantes puedan ofertar bienes o servicios a través de medios electrónicos, también podrán conservar la información que por ley deben llevar mediante medios electrónicos.

La Ley Federal de Protección al Consumidor, tiene por objeto promover y proteger los derechos del consumidor, para incorporar las disposiciones mínimas que aseguren los derechos básicos del consumidor en las operaciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología.

Con esta adecuación al sistema jurídico mexicano se logrará:

1. Fomentar el desarrollo de la infraestructura para poder acceder a los nuevos mercados informáticos;

2. Fomentar el uso de medios electrónicos en las operaciones comerciales, y

3. Contar con un esquema jurídico integral.

2.2.3 ANÁLISIS A LAS REFORMAS DEL 29-05-00

Las reformas vigentes desde mayo del 2000 incluyen: Validación del consentimiento otorgado vía electrónica, reconocimiento a los medios electrónicos como prueba de una transacción, siempre y cuando cumplan con los requisitos de confiabilidad, factibilidad y accesibilidad. Si estos requisitos se cumplen se reconoce la integridad y autenticidad del mensaje electrónico, además se eliminó la necesidad de un acuerdo previo por escrito para realizar la transacción electrónica.

En cuanto a la Ley Federal de Protección al Consumidor, se estableció que el proveedor utilizará la información proporcionada por el cliente en forma confidencial, además deberá usar los medios tecnológicos disponibles para brindar seguridad y confidencialidad a la información proporcionada.

[13] Autenticidad.- Es simplemente "verificar" la identidad.
[14] Integridad.- Se asegura que el contenido de los datos no haya sido modificado, y que la secuencia de los datos se mantenga durante la transmisión.
[15] Confiabilidad.- La privacia o la confidencialidad es la capacidad de asegurar que sólo las personas autorizadas tienen acceso a algo.

Finalmente, el proveedor debe informar al consumidor acerca del lugar y procedimiento sobre cómo presentar sus reclamaciones, y el proveedor debe evitar las prácticas comerciales engañosas.

Básicamente el contenido de las reformas del 29 de mayo de 2000 (ver anexo III) pueden resumirse en un reconocimiento de los medios electrónicos (y de otras tecnologías) para la celebración válida de actos jurídicos (contratos). Dicho reconocimiento implica la viabilidad de expresar la voluntad de una persona (consentimiento) por estos medios y con ello la posibilidad de celebrar, "en línea", contratos válidos y exigibles.

El modificar la letra de la ley es un hecho que, por sí sólo, no cambia nada. Es necesario un cambio cultural para que lo plasmado en las reformas llegue a ser útil. Se requiere que las empresas nacionales tomen conciencia de que hacer negocios en línea puede ser más barato, más efectivo y más seguro y que comiencen – como lo están haciendo ya en el resto del mundo – a aprovechar las posibilidades que ofrece la tecnología.

Los bancos son un excelente ejemplo del aprovechamiento de cómo es posible aprovechar las oportunidades que otorga la tecnología. Hay que ver lo que están haciendo los bancos como Banorte y Banamex (sólo por mencionar algunos) para darnos cuenta que sí es posible hacer las cosas de siempre de forma innovadora.

Las oportunidades son infinitas. Sin embargo, es necesario tomar las precauciones necesarias para contar, en caso de incumplimiento, con un contrato que pueda incluso ser presentado ante un juez.

Las reformas expresan cuándo y cómo se considera que un "mensaje de datos" (es decir, toda comunicación por medios electrónicos) es equivalente a un documento escrito. Asimismo, las reformas y las normas que en su momento las complementarán, nos definen lo que se requiere para confiar en un mensaje de datos y para saber que el mismo no ha sido alterado antes, durante o después de su transmisión. Sólo en la medida en que se pueda tener la certeza de que un mensaje efectivamente fue emitido por quien lo firma, se podrá confiar en él.

2.2.4 ANÁLISIS DE LA PROBLEMÁTICA REFERENTE A LA PROPIEDAD INDUSTRIAL Y LA LEY DE DERECHOS DE AUTOR.

La Ley de la Propiedad Industrial en su Título Segundo, del Capítulo Primero, Artículo 12, Fracción I, define lo que se debe de entender como nuevo: todo aquello que no se encuentre en estado de la técnica, es decir en uso; a su vez define el estado de la técnica como al conjunto de conocimientos que se han hecho públicos mediante una descripción oral o escrita, por la explotación o por cualquier otro medio de difusión o información, en el país o en el extranjero.

La actividad inventiva se considera de acuerdo a esta Ley, como el proceso creativo cuyos resultados no se deduzcan del estado de la técnica en forma evidente para un técnico en la materia.

Además agrega esta Ley en su artículo 15, que se considera invención, toda creación humana que permita transformar la materia o la energía que existe en la naturaleza para su aprovechamiento por el hombre y satisfacer sus necesidades concretas; quedan entendidos entre las invenciones los procesos o productos de aplicación industrial.

Esta Ley es tajante al considerar al software informático en su artículo 19, fracción IV, que los programas de computación **NO son invenciones**, revisemos si la Ley es acertada, ¿pero, que se entiende por programa de cómputo?

"Es la expresión de un conjunto organizado de instrucciones en lenguaje natural o codificado contenido dentro de un soporte físico de cualquier naturaleza, de empleo necesario en máquinas automáticas de tratamiento de la información, dispositivos, instrumentos o equipos periféricos basados en técnica digital, para hacerlos funcionar de modo y para fines determinados".

"Programas de cómputo es el conjunto de procedimientos o reglas que integran el soporte lógico de las máquinas que permiten la consecución del proceso de tratamiento de la información clasificando el programa de cómputo en:

a).- Por la fuente

b).- Por el objeto

a).- Los programas fuente conocidos también como sistemas operativos o de explotación, están ligados al funcionamiento mismo de la máquina, guardando una estrecha relación con las memorias centrales y auxiliares del computador a través de dispositivos como los compiladores, traductores, intérpretes, editores, etcétera, que permiten el adecuado enlace entre la máquina y los trabajos del usuario.

b).- Los programas objeto, son aquellos que se realizan para satisfacer las necesidades más variadas de los usuarios".

Agregando otra clasificación. Esta debe basarse en cuanto a la finalidad del programa:

a).- Programas de cómputo para la recreación, y

b).- Programas de cómputo para la industria.

a).- Si al utilizar el programa en la computadora se visualiza en la pantalla su contenido y mediante este se satisface una necesidad del hombre, se dice que estamos en presencia de un programa de cómputo que no transforma la energía.

b).- Pero si al usar el programa, satisface los objetivos para los que fue diseñado, porque su contenido este compuesto de algoritmos que son el medio para transformar la energía conectándose al equipo necesario, entonces estaremos en presencia de un programa que transforma la energía.

Como ejemplos de la clasificación anterior, podemos mencionar la elaboración de un programa para juegos donde claramente se ve que no cumple los requisitos de invención que marca el artículo 16 de la Ley de Propiedad Industrial ya que solamente servirá para el lucro y/o diversión;

El otro tipo de programas son aquellos cuya aplicación en sistemas de procesos industriales transforman mediante el equipo necesario la materia o la energía, como puede ser el caso de una central hidroeléctrica donde el agua almacenada en la presa pasa a través de unas tuberías las cuales apuntan el chorro de agua hacia las turbinas a través de unas compuertas que moverán los generadores que producirán electricidad. Dichas compuertas, turbinas, generadores, serán manejados por equipo que requieran programas de computación para que éstos puedan funcionar.

Como se ve en el ejemplo anterior, el programa de computación sirve para el funcionamiento del equipo y dicho equipo para llevar a cabo el proceso de transformar la materia que existe en la naturaleza para el aprovechamiento del hombre a través de la satisfacción inmediata de una necesidad concreta.

Por lo tanto, los programas de cómputo no se podrán clasificar como invenciones o programas industriales hasta que con el equipo necesario se transforme la energía de acuerdo al criterio de invención.

De acuerdo a la conclusión anterior, o bien se tendrá el equipo necesario para corroborar que tipo de programas son, o de otra forma, con simuladores hechos a base de software y hardware que posibiliten saber si son programas para la industria, estos simuladores estarán constituidos por programas y/o equipo a escala que nos permitan determinar la utilidad que se le dará al programa.

De lo anterior se deduce que, algunos programas de computación deberán ser considerados como invenciones por el razonamiento antes mencionado, y otros programas servirán sólo para la recreación del espíritu.

Esta distinción debe ser tomada en cuenta por el legislador y evitar el que se regule sólo los programas de cómputo en la Ley de Derechos de Autor.

Debe existir, si no, una legislación especial para los bienes y servicios informáticos, si un apartado especial que abarque tanto los programas de cómputo destinados a la industria, como los que sirvan sólo a la recreación del espíritu. Pudiera ser dentro de la misma Ley de la Propiedad Industrial, porque es la que más incentivos ofrece al creador de una obra intelectual.

2.2.5 ANEXO III

Diario Oficial de la Federación, 29 de mayo de 2000
SECRETARIA DE COMERCIO Y FOMENTO INDUSTRIAL
DECRETO por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor.
Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Presidencia de la República.
ERNESTO ZEDILLO PONCE DE LEON, Presidente de los Estados Unidos Mexicanos, a sus habitantes sabed Que el Honorable Congreso de la Unión, se ha servido dirigirme el siguiente **DECRETO**
"EL CONGRESO DE LOS ESTADOS UNIDOS MEXICANOS, D E C R E T A:
REFORMAN Y ADICIONAN DIVERSAS DISPOSICIONES DEL CODIGO CIVIL PARA EL DISTRITO FEDERAL EN MATERIA COMUN Y PARA TODA LA REPUBLICA EN MATERIA FEDERAL, DEL CODIGO FEDERAL DE PROCEDIMIENTOS CIVILES, DEL CODIGO DE COMERCIO Y DE LA LEY FEDERAL DE PROTECCION AL CONSUMIDOR.
ARTICULO PRIMERO.- Se modifica la denominación del **Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal**, y con ello se reforman sus artículos 1o., 1803, 1805 y 1811, y se le adiciona el artículo 1834 bis, para quedar como sigue:
"CODIGO CIVIL FEDERAL
Artículo 1o.- Las disposiciones de este Código regirán en toda la República en asuntos del orden federal.
Artículo 1803.- El consentimiento puede ser expreso o tácito, para ello se estará a lo siguiente:
I.- Será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, y
II.- El tácito resultará de hechos o de actos que lo presupongan o que autoricen a presumirlo, excepto en los casos en que por ley o por convenio la voluntad deba manifestarse expresamente.
Artículo 1805.- Cuando la oferta se haga a una persona presente, sin fijación de plazo para aceptarla, el autor de la oferta queda desligado si la aceptación no se hace inmediatamente. La misma regla se aplicará a la oferta hecha por teléfono o a través de cualquier otro medio electrónico, óptico o de cualquier otra tecnología que permita la expresión de la oferta y la aceptación de ésta en forma inmediata.
Artículo 1811.- ...
Tratándose de la propuesta y aceptación hechas a través de medios electrónicos, ópticos o de cualquier otra tecnología no se requerirá de estipulación previa entre los contratantes para que produzca efectos.
Artículo 1834 bis.- Los supuestos previstos por el artículo anterior se tendrán por cumplidos mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, siempre que la información generada o comunicada en forma íntegra, a través de dichos medios sea atribuible a las personas obligadas y accesible para su ulterior consulta.
En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán generar, enviar, recibir, archivar o comunicar la información que contenga los términos exactos en que las partes han decidido obligarse, mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, en cuyo caso el fedatario público, deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuye dicha información a las partes y conservar bajo su resguardo una versión íntegra de la misma para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige."
ARTICULO SEGUNDO.- Se adiciona el artículo 210-A al **Código Federal de Procedimientos Civiles**, en los términos siguientes:
"Artículo 210-A.- Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.
Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.
Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta."
ARTICULO TERCERO.- Se reforman los artículos 18, 20, 21 párrafo primero, 22, 23, 24, 25, 26, 27, 30, 31, 32, 49, 80 y 1205, y se adicionan los artículos 20 bis, 21 bis, 21 bis 1, 30 bis, 30 bis 1 y 32 bis 1298-A; el Título II que se denominará "Del Comercio Electrónico", que comprenderá los artículos 89 a 94, y se modifica la

denominación del Libro Segundo del Código de Comercio, disposiciones todas del referido **Código de Comercio**, para quedar como sigue:

"Artículo 18.- En el Registro Público de Comercio se inscriben los actos mercantiles, así como aquellos que se relacionan con los comerciantes y que conforme a la legislación lo requieran.

La operación del Registro Público de Comercio está a cargo de la Secretaría de Comercio y Fomento Industrial, en adelante la Secretaría, y de las autoridades responsables del registro público de la propiedad en los estados y en el Distrito Federal, en términos de este Código y de los convenios de coordinación que se suscriban conforme a lo dispuesto por el artículo 116 de la Constitución Política de los Estados Unidos Mexicanos. Para estos efectos existirán las oficinas del Registro Público de Comercio en cada entidad federativa que demande el tráfico mercantil.

La Secretaría emitirá los lineamientos necesarios para la adecuada operación del Registro Público de Comercio, que deberán publicarse en el **Diario Oficial de la Federación**.

Artículo 20.- El Registro Público de Comercio operará con un programa informático y con una base de datos central interconectada con las bases de datos de sus oficinas ubicadas en las entidades federativas.

Las bases de datos contarán con al menos un respaldo electrónico.

Mediante el programa informático se realizará la captura, almacenamiento, custodia, seguridad, consulta, reproducción, verificación, administración y transmisión de la información registral .

Las bases de datos del Registro Público de Comercio en las entidades federativas se integrarán con el conjunto de la información incorporada por medio del programa informático de cada inscripción o anotación de los actos mercantiles inscribibles, y la base de datos central con la información que los responsables del Registro incorporen en las bases de datos ubicadas en las entidades federativas.

El programa informático será establecido por la Secretaría. Dicho programa y las bases de datos del Registro Público de Comercio, serán propiedad del Gobierno Federal.

En caso de existir discrepancia o presunción de alteración de la información del Registro Público de Comercio contenida en la base de datos de alguna entidad federativa, o sobre cualquier otro respaldo que hubiere, prevalecerá la información registrada en la base de datos central, salvo prueba en contrario.

La Secretaría establecerá los formatos, que serán de libre reproducción, así como los datos, requisitos y demás información necesaria para llevar a cabo las inscripciones, anotaciones y avisos a que se refiere el presente Capítulo. Lo anterior deberá publicarse en el **Diario Oficial de la Federación**.

Artículo 20 bis.- Los responsables de las oficinas del Registro Público de Comercio tendrán las atribuciones siguientes:

I.- Aplicar las disposiciones del presente Capítulo en el ámbito de la entidad federativa correspondiente;

II.- Ser depositario de la fe pública registral mercantil, para cuyo ejercicio se auxiliará de los registradores de la oficina a su cargo;

III.- Dirigir y coordinar las funciones y actividades de las unidades administrativas a su cargo para que cumplan con lo previsto en este Código, el reglamento respectivo y los lineamientos que emita la Secretaría;

IV.- Permitir la consulta de los asientos registrales que obren en el Registro, así como expedir las certificaciones que le soliciten;

V.- Operar el programa informático del sistema registral automatizado en la oficina a su cargo, conforme a lo previsto en este Capítulo, el reglamento respectivo y en los lineamientos que emita la Secretaría;

VI.- Proporcionar facilidades a la Secretaría para vigilar la adecuada operación del Registro Público de Comercio, y

VII.- Las demás que se señalen en el presente Capítulo y su reglamento.

Artículo 21.- Existirá un folio electrónico por cada comerciante o sociedad, en el que se anotarán: I a XIX.- . . .

Artículo 21 bis.- El procedimiento para la inscripción de actos mercantiles en el Registro Público de Comercio se sujetará a las bases siguientes:

I.- Será automatizado y estará sujeto a plazos máximos de respuesta;

II.- Constará de las fases de:

a) Recepción, física o electrónica de una forma precodificada, acompañada del instrumento en el que conste el acto a inscribir, pago de los derechos, generación de una boleta de ingreso y del número de control progresivo e invariable para cada acto;

b) Análisis de la forma precodificada y la verificación de la existencia o inexistencia de antecedentes registrales y, en su caso, preinscripción de dicha información a la base de datos ubicada en la entidad federativa;

c) Calificación, en la que se autorizará en definitiva la inscripción en la base de datos mediante la firma electrónica del servidor público competente, con lo cual se generará o adicionará el folio mercantil electrónico correspondiente, y

d) Emisión de una boleta de inscripción que será entregada física o electrónicamente. El reglamento del presente Capítulo desarrollará el procedimiento registral de acuerdo con las bases anteriores.

Artículo 21 bis 1.- La prelación entre derechos sobre dos o más actos que se refieran a un mismo folio mercantil electrónico, se determinará por el número de control que otorgue el registro, cualquiera que sea la fecha de su constitución o celebración.

Artículo 22.- Cuando, conforme a la ley, algún acto o contrato deba inscribirse en el Registro Público de la Propiedad o en registros especiales, su inscripción en dichos registros será bastante para que surtan los efectos correspondientes del derecho mercantil, siempre y cuando en el Registro Público de Comercio se tome razón de dicha inscripción y de las modificaciones a la misma.
Artículo 23.- Las inscripciones deberán hacerse en la oficina del Registro Público de Comercio del domicilio del comerciante, pero si se trata de bienes raíces o derechos reales constituidos sobre ellos, la inscripción se hará, además, en la oficina correspondiente a la ubicación de los bienes, salvo disposición legal que establezca otro procedimiento.
Artículo 24.- Las sociedades extranjeras deberán acreditar, para su inscripción en el Registro Público de Comercio, estar constituidas conforme a las leyes de su país de origen y autorizadas para ejercer el comercio por la Secretaría, sin perjuicio de lo establecido en los tratados o convenios internacionales.
Artículo 25.- Los actos que conforme a este Código u otras leyes deban inscribirse en el Registro Público de Comercio deberán constar en:
I.- Instrumentos públicos otorgados ante notario o corredor público;
II.- Resoluciones y providencias judiciales o administrativas certificadas;
III.- Documentos privados ratificados ante notario o corredor público, o autoridad judicial competente, según corresponda, o
IV.- Los demás documentos que de conformidad con otras leyes así lo prevean.
Artículo 26.- Los documentos de procedencia extranjera que se refieran a actos inscribibles podrán constar previamente en instrumento público otorgado ante notario o corredor público, para su inscripción en el Registro Público de Comercio.
Las sentencias dictadas en el extranjero sólo se registrarán cuando medie orden de autoridad judicial mexicana competente, y de conformidad con las disposiciones internacionales aplicables.
Artículo 27.- La falta de registro de los actos cuya inscripción sea obligatoria, hará que éstos sólo produzcan efectos jurídicos entre los que lo celebren, y no podrán producir perjuicio a tercero, el cual sí podrá aprovecharse de ellos en lo que le fueren favorables.
Artículo 30.- Los particulares podrán consultar las bases de datos y, en su caso, solicitar las certificaciones respectivas, previo pago de los derechos correspondientes.
Las certificaciones se expedirán previa solicitud por escrito que deberá contener los datos que sean necesarios para la localización de los asientos sobre los que deba versar la certificación y, en su caso, la mención del folio mercantil electrónico correspondiente.
Cuando la solicitud respectiva haga referencia a actos aún no inscritos, pero ingresados a la oficina del Registro Público de Comercio, las certificaciones se referirán a los asientos de presentación y trámite.
Artículo 30 bis.- La Secretaría podrá autorizar el acceso a la base de datos del Registro Público de Comercio a personas que así lo soliciten y cumplan con los requisitos para ello, en los términos de este Capítulo, el reglamento respectivo y los lineamientos que emita la Secretaría, sin que dicha autorización implique en ningún caso inscribir o modificar los asientos registrales.
La Secretaría certificará los medios de identificación que utilicen las personas autorizadas para firmar electrónicamente la información relacionada con el Registro Público de Comercio, así como la de los demás usuarios del mismo, y ejercerá el control de estos medios a fin de salvaguardar la confidencialidad de la información que se remita por esta vía.
Artículo 30 bis 1.- Cuando la autorización a que se refiere el artículo anterior se otorgue a notarios o corredores públicos, dicha autorización permitirá, además, el envío de información por medios electrónicos al Registro y la remisión que éste efectúe al fedatario público correspondiente del acuse que contenga el número de control a que se refiere el artículo 21 bis 1 de este Código.
Los notarios y corredores públicos que soliciten dicha autorización deberán otorgar una fianza a favor de la Tesorería de la Federación y registrarla ante la Secretaría, para garantizar los daños que pudieran ocasionar a los particulares en la operación del programa informático, por un monto mínimo equivalente a 10 000 veces el salario mínimo diario vigente en el Distrito Federal.
En caso de que los notarios o corredores públicos estén obligados por la ley de la materia a garantizar el ejercicio de sus funciones, sólo otorgarán la fianza a que se refiere el párrafo anterior por un monto equivalente a la diferencia entre ésta y la otorgada.
Dicha autorización y su cancelación deberán publicarse en el **Diario Oficial de la Federación.**
Artículo 31.- Los registradores no podrán denegar la inscripción de los documentos mercantiles que se les presenten, salvo cuando:
I. El acto o contrato que en ellos se contenga no sea de los que deben inscribirse;
II. Esté en manifiesta contradicción con los contenidos de los asientos registrales preexistentes, o
III. El documento de que se trate no exprese, o exprese sin claridad suficiente, los datos que deba contener la inscripción.
Si la autoridad administrativa o judicial ordena que se registre un instrumento rechazado, la inscripción surtirá sus efectos desde que por primera vez se presentó.

El registrador suspenderá la inscripción de los actos a inscribir, siempre que existan defectos u omisiones que sean subsanables. En todo caso se requerirá al interesado para que en el plazo que determine el reglamento de este Capítulo las subsane, en el entendido de que, de no hacerlo, se le denegará la inscripción.
Artículo 32.- La rectificación de los asientos en la base de datos por causa de error material o de concepto, sólo procede cuando exista discrepancia entre el instrumento donde conste el acto y la inscripción. Se entenderá que se comete error material cuando se escriban unas palabras por otras, se omita la expresión de alguna circunstancia o se equivoquen los nombres propios o las cantidades al copiarlas del instrumento donde conste el acto, sin cambiar por eso el sentido general de la inscripción ni el de alguno de sus conceptos.
Se entenderá que se comete error de concepto cuando al expresar en la inscripción alguno de los contenidos del instrumento, se altere o varíe su sentido porque el responsable de la inscripción se hubiere formado un juicio equivocado del mismo, por una errónea calificación del contrato o acto en él consignado o por cualquiera otra circunstancia similar.
Artículo 32 bis.- Cuando se trate de errores de concepto, los asientos practicados en los folios del Registro Público de Comercio sólo podrán rectificarse con el consentimiento de todos los interesados en el asiento. A falta del consentimiento unánime de los interesados, la rectificación sólo podrá efectuarse por resolución judicial. El concepto rectificado surtirá efectos desde la fecha de su rectificación. El procedimiento para efectuar la rectificación en la base de datos lo determinará la Secretaría en los lineamientos que al efecto emitan.
Artículo 49.- Los comerciantes están obligados a conservar por un plazo mínimo de diez años los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones.
Para efectos de la conservación o presentación de originales, en el caso de mensajes de datos, se requerirá que la información se haya mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta. La Secretaría de Comercio y Fomento Industrial emitirá la Norma Oficial Mexicana que establezca los requisitos que deberán observarse para la conservación de mensajes de datos.

LIBRO SEGUNDO
DEL COMERCIO EN GENERAL

...

Artículo 80.- Los convenios y contratos mercantiles que se celebren por correspondencia, telégrafo, o mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, quedarán perfeccionados desde que se reciba la aceptación de la propuesta o las condiciones con que ésta fuere modificada.

TITULO II
DEL COMERCIO ELECTRONICO

Artículo 89.- En los actos de comercio podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efecto del presente Código, a la información generada, enviada, recibida, archivada o comunicada a través de dichos medios se le denominará mensaje de datos.
Artículo 90.- Salvo pacto en contrario, se presumirá que el mensaje de datos proviene del emisor si ha sido enviado:
I.- Usando medios de identificación, tales como claves o contraseñas de él, o
II.- Por un sistema de información programado por el emisor o en su nombre para que opere automáticamente.
Artículo 91.- El momento de recepción de la información a que se refiere el artículo anterior se determinará como sigue:
I.- Si el destinatario ha designado un sistema de información para la recepción, ésta tendrá lugar en el momento en que ingrese en dicho sistema, o
II.- De enviarse a un sistema del destinatario que no sea el designado o de no haber un sistema de información designado, en el momento en que el destinatario obtenga dicha información. Para efecto de este Código, se entiende por sistema de información cualquier medio tecnológico utilizado para operar mensajes de datos.
Artículo 92.- Tratándose de la comunicación de mensajes de datos que requieran de un acuse de recibo para surtir efectos, bien sea por disposición legal o por así requerirlo el emisor, se considerará que el mensaje de datos ha sido enviado, cuando se haya recibido el acuse respectivo. Salvo prueba en contrario, se presumirá que se ha recibido el mensaje de datos cuando el emisor reciba el acuse correspondiente.
Artículo 93.- Cuando la ley exija la forma escrita para los contratos y la firma de los documentos relativos, esos supuestos se tendrán por cumplidos tratándose de mensaje de datos siempre que éste sea atribuible a las personas obligadas y accesible para su ulterior consulta.
En los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán, a través de mensajes de datos, expresar los términos exactos en que las partes han decidido obligarse, en cuyo caso el fedatario público, deberá hacer constar en el propio instrumento los elementos a través de los cuales se atribuyen dichos mensajes a las partes y conservar bajo su resguardo una versión íntegra de los mismos para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige.

Artículo 94.- Salvo pacto en contrario, el mensaje de datos se tendrá por expedido en el lugar donde el emisor tenga su domicilio y por recibido en el lugar donde el destinatario tenga el suyo.
Artículo 1205.- Son admisibles como medios de prueba todos aquellos elementos que puedan producir convicción en el ánimo del juzgador acerca de los hechos controvertidos o dudosos y en consecuencia serán tomadas como pruebas las declaraciones de las partes, terceros, peritos, documentos públicos o privados, inspección judicial, fotografías, facsímiles, cintas cinematográficas, de videos, de sonido, mensajes de datos, reconstrucciones de hechos y en general cualquier otra similar u objeto que sirva para averiguar la verdad.
Artículo 1298-A.- Se reconoce como prueba los mensajes de datos. Para valorar la fuerza probatoria de dichos mensajes, se estimará primordialmente la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada."
ARTICULO CUARTO.- Se reforma el párrafo primero del artículo 128, y se adiciona la fracción VIII al artículo 1o., la fracción IX bis al artículo 24 y el Capítulo VIII bis a la **Ley Federal de Protección al Consumidor**, que contendrá el artículo 76 bis, para quedar como sigue:
"Artículo 1o.-.....
I a VII.- ...
VIII.- La efectiva protección al consumidor en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología y la adecuada utilización de los datos aportados.
Artículo 24.- ...
I a IX.- ...
IX bis.- Promover en coordinación con la Secretaría la formulación, difusión y uso de códigos de ética, por parte de proveedores, que incorporen los principios previstos por esta Ley respecto de las transacciones que celebren con consumidores a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología;
X a XXI.- ...
CAPITULO VIII BIS DE LOS DERECHOS DE LOS CONSUMIDORES EN LAS TRANSACCIONES EFECTUADAS A TRAVES DEL USO DE MEDIOS ELECTRONICOS, OPTICOS O DE CUALQUIER OTRA TECNOLOGIA
Artículo 76 bis.- Las disposiciones del presente Capítulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente:
I. El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente;
II. El proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos;
III. El proveedor deberá proporcionar al consumidor, antes de celebrar la transacción, su domicilio físico, números telefónicos y demás medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones;
IV. El proveedor evitará las prácticas comerciales engañosas respecto de las características de los productos, por lo que deberá cumplir con las disposiciones relativas a la información y publicidad de los bienes y servicios que ofrezca, señaladas en esta Ley y demás disposiciones que se deriven de ella;
V. El consumidor tendrá derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, en su caso, formas de pago de los bienes y servicios ofrecidos por el proveedor;
VI. El proveedor respetará la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como la de no recibir avisos comerciales, y
VII. El proveedor deberá abstenerse de utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos, y cuidará las prácticas de mercadotecnia dirigidas a población vulnerable, como niños, ancianos y enfermos, incorporando mecanismos que adviertan cuando la información no sea apta para esa población.
Artículo 128.- Las infracciones a lo dispuesto por los artículos 8, 10, 12, 60, 63, 65, 74, 76 bis, 80 y 121 serán sancionadas con multa por el equivalente de una y hasta dos mil quinientas veces el salario mínimo general vigente para el Distrito Federal.
..."
TRANSITORIOS

Primero.- El presente Decreto entrará en vigor a los nueve días siguientes de su publicación en el **Diario Oficial de la Federación**.
Segundo.- Las menciones que en otras disposiciones de carácter federal se hagan al Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, se entenderán referidas al Código Civil Federal.

Las presentes reformas no implican modificación alguna a las disposiciones legales aplicables en materia civil para el Distrito Federal, por lo que siguen vigentes para el ámbito local de dicha entidad todas y cada una de las disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, vigentes a la entrada en vigor del presente Decreto.

Tercero.- La operación automatizada del Registro Público de Comercio conforme a lo dispuesto en el presente Decreto deberá iniciarse a más tardar el 30 de noviembre del año 2000.

Para tal efecto, la Secretaría de Comercio y Fomento Industrial proporcionará a cada uno de los responsables de las oficinas del Registro Público de Comercio, a partir de la entrada en vigor del presente Decreto y a más tardar el 31 de agosto del año 2000, el programa informático del sistema registral automatizado a que se refiere el presente Decreto, la asistencia y capacitación técnica, así como las estrategias para su instrumentación, de conformidad con los convenios correspondientes.

Cuarto.- En tanto se expide el Reglamento correspondiente, seguirán aplicándose los capítulos I a IV y VII del Título II del Reglamento del Registro Público de Comercio, publicado en el **Diario Oficial de la Federación** el 22 de enero de 1979, en lo que no se opongan a lo dispuesto en el presente Decreto.

Quinto.- La captura del acervo histórico del Registro Público de Comercio deberá concluirse, en términos de los convenios de coordinación previstos en el artículo 18 del Código de Comercio a que se refiere el presente Decreto, a más tardar el 30 de noviembre del 2002.

Sexto.- La Secretaría, en coordinación con los gobiernos estatales, determinará los procedimientos de recepción de los registros de los actos mercantiles que hasta la fecha de entrada en vigor del presente Decreto efectuaban los oficios de hipotecas y los jueces de primera instancia del orden común, así como los mecanismos de integración a las bases de datos central y a las ubicadas en las entidades federativas. Dicha recepción deberá efectuarse en un plazo máximo de ciento ochenta días contados a partir de la entrada en vigor del presente Decreto.

Séptimo.- Las solicitudes de inscripción de actos mercantiles en el Registro Público de Comercio y los medios de defensa iniciados con anterioridad a la entrada en vigor del presente Decreto, se substanciarán y resolverán, hasta su total conclusión, conforme a las disposiciones que les fueron aplicables al momento de iniciarse o interponerse.

Octavo.- La Secretaría deberá publicar en el **Diario Oficial de la Federación** los lineamientos y formatos a que se refieren los artículos 18 y 20, que se reforman por virtud del presente Decreto, en un plazo máximo de noventa días, contados a partir de la fecha de su entrada en vigor.

México, D.F., a 29 de abril de 2000.- Dip. **Francisco José Paoli Bolio**, Presidente.- Sen. **Dionisio Pérez Jácome**, Vicepresidente en funciones.- Dip. **Marta Laura Carranza Aguayo**, Secretario.- Sen. **Raúl Juárez Valencia**, Secretario.- Rúbricas".

En cumplimiento de lo dispuesto por la fracción I del Artículo 89 de la Constitución Política de los Estados Unidos Mexicanos, y para su debida publicación y observancia, expido el presente Decreto en la residencia del Poder Ejecutivo Federal, en la Ciudad de México, Distrito Federal, a los veintitrés días del mes de mayo de dos mil.- **Ernesto Zedillo Ponce de León**.- Rúbrica.- El Secretario de Gobernación, **Diódoro Carrasco Altamirano**.- Rúbrica.

BIBLIOGRAFÍA

Diario Oficial de la Federación 29/05/2000
http/200.15.45.216.dofdia/otros/pdfs/mayoy2k/290500cpd

Reformas Al Código de Comercio 29/05/2000
http://mx.google.yahoo.com/bin/query_mx?p=reformas+al+comercio+electronico+mexico&hc=0&hs=0

CAPÍTULO III

SEGURIDAD DE LA INFORMACIÓN

3.- SEGURIDAD DE LA INFORMACIÓN

3.1 Introducción

La importancia de la informática en la sociedad actual, ha provocado la Segunda Revolución Industrial, debido a que su impacto ha sido mayor que el de cualquier otro invento de la segunda mitad del siglo XX, lo cual se ha manifestado, y hemos podido experimentar en toda su magnitud, a través del desarrollo en diversas disciplinas.

El intercambio electrónico de información es una forma de trabajo que habilita a una organización a operar en forma más dinámica. Todas las organizaciones funcionan con base en datos recibidos del entorno en que se desenvuelven. Los datos relacionados se convierten en información para la toma de decisiones. La rapidez con la que se puede recibir información del entorno, y la agilidad con la que se transmiten las decisiones son cada vez más determinantes para el éxito de las organizaciones en el mundo moderno.

Hasta hace poco cada forma de comunicación (voz, datos, video) requería su propia infraestructura. Los adelantos en comunicaciones y computación hacen posible que las diversas formas de comunicarnos no sólo compartan la misma infraestructura sino que puedan llevarse a cabo en forma más rápida y más económica. Tanto con personas dentro de nuestras organizaciones como con personas fuera de ella.

Por lo que debido a la difusión de las tecnologías de la información, la mayoría de las organizaciones actuales están expuestas a una serie de riesgos derivados de una protección inadecuada o inapropiada de la información, lo que las hace vulnerables[16] a muy diversos tipos de ataques desde amenazas físicas, como cortes eléctricos, hasta errores no intencionados de los usuarios, pasando por los virus informáticos o el robo, destrucción o modificación de la información, por lo que se plantean retos importantes a la seguridad de la información.

3.2 Seguridad En Los Sistemas De Información

La ***Seguridad de la Información*** se refiere a la protección de sistemas de información contra los accesos no autorizados o la modificación de información, si se encuentra en una fase de almacenamiento, procesamiento o tránsito. También protege la negación de servicios a usuarios no autorizados incluyendo las medidas necesarias para detectar, documentar, y contrarrestar tales amenazas.

[16] Vulnerable.- Es una debilidad que puede ser explotada para violar la seguridad.

La seguridad en la comunicación a través de redes, consiste en prevenir, impedir, detectar y corregir violaciones a la seguridad durante la transmisión de información.

La seguridad de la información considera tres aspectos:

1. Amenazas
2. Servicios de Seguridad
3. Mecanismos de Seguridad

3.2.1 Amenazas

Se entiende por amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). La política de seguridad y el análisis de riesgos habrán identificado los ataques que han de ser contrarrestados, dependiendo del diseñador del sistema de seguridad especificando los servicios y mecanismos de seguridad necesarios.

Los problemas técnicos, las amenazas ambientales, las condiciones de instalación desfavorables, los usuarios, la situación política y social, son factores susceptibles de poner en peligro el buen funcionamiento de los sistemas de información.

Las amenazas a los sistemas de información van desde:

Desastres naturales o físicos tales como inundaciones, accidentes o incendios, terremotos, rayos, condiciones ambientales como la temperatura, humedad, presencia de polvo.

Amenazas involuntarias como borrar sin querer la información, dejar sin protección determinados archivos, dejar un post-it con nuestro password.

Amenazas intencionales como fraudes, robos, virus, con un origen tanto interno como los empleados despedidos o descontentos, empleados que obtienen beneficios personales así como empleados en acuerdo con personas externas.

Un ataque no es más que la realización de una amenaza.

Las cuatro categorías generales de amenazas o ataques son las siguientes:

Interrupción: Un recurso del sistema es destruido o se vuelve no disponible. Interrumpir mediante algún método el funcionamiento del sistema. Este es un ataque

contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación, saturar la memoria. (Fig. 3.1).

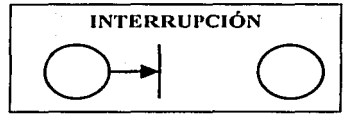

Figura 3.1 Interrupción.

Intercepción: Una entidad[17] no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplo de este ataque son la copia ilícita de archivos o programas (intercepción de datos). Son los más difíciles de detectar pues en la mayoría de los casos no alteran la información del sistema.(Fig. 3.2).

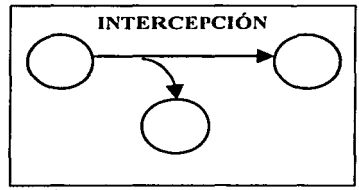

Figura 3.2 Interceptación.

Modificación: Una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambiar el contenido de una base de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red, cambiar datos en una cuenta bancaria.(Fig.3.3).

[17] Entidad.- Ente o realidad, especialmente cuando no es material. Aquello que es, existe o puede existir. Colectividad, corporación.

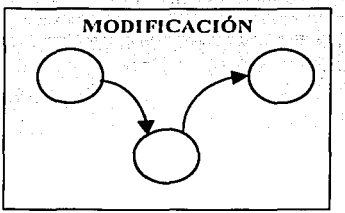

Figura 3.3 Modificación.

Suplantación: Una entidad no autorizada inserta objetos falsificados en el sistema. Se refiere a la posibilidad de añadir información o programas no autorizados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes ilegítimos en una red o añadir registros a un archivo, introducir mensajes no autorizados en una línea de datos.

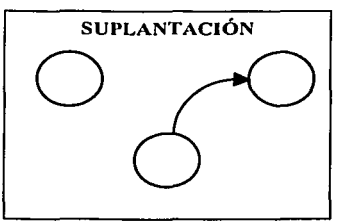

Figura 3.1 Suplantación.

Estos ataques se pueden asimismo clasificar en ataques pasivos y ataques activos.

Ataques pasivos

En los ataques pasivos el atacante no altera la información, sino que únicamente la escucha, observa, copia o monitorea, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

Algunas técnicas empleadas para la misión de los ataques pasivo son:

Fisgoneo.- Mirar a un usuario lo que está escribiendo con el teclado, escuchar una platica, así como escuchar o analizar de una manera sofisticada la que se transmite en una ruta de comunicación.

Residuo.- Se refiere al desecho de discos, segmentos de memoria, que son reutilizados por otros usuarios sin que se borre la información anterior, papel reciclado.

Hojeo.- El hojeo se refiere a la búsqueda ociosa a través del almacenaje(información disponible) sin saber exactamente que información se busca o si existe.

Ataques activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

Suplantación de identidad: El intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

Reproducción: Uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, por ejemplo ingresar dinero repetidas veces en una cuenta bancaria.

Modificación de mensajes: Una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Ingresa un millón de pesos en la cuenta A" podría ser modificado para decir "Ingresa un millón de pesos en la cuenta B".

Degradación fraudulenta del servicio: impide o inhibe el uso normal de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes ilegítimos. Entre estos ataques se encuentra la interrupción de servicio, consistente en paralizar temporalmente el servicio de un servidor de correo.

La misión en los ataques activos son:

Los mensajes puedes ser alterados, borrados o insertados. Las personas que contengan información secreta, pueden destruir datos valiosos, alterar la autorización

de los sistema, afectando la integridad de la información o disponibilidad de los servicios.

3.2.2 Servicios De Seguridad

Para hacer frente a las amenazas, la seguridad de la información cuenta con una serie de servicios para proteger los sistemas, procesos de datos y transferencia de información de una organización. Estos servicios hacen uso de uno o varios mecanismos de seguridad. Una clasificación útil de los servicios de seguridad es la siguiente:

CONFIDENCIALIDAD.- La privacidad o la confidencialidad es la capacidad de asegurar que sólo las personas autorizadas tienen acceso a algo, es mantener la información secreta para proteger los recursos y la información contra en descubrimiento intencional o accidental, es la protección de los datos transmitidos de cualquier ataque pasivo. El control de la seguridad depende de lo que se desea proteger, en que medida puede afectar su privacidad y qué tan peligroso puede ser en manos desconocidas.

AUTENTICACIÓN.- La autenticación es uno de los requerimientos más fáciles de comprender. Es simplemente: "verificación" de la identidad. Requiere una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa. Se distinguen dos tipos: *de entidad*, que asegura la identidad de los participantes en la comunicación, mediante biométrica (huellas dactilares, identificación de iris, etc.), tarjetas de banda magnética, contraseñas, o procedimientos similares; y *de origen de información*, que asegura que una unidad de información proviene de cierta entidad, siendo la firma digital el mecanismo más usado.

INTEGRIDAD.- Es el servicio de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado. Permite asegurar que no se ha falsificado la información, que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados. Este servicio de integridad se relaciona con los ataque activos, se refiere a la detección más que a la prevención.

NO-REPUDIO.- Permite asegurar que cualquier entidad que envía o recibe información, no puede alegar ante un tercero que no la envió o la recibió. Esta propiedad es especialmente importante en el entorno bancario y en el uso del comercio electrónico.

CONTROL DE ACCESO.- Se ejecuta con el fin de que un usuario sea identificado y autenticado para que le sea permitido el acceso. Los derechos de acceso permite tener privilegios a la entidad o los permisos a los recursos de la red. Ejemplos de privilegios o

permisos de una entidad: creación o destrucción, lectura o escritura, insertar, borrar o modificar el contenido, trasladar o copiar así como ejecutar información.

DISPONIBILIDAD.- Se cumple si las personas autorizadas pueden acceder a la información deseada cuando lo requieran y tantas veces cuando sea necesario. Es el grado en que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. Muchos ataques como los gusanos, no buscan borrar, robar o modificar la información, sino bloquear el sistema creando nuevos procesos que saturan los recursos.

3.2.3 Mecanismos De Seguridad

No existe un único mecanismo capaz de proveer todos los servicios anteriormente citados, pero la mayoría de ellos hacen uso de técnicas criptográficas basadas en el cifrado de la información. Los más importantes son los siguientes:

Intercambio de autenticación: corrobora que una entidad, ya sea origen o destino de la información, es la deseada, por ejemplo, A envía un número aleatorio cifrado con la clave pública de B, B lo descifra con su clave privada y se lo reenvía a A, demostrando así que es quien pretende ser. Por supuesto, hay que ser cuidadoso a la hora de diseñar estos protocolos, ya que existen ataques para desbaratarlos.

Cifrado: garantiza que la información no sea accesible para individuos, entidades o procesos no autorizados (confidencialidad). La protección de la información se puede llevar a cabo por medio de la criptografía. La criptografía es una rama de la criptología, es un campo que trata con las comunicaciones seguras. La otra rama de la criptología es el criptoanálisis, éste se refiere a la ruptura o derrota de la criptografía, es el proceso que intenta descubrir el texto o la clave. Por tanto la criptografía y el criptoanálisis siempre están unidos.

> **La criptografía**[18] es el arte y la ciencia de transformar la información para asegurar su secreto, su autenticidad o ambas y prevenir a los usuarios de acciones no autorizadas o ilegales en contra de la información.
>
> La criptografía está íntimamente relacionada con la seguridad por lo que es cada vez más importante debido a la gran información que las organizaciones actualmente generan, procesan, almacenan y/o distribuyen de manera segura (confidencial o íntegra). Éstas transportan información cada vez más valiosas y vitales para las más diversas organizaciones.

[18] Criptografía.- (Kryptós = escondido, oculto; graphé=grafía,escritura): Es el arte o la ciencia de escribir en cifra o en código, de tal forma que permita que sólo el destinatario lo descifre y comprenda.

La criptografía intenta garantizar: discreción, integridad de la información, autenticación de usuario, autenticación de remitente, autenticación del destinatario, autenticación de actualidad.

En la criptografía, los mensajes originales se conocen como ***texto en claro o texto fuente*** y a la operación con la cual los símbolos básicos se transportan o sustituyen para transformar los datos, se denomina ***puesta en cifra***. El resultado (mensaje cifrado) de la puesta en cifra se conoce como ***texto cifrado o criptograma***

Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que la criptografía es simétrica.

Estos sistemas son mucho más rápidos que los de clave pública, resultando apropiados para funciones de cifrado de grandes volúmenes de datos. Se pueden dividir en dos categorías: ***cifradores de bloque***, que cifran los datos en bloques de tamaño fijo (típicamente bloques de 64 bits), y ***cifradores en flujo***, que trabajan sobre flujos continuos de bits.

Cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que la criptografía es asimétrica o de clave pública. Una clave, la privada, se mantiene secreta, mientras que la segunda clave, la pública, puede ser conocida por todos. De forma general, las claves públicas se utilizan para cifrar y las privadas, para descifrar.

El sistema tiene la propiedad de que a partir del conocimiento de la clave pública no es posible determinar la clave privada. La criptografía de clave pública, aunque más lenta que la criptografía simétrica, resulta adecuada para las funciones de autenticación, distribución de claves y firmas digitales.

Integridad de datos: este mecanismo implica el cifrado de una cadena comprimida de datos a transmitir, llamada generalmente valor de comprobación de integridad (Integrity Check Value o ICV). Este mensaje se envía al receptor junto con los datos. El receptor repite la compresión y el cifrado posterior de los datos y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados.

Firma digital: este mecanismo implica el cifrado, por medio de la clave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía junto con los datos ordinarios. Este mensaje se procesa en el receptor, para verificar su integridad. Juega un papel esencial en el servicio de no repudio.

Control de acceso: esfuerzo para que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red, como por ejemplo mediante las contraseñas de acceso.

Tráfico de relleno: consiste en enviar tráfico ilegítimo junto con los datos válidos para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se están transmitiendo.

Control de encaminamiento: permite enviar determinada información por determinadas zonas consideradas clasificadas. Asimismo posibilita solicitar otras rutas, en caso que se detecten persistentes violaciones de integridad en una ruta determinada.

Unicidad: consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, que se incluyen en la firma digital o integridad de datos. De esta forma se evitan amenazas como la repetición de mensajes.

Los mecanismos básicos pueden agruparse de varias formas para proporcionar los servicios previamente mencionados. Conviene resaltar que los mecanismos poseen tres componentes principales:

Una información secreta, como claves y contraseñas, conocidas por las entidades autorizadas.

Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado, y generación de números aleatorios.

Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envía qué a quién y cuándo.

3.2.3.1 Gestión De Claves

Abarca la generación, distribución, almacenamiento, tiempo de vida, destrucción y aplicación de las claves de acuerdo con una política de seguridad.

Generación de claves

La seguridad de un algoritmo descansa en la clave. Un criptosistema que haga uso de claves criptográficamente débiles será él mismo débil. Algunos aspectos a considerar que se presentan a la hora de la elección de las claves son:

Espacio de claves reducido

Cuando existen restricciones en el número de bits de la clave, o bien en la clase de bytes permitidos (caracteres ASCII, caracteres alfanuméricos, imprimibles, etc.), los

ataques de fuerza bruta con hardware especializado o proceso en paralelo pueden desbaratar en un tiempo razonable estos sistemas.

Elección pobre de la clave

Cuando los usuarios eligen sus claves, la elección suele ser muy pobre en general (por ejemplo, el propio nombre o el de la mujer), haciéndolas muy débiles para un ataque de fuerza bruta que primero pruebe las claves más obvias (ataque de diccionario).

Claves aleatorias

Claves buenas son las cadenas de bits aleatorios generadas por medio de algún proceso automático (como una fuente aleatoria fiable o un generador pseudo - aleatorio criptográficamente seguro), de forma que si la clave consta de 64 bits, las 264 claves posibles sean igualmente probables. En el caso de los criptosistemas de clave pública, el proceso se complica, ya que a menudo las claves deben verificar ciertas propiedades matemáticas.

Frases de paso

La solución al problema de la generación de contraseñas seguras (y fáciles de recordar) por parte del usuario consiste en utilizar una frase suficientemente larga que posteriormente es convertida en una clave aleatoria por medio de un algoritmo.

Distribución de claves

El problema central de todo sistema de gestión de claves lo constituyen los procedimientos de distribución de éstas. Esta distribución debe efectuarse previamente a la comunicación. Los requisitos específicos en cuanto a seguridad de esta distribución dependerán de para qué y cómo van a ser utilizadas las claves. Así pues, será necesario garantizar la identidad de su origen, su integridad y, en el caso de claves secretas, su confidencialidad.

Las consideraciones más importantes para un sistema de gestión de claves son el tipo de ataques que lo amenazan y la arquitectura del sistema. Normalmente, es necesario que la distribución de claves se lleve a cabo sobre la misma red de comunicación donde se está transmitiendo la información a proteger. Esta distribución es automática y la transferencia suele iniciarse con la petición de clave por parte de una entidad a un Centro de Distribución de Claves (intercambio centralizado) o a la otra entidad involucrada en la comunicación (intercambio directo). La alternativa es una distribución manual (mediante el empleo de correos seguros, por ejemplo), independiente del canal de comunicación. Esta última alternativa implica un alto costo económico y un tiempo relativamente largo para llevarse a cabo, por lo que se descarta en la mayoría de las situaciones. La distribución segura de claves sobre canal inseguro requiere protección

criptográfica y, por tanto, la presencia de otras claves, conformando una jerarquía de claves. En cierto punto se requerirá protección no criptográfica de algunas claves (llamadas maestras), usadas para intercambiar con los usuarios de forma segura las claves que usarán en su(s) futura(s) comunicación(es). Entre las técnicas y ejemplos no criptográficos podemos citar seguridad física y confianza.

La distribución de claves se lleva siempre a cabo mediante protocolos, es decir, secuencias de pasos de comunicación (transferencia de mensajes) y pasos de computación.

Las claves criptográficas temporales usadas durante la comunicación, llamadas claves de sesión, deben ser generadas de forma aleatoria. Para protegerlas será necesaria seguridad física o cifrado mediante claves maestras, mientras que para evitar que sean modificadas deberá utilizarse seguridad física o autenticación.

Almacenamiento de claves

En sistemas con un solo usuario, la solución más sencilla pasa por ser su retención en la memoria del usuario. Una solución más sofisticada y que desde luego funcionará mejor para claves largas, consiste en almacenarlas en una tarjeta de banda magnética, en una llave de plástico con un chip ROM (ROM key) o en una tarjeta inteligente, de manera que el usuario no tenga más que insertar el dispositivo empleado en alguna ranura a tal efecto para introducir su clave.

Tiempo de vida de claves

Una clave nunca debería usarse por tiempo indefinido. Debe tener una fecha de caducidad, por las siguientes razones:

Cuanto más tiempo se usa una clave, aumenta la probabilidad de que se comprometa (la pérdida de una clave por medios no criptoanalíticos se denomina compromiso).

Cuanto más tiempo se usa una clave, mayor será el daño si la clave se compromete, ya que toda la información protegida con esa clave queda al descubierto.

Cuanto más tiempo se usa una clave, mayor será la tentación de alguien para intentar desbaratarla.

En general es más fácil realizar criptoanálisis con mucho texto cifrado con la misma clave.

Las claves maestras no necesitan ser reemplazadas tan frecuentemente, ya que se usan ocasionalmente para el intercambio de claves. En cualquier caso, no hay que

olvidar que si una clave maestra se compromete, la pérdida potencial es enorme, de hecho, todas las comunicaciones cifradas con claves intercambiadas con esa clave maestra.

En el caso del cifrado de grandes ficheros de datos, una solución económica y segura, mejor que andar descifrando y volviendo a cifrar los ficheros con una nueva clave todos los días, sería cifrar cada fichero con una única clave y después cifrar todas las claves con una clave maestra, que deberá ser almacenada en un lugar de alta seguridad, ya que su pérdida o compromiso echaría a perder la confidencialidad de todos los ficheros.

Destrucción de claves

Las claves caducadas deben ser destruidas con la mayor seguridad, de modo que no caigan en manos de un adversario, puesto que con ellas podría leer los mensajes antiguos. En el caso de haber sido escritas en papel, éste deberá ser debidamente destruido; si habían sido grabadas en una EEPROM, deberá sobreescribirse múltiples veces, y si se encontraba en EPROM, PROM o tarjeta de banda magnética, deberán ser hechas añicos. En función del dispositivo empleado, deberá buscarse la forma de que se vuelvan irrecuperables.

Asimismo es importante notar que los sistemas de seguridad requieren administrar la seguridad. La administración comprende dos campos:

Seguridad en la generación (procesamiento), localización (almacenamiento) y distribución (tránsito) de la información secreta, de modo que sólo pueda ser accedida por aquellas entidades autorizadas.

La política de los servicios y mecanismos de seguridad para detectar infracciones de seguridad y emprender acciones correctivas.

BIBLIOGRAFÍA

Gestión de Claves
Libro "Applied Cryptography", por Bruce Schneier.

Criptografía No Repudio, Autenticidad
http://webs.ono.com/usr016/Agika/6temas_relacionados/encriptar.htm#arriba

Encriptación, Confidencialidad
http://www.suratep.com/seguridad/seguridad.html

La Seguridad En La Ingeniería
http://www.acm.org/crossroads/espanol/xrds7-4/onpatrol74.html

Seguridad
http://www.iec.csic.es/criptonomicon/seguridad/

Seguridad Y Protección
http://www.onnet.es/03003001.htm

CAPÍTULO IV

ADMINISTRACIÓN DE LA SEGURIDAD

53-A

4.- ADMINISTRACIÓN DE LA SEGURIDAD

4.1 Introducción

La información es uno de los activos más importantes de las entidades; cada día dependen en mayor medida de la tecnología, en comparación con décadas atrás.

Por otra parte, hace unos años la protección era más fácil, con arquitecturas centralizadas y terminales no inteligentes, por eso hoy en día los entornos son complejos, con diversas plataformas y variedad de redes, no sólo internas sino también externas, incluso con enlaces internacionales.

Entre las plataformas físicas ("hardware") pueden estar: computadoras grandes y personales, solos o formando parte de redes, e incluso computadoras portátiles. Esta diversidad acerca la información a los usuarios, lo que hace más difícil proteger los datos.

Diseñar sistemas mediante criterios de seguridad es más complejo, pues las amenazas son en muchos casos poco cuantificables y muy variadas. La aplicación de medidas para proteger el sistema supone un análisis y cuantificación previa de los riesgos o vulnerabilidades del sistema. La definición de una política de seguridad y su implementación a través de una serie de medidas.

4.2 Principios Fundamentales De La Seguridad En Informática

Algunos principios fundamentales para diseñar una política de seguridad:

*** Principio de menor privilegio**

Cualquier objeto (usuario, administrador, programa, sistema, etc.) debe tener los privilegios necesarios para desarrollar su tarea y ninguno más. Esto quiere decir, cualquier usuario debe acceder a los recursos que necesite, para realizar las tareas que tenga encomendadas y sólo durante el tiempo necesario.

Al diseñar cualquier política de seguridad es necesario estudiar las funciones de cada usuario, programa, etc., definir los recursos a los que necesita acceder para llevarlas a cabo, identificar las acciones que necesita realizar con estos recursos, y establecer las medidas necesarias para que solo pueda llevar a cabo estas acciones.

*** La seguridad no se obtiene a través de la oscuridad**

Un sistema no es seguro escondiendo sus defectos o vulnerabilidades, debemos conocerlos y corregirlos, estableciendo las medidas de seguridad adecuadas.

Manteniendo los errores o vulnerabilidades en secreto no evita que existan, y por lo tanto evita que se corrijan.

No es una buena medida basar la seguridad en que un posible atacante no conozca las vulnerabilidades de nuestro sistema. Los atacantes siempre disponen de los medios necesarios para descubrir las debilidades más insospechadas de nuestro sistema.

No se consigue proteger un sistema evitando el acceso de los usuarios a la información relacionada con la seguridad. El mejor método para protegerlo es educar a los usuarios o diseñadores sobre el funcionamiento del sistema y las medidas de seguridad incluidas.

Tampoco se trata de hacer público en las noticias un nuevo fallo de nuestro sistema o un método para romperlo. En primer lugar hay que intentar resolverlo, obtener un medio para eliminar la vulnerabilidad y luego publicar el método de protección.

*** Principio del eslabón[19] más débil**

Al igual que en la vida real la cadena siempre se rompe por el eslabón más débil, en un sistema de seguridad el atacante siempre acaba encontrando y aprovechando los puntos débiles o vulnerabilidades.

Cuando diseñemos una política de seguridad o establezcamos los mecanismos necesarios para ponerla en práctica, debemos contemplar todas las vulnerabilidades y amenazas. No basta establecer mecanismos muy fuertes y complejos en algún punto en concreto, sino que hay que proteger todos los posibles puntos de ataque.

Por ejemplo, supongamos que establecemos una política de asignación de passwords muy segura, en la que estos se asignan automáticamente, son aleatorios y se cambian cada semana. Si en nuestro sistema utilizamos la red ethernet para conectar nuestras máquinas, y no protegemos la conexión, no nos servirá de nada la política de passwords establecidas. Por defecto, por ethernet los passwords circulan descifrados.

*** Defensa en profundidad**

La seguridad de nuestro sistema no debe depender de un solo mecanismo por muy fuerte y robusto que este sea, es necesario establecer varios mecanismos sucesivos.

[19] Eslabón.- Pieza que, enlazada con otras, forma una cadena.

De este modo cualquier atacante tendrá que superar varias barreras para acceder a nuestro sistema.

Por ejemplo en nuestro sistema podemos establecer un mecanismo de passwords altamente seguro como primera barrera de seguridad. Adicionalmente podemos utilizar algún método criptográfico fuerte para cifrar la información almacenada. De este modo cualquier atacante que consiga averiguar nuestro password y atravesar la primera barrera, se encontrará con la información cifrada y podremos seguir manteniendo su confidencialidad.

*** Punto de control centralizado**

Se trata de establecer un único punto de acceso a nuestro sistema, de modo que cualquier atacante que intente acceder al mismo tenga que pasar por él. No se trata de utilizar un sólo mecanismo de seguridad, sino de "alinearlos" todos de modo que el usuario tenga que pasar por ellos para acceder al sistema.

Este único canal de entrada simplifica nuestro sistema de defensa, puesto que nos permite concentrarnos en un único punto. Además nos permite monitorizar todos los accesos o acciones sospechosas.

*** Seguridad en caso de fallo**

En caso de que cualquier mecanismo de seguridad falle, nuestro sistema debe quedar en un estado seguro. Por ejemplo, si nuestros mecanismos de control de acceso al sistema fallan, es mejor que como resultado no dejen pasar a ningún usuario a que dejen pasar a cualquiera que no esté autorizado.

Quizás algunos ejemplos de la vida real nos ayuden más a aclarar este concepto. Normalmente cuando hay un corte de fluido eléctrico los ascensores están preparados para bloquearse mediante algún sistema de agarre, mientras que las puertas automáticas están diseñadas para poder abrirse y no quedar bloqueadas.

*** Participación universal**

Para que cualquier sistema de seguridad funcione es necesaria la participación universal, o al menos no la oposición activa, de los usuarios del sistema. Prácticamente cualquier mecanismo de seguridad que establezcamos puede ser vulnerable si existe la participación voluntaria de algún usuario autorizado para romperlo.

La participación voluntaria de todos los usuarios en la seguridad de un sistema es el mecanismo más fuerte conocido para hacerlo seguro. Si todos los usuarios prestan su apoyo y colaboran en establecer las medidas de seguridad y en ponerlas en práctica el sistema siempre tenderá a mejorar.

*** Simplicidad**

La simplicidad es un principio de seguridad por dos razones. En primer lugar, mantener las cosas lo más simples posibles, las hace más fáciles de comprender. Si no se entiende algo, difícilmente puede saberse si es seguro. En segundo lugar, la complejidad permite esconder múltiples fallos. Los programas más largos y complejos son propensos a contener múltiples fallos y puntos débiles.

4.3 Política De Seguridad

La política de seguridad es la declaración de intenciones significativas para proteger la seguridad de los Sistemas de Información(SI), proporcionan las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y de organización que se requieran.

La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las distintas medias a tomar para proteger la seguridad de los SI, las funciones y responsabilidades de los distintos componentes de la organización y los mecanismos para controlar su correcto funcionamiento.

Son los directivos, junto con los expertos en tecnologías de la información, quienes deben definir los requisitos de seguridad, identificando y dando prioridad a la importancia de los distintos elementos de la actividad a realizar, para que los procesos más importantes reciban más protección. La seguridad debe considerarse como parte operativa habitual, no como un extraño añadido. Dicha política tiene que ser consistente con las prácticas de seguridad de otros departamentos, puesto que muchas amenazas (incendio, inundación) son comunes a otras actividades de la organización.

Algunas reglas básicas para establecer una Política de Seguridad:

- Toda política de seguridad debe ser holísitca, es decir, debe cubrir todos los aspectos relacionados con el sistema.
  - Debe proteger el sistema en todos los niveles: físico, administrativo y legal.
  - Debe tener en cuenta no sólo los distintos componentes del sistema, tales como el hardware, software, entorno físico y usuarios, sino también la interacción entre los mismos.
  - Debe tener en cuenta el entorno del sistema, esto es, el tipo de compañía o entidad con que tratamos (comercial, bancaria, educativa, ...). De esta consideración surge la segunda regla básica

- La política de seguridad debe adecuarse a nuestras necesidades y recursos, el valor que se le da a los recursos y a la información, el uso que se hace del sistema en todos los departamentos.

  - Deben evaluarse los riesgos, el valor del sistema protegido y el coste de atacarlo. Las medidas de seguridad tomadas deben ser proporcionales a estos valores.

- Toda política de seguridad debe basarse fundamentalmente en el sentido común. Es necesario:
  - Un conocimiento del sistema a proteger y de su entorno.
  - Un conocimiento y experiencia en la evaluación de riesgos y el establecimiento de medidas de seguridad.
  - Un conocimiento de la naturaleza humana, de los usuarios y de sus posibles motivaciones.

A la hora de establecer una política de seguridad debemos responder a las siguientes tres preguntas:

- • ¿ Qué necesitamos proteger?
- • ¿ De qué necesitamos protegerlo?
- • ¿ Cómo vamos a protegerlo?

lo que nos lleva a los siguientes pasos básicos:

- 1. Determinar los recursos a proteger y su valor.
- 2. Analizar la vulnerabilidad y amenazas de nuestro sistema, su probabilidad y su costo.
- 3. Definir las medidas a establecer para proteger el sistema.
- Estas medidas deben ser proporcionales a lo definido en los pasos 1 y 2.
- Las medidas deben establecerse a todos los niveles: físico, lógico, administrativos y legales.
- Además debe definirse una estrategia a seguir en caso de fallo.

- 4. Monitorizar el cumplimiento de la política y revisarla y mejorarla cada vez que se detecte un problema.

Los pasos 1 y 2 se denominan Análisis de riesgos, mientras los pasos 3 y 4 se denominan Gestión de riesgos. La política de seguridad es el conjunto de medidas establecidas en el paso 3.

4.4 Medias De Seguridad

En muchos casos llevan un costo que obliga a subordinar algunas de las ventajas del sistema. Por ejemplo, la velocidad de las transacciones. En relación a esto, se hace obvio que a mayores y más restrictivas medidas de seguridad, menos amigable es el sistema. Se hace menos cómodo para los usuarios ya que limita su actuación y establece unas reglas más estrictas que a veces dificultan el manejo del sistema. Por ejemplo, el uso de una política adecuada de passwords, con cambios de las mismas.

Las medidas de seguridad que pueden establecerse en un sistema informático son de cuatro tipos fundamentales: lógicas, físicas, administrativas y legales. Vamos a verlas con más detalle.(Fig. 4.3).

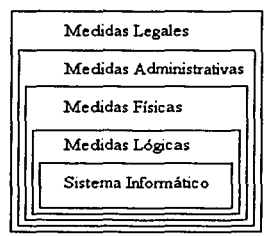

Figura 4.3 Medidas de Seguridad

4.4.1 Medidas Lógicas

Incluye las medidas de acceso a los recursos, a la información y al uso correcto de los mismos, así como a la distribución de las responsabilidades entre los usuarios. Se refiere más a la protección de la información almacenada.

Entre los tipos de controles lógicos que es posible incluir en una política de seguridad podemos destacar los siguientes:

•Establecimiento de una política de control de accesos. Incluyendo un sistema de identificación y autenticación de usuarios autorizados y un sistema de control de acceso a la información.

•Definición de una política de instalación y copia de software.

•Uso de la criptografía para proteger los datos y las comunicaciones.
•Uso de Firewalls[20] para proteger una red local de Internet.

•Definición de una política de copias de seguridad.

•Definición de una política de monitorización (logging) y auditoría (auditing) del sistema.

Dentro de las medidas lógicas se incluyen también aquellas relativas a las personas y que podríamos denominar medidas humanas. Se trata de definir las funciones, relaciones y responsabilidades de distintos usuarios potenciales del sistema. Se trataría entonces de responder a preguntas tales como:

•¿ A quién se le autoriza el acceso y uso de los recursos?

•¿ A qué recursos accede cada usuario y qué uso puede hacer de ellos?

•¿ Cuáles son las funciones del administrador del sistema y del administrador de la seguridad?

•¿ Cuáles son los derechos y responsabilidades de cada usuario?

Para responder a las preguntas anteriores debemos diferenciar cuatro tipos fundamentales de usuarios. A cada tipo se le aplicará una política de control de acceso distinta y se le asignará un grado de responsabilidad sobre el sistema:

•El administrador del sistema y en su caso el administrador de la seguridad.

•Los usuarios del sistema.

•Las personas relacionadas con el sistema pero sin necesidad de usarlo

•Las personas ajenas al sistema

[20] Firewalls.- el propósito de un firewall es proporcionar el acceso controlado y auditado a los servicios, tanto al interior como al exterior de la red de la organización en cuestión y esto lo hace permitiendo, denegando o redireccionando el flujo de los datos que pasan a través de él.

4.4.2 Medidas Físicas

Aplican mecanismos para impedir el acceso directo o físico no autorizado al sistema.

También protegen al sistema de desastres naturales o condiciones medioambientales adversas. Se trata fundamentalmente de establecer un perímetro de seguridad en nuestro sistema.

Existen tres factores fundamentales a considerar:

- El acceso físico al sistema por parte de personas no autorizadas
- Los daños físicos por parte de agentes nocivos o contingencias
- Las medidas de recuperación en caso de fallo

Concretando algo más los tipos de controles que se pueden establecer, estos incluyen:

- Control de las condiciones medioambientales (temperatura, humedad, polvo, etc....)
- Prevención de catástrofes (incendios, tormentas, cortes de fluido eléctrico, sobrecargas, etc.)
- Vigilancia (cámaras, guardias jurados, etc.)
- Sistemas de contingencia (extintores, fuentes de alimentación ininterrumpida, estabilizadores de corriente, fuentes de ventilación alternativa, etc.)
- Sistemas de recuperación (copias de seguridad, redundancia, sistemas alternativos geográficamente separados y protegidos, etc.)
- Control de la entrada y salida de material (elementos desechables, consumibles, material anticuado, etc.)

4.4.3 Medidas Administrativas

Las medidas técnico - administrativas, como la existencia de políticas y procedimientos, o la creación de funciones, como la administración de la seguridad o auditoría de sistemas de información interna, serán independientes y nunca una misma persona podrá realizar las dos ni existir dependencia jerárquica de una función respecto a otra.

En cuanto a la administración de seguridad pueden existir, además, coordinadores en las diferentes áreas funcionales y geográficas de cada entidad, especialmente si la dispersión o la complejidad organizativa o el volumen de la entidad así lo demandan.

En el caso de multinacionales o grupos de empresas nacionales no está de más que exista una coordinación a niveles superiores.

Debe existir una definición de funciones y separación suficiente de tareas; no tiene sentido que una misma persona autorice una transacción, la introduzca, y revise después los resultados (un diario de operaciones, por ejemplo), porque podría planificar un fraude o encubrir cualquier anomalía; por ello deben intervenir funciones, personas diferentes y existir controles suficientes.

Las medidas administrativas son aquellas que deben ser tomadas por las personas encargadas de definir la política de seguridad para ponerla en práctica, hacerla viable y vigilar su correcto funcionamiento. Algunas de las medidas administrativas fundamentales a tomar son las siguientes:

•Documentar y publicar la política de seguridad y de las medidas tomadas para ponerla en práctica.

•Definir quien fija la política de seguridad y quien la pone en práctica.

•Establecer un plan de formación del personal.

Los usuarios deben tener los conocimientos técnicos necesarios para usar la parte del sistema que les corresponda. Este tipo de conocimiento son fundamentales para evitar una serie de fallos involuntarios que pueden provocar graves problemas de seguridad.

Los usuarios deben ser conscientes de los problemas de seguridad de la información a la que tienen acceso.

Los usuarios deben conocer la política de seguridad de la empresa y las medidas de seguridad tomadas para ponerla en práctica. Además deben colaborar, a ser posible voluntariamente, en la aplicación de las medidas de seguridad.

Los usuarios deben conocer sus responsabilidades respecto al uso del sistema informático, y deben ser conscientes de las consecuencias de un mal uso del mismo.

4.4.4 Medidas Legales

Se refiere más a la aplicación de medidas legales para disuadir al posible atacante o para aplicarle algún tipo de castigo a posteriori.
Este tipo de medidas trascienden el ámbito de la empresa y normalmente son fijadas por instituciones gubernamentales e incluso instituciones internacionales. Un ejemplo de este tipo de medidas es la LORTAD (Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal). Esta ley vincula a todas las entidades que trabajen con datos de carácter personal, define las medias de seguridad para su protección y las penas a imponer en caso de su incumplimiento.

4.5 Riesgos

El mayor riesgo, aun teniendo un entorno muy seguro, es que la Informática, y la Tecnología de la Información en general, no cubran las necesidades de la entidad: no estén alineadas con el Plan de "Negocio".

Limitándonos a la seguridad propiamente dicha, los riesgos pueden ser múltiples: el primer paso es conocerlos, y el segundo es tomar decisiones al respecto; el conocerlos y no tomar decisiones no tiene sentido y crea una situación de intranquilidad.

Como las medidas tienen un costo, a veces los directivos se preguntan, cuál es el riesgo máximo que podría soportar su entidad, la respuesta no es fácil, depende de su dependencia respecto a la información, y del impacto que su no disponibilidad pudiera tener en la entidad.

Hay daños de menores consecuencias, siendo los errores y omisiones las causas más frecuentes, normalmente de poco impacto pero frecuencia muy alta, y otras el acceso indebido a los datos (a veces a través de redes), la cesión no autorizada de soportes magnéticos con información crítica (algunos dicen "sensible"), los daños por fuego, por agua (del exterior como puede ser una inundación, o una tubería interior), la variación no autorizada de programas, su copia indebida, persiguiendo el propio beneficio o el causar un daño, a veces por venganza.

El hacker, intenta acceder a los sistemas para demostrar (a veces sobre todo para demostrarse a sí mismo/a) de qué es capaz, así como poder superar las barreras de protección que le hayan establecido.

Con los virus, existe un riesgo constante porque de forma continua aparecen nuevas modalidades, que no son detectadas por los programas antivirus hasta que las nuevas versiones los contemplan, puedan llegar a afectar a los grandes sistemas, sobre todo a través de las redes, pero esto es realmente difícil - no nos atrevemos a decir que imposible- por las características y complejidad de los grandes equipos y las características de diseño de sus sistemas operativos.

Las amenazas hechas realidad pueden llegar a impactar en los datos, en las personas, en los programas, en los equipos, en la red... y alguna incidencia en varios de ellos, como puede ser un incendio.

Nos preguntamos ¿qué es lo más crítico a proteger? La respuesta de la mayoría probablemente sería que las personas somos lo más crítico, y el valor de una vida humana no se puede comparar con los ordenadores, las aplicaciones o los datos de cualquier entidad.

Como consecuencia de cualquier incidencia se pueden producir pérdidas, que pueden ser no sólo directas (y éstas las pueden cubrir los seguros), sino también indirectas,

como la no recuperación al perder los datos, o no poder tomar las decisiones adecuadas en el momento oportuno por carecer de información.

Protección de Activos Vitales

Son activos vitales todos aquellos relacionados con la continuidad de la entidad, como pueden ser: planes estratégicos, fórmulas magistrales, diseño de prototipos, resguardos, contratos, pólizas... y datos estratégicos, que son los que más nos interesan bajo la perspectiva de la seguridad de la información.

Debemos protegerlos pensando en los intereses de los accionistas, de los clientes, y también pensando en los empleados y en los proveedores.

La protección no ha de basarse sólo en dispositivos y medios físicos, sino en formación e información adecuada al personal, empezando por los directivos para que, "en cascada", afecte a todos los niveles de la pirámide organizativa.

Además, la existencia de funciones específicas cuando el entorno lo justifica, contribuye a incrementar la seguridad. Entre ellas las citadas de administración de la seguridad y auditoría de sistemas de información interna.

Deben existir tres niveles de protección:

El CONTROL INTERNO, basado en objetivos de control y llevado a cabo por los supervisores a distinto nivel,

La AUDITORÍA DE SISTEMAS DE INFORMACIÓN INTERNA, objetiva e independiente y con una preparación adecuada, como control del control,

La AUDITORIA DE SISTEMAS DE INFORMACIÓN EXTERNA, contratada cuando se considera necesaria, y como un nivel de protección más. Igualmente objetiva e independiente.

Los informes de auditores, internos o externos, han de señalar las posibles deficiencias e indicar, en su caso, las recomendaciones correspondientes.

BIBLIOGRAFÍA

CRIPTOGRAFÍA NO REPUDIO, AUTENTICIDAD
http://webs.ono.com/usr016/Agika/6temas_relacionados/encriptar.htm#arriba

ENCRIPTACIÓN, CONFIDENCIALIDAD
http://www.suratep.com/seguridad/seguridad.html

LA SEGURIDAD EN LA INGENIERÍA
http://www.acm.org/crossroads/espanol/xrds7-4/onpatrol74.html

SEGURIDAD
http://www.iec.csic.es/criptonomicon/seguridad/

SEGURIDAD Y PROTECCIÓN
http://www.onnet.es/03003001.htm

CAPÍTULO V

PROPUESTAS

5.- PROPUESTAS

5.1 INTRODUCCIÓN

¿Que ha ocurrido con los esquemas de seguridad y su legislación?

Los diferentes proveedores de hardware y software, han invertido importantes cantidades de dinero en sus laboratorios e investigadores, para poner a disposición de los usuarios herramientas tecnológicas que se encarguen de actuar como agentes de seguridad en sus redes de cómputo y comunicaciones, así como para custodiar sus instalaciones estratégicas. Pero ¿qué ocurre cuando se realizan las auditorías, o se presentan contingencias, o aparecen los virus, u otros factores que nos hacen recapacitar sobre la importancia de los esquemas de seguridad?.

Propuesta para atenuar este impacto:

Sensibilizar a los diferentes niveles que integran la Federación, los Estados, el Distrito Federal y los Municipios sobre la importancia que representa el proteger la información contenida en medios electrónicos, los equipos de computo y sus instalaciones, bajo los siguientes planteamientos:

¿Dónde se necesita la seguridad?

¿Qué debemos proteger?

¿Para qué se debe proteger?

Formalizar la función de seguridad informática, con personal que cubra el perfil idóneo para involucrarse en las diferentes plataformas tecnológicas y sectores de negocios para:

La incorporación de las medidas de seguridad que deben regir el uso de los recursos informáticos en su organización, con el apoyo de las herramientas tecnológicas (hardware y software) disponibles en el mercado para tal fin.

Contar con un marco jurídico que permita que la falta de apego a las políticas, normas y procedimientos, cubran a las Entidades de la Administración Pública Federal, Estatal y Municipal y de las empresas que conforman el Sector Privado en materia de informática, de las acciones fraudulentas, espionaje, violaciones, falta de honradez, etc., las que constituyan una conducta delictiva; buscando con ello asegurar la integridad, la confidencialidad y la confiabilidad de la información electrónica; como parte primordial de su patrimonio.

Adición de los Artículos 43-bis, 43 bis-I, 44 bis, 45 bis y 45 bis-I a la Ley General que Establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.

5.2 ALMACENAMIENTO Y RESPALDO DE LA INFORMACIÓN

TÍTULO SEGUNDO
DEL SISTEMA NACIONAL DE SEGURIDAD PÚBLICA

CAPÍTULO IV
De la Información Nacional sobre Seguridad Pública

Sección Quinta
De las Reglas Generales sobre la Información

Artículo 43 bis.- El almacenamiento y respaldo de la información para el sector de la Federación, los Estados, el Distrito Federal y los Municipios que utilizan equipos de cómputo; protegerán la seguridad de los datos, con técnicas para su almacenamiento y recuperación, utilizando los recursos informáticos para garantizar la existencia y veracidad de la información en medios magnéticos u ópticos.

Almacenamiento Seguro

La información almacenada en medios magnéticos u ópticos debe contar con un documento donde se registre:

Si se trata de:

Archivo Maestro.- Aquél que contiene información que generalmente se toma como referencia para otros procesos.

Base de Datos.- Conjunto de datos organizados entre los cuales existe una correlación y que están almacenados con criterios independientes de los programas que los utilizan. La filosofía de las bases de datos es la de almacenar grandes cantidades de información tal que permita las posibles consultas de acuerdo a los derechos de acceso y mediante una redundancia controlada.

Archivo Primario.- Archivo inicial o de partida que después de ser procesado generará archivos secundarios o complementarios.

Archivo Temporal.- Archivo intermedio que se genera en forma temporal que servirá para alimentar procesos intermedios y posteriores. Se trata de archivos eventuales o de corta duración.

Dejar especificado en el documento el nombre del sistema o aplicación, frecuencia de los procesos y la longitud del registro (tamaño del archivo).

Los medios magnéticos u ópticos (diskettes,CD's, cintas, y discos duros), deben tener etiquetas con el nombre de la aplicación, nombre del archivo, fecha de creación y si está empaquetado o no. Para el caso de las cintas magnéticas, las etiquetas deberán contener adicionalmente longitud del archivo, número de archivos, versión, nombre de la persona responsable, fecha de creación, así como especificar si es copia u original.

Respaldo de seguridad

Artículo 43 bis 1.- La información generada en un equipo de cómputo dentro de una entidad deberá ser almacenada en medios magnéticos u ópticos y por lo menos tendrán una copia de respaldo en diskettes o en otro medio de que disponga la entidad.

Debe haber un lugar designado de manera específica por la organización para resguardar los respaldos.

La información almacenada debe ser verificada íntegramente, tanto el original como las copias (en caso de encontrarse empaquetada, desempaquetarla para su revisión), antes de ser guardada en algún lugar asignado, así como también se debe examinar que la información no esté contaminada con virus informático.

Debe existir una copia de respaldo de los archivos, clasificandolos de acuerdo a su duración, importancia, frecuencia de actualización y función principal.

Los archivos que son textos, hojas de cálculo, gráficos, etc., mientras no se concluyan, serán guardados en una sola copia por cada actualización para facilitar su almacenamiento. Una vez concluidos se debe guardar una copia adicional de respaldo, en forma empaquetada o no, dependiendo del tamaño del archivo.

Cuando se quiera almacenar un archivo de respaldo éste deberá guardarse físicamente en otra unidad magnética (CD's, diskette, cinta o disco duro) diferente a la que contiene el archivo original, es decir, deben existir al menos dos medios magnéticos u ópticos de un mismo respaldo de información.

La información que se procesa periódicamente, se respaldará por periodos.

Entendiéndose por período, al tiempo (semanal, mensual, bimensual, trimestral, semestral, o anual) que transcurre para que se ejecute el procesamiento de la información.

En el caso de las Encuestas y Censos se deberá contar con las dos versiones de los archivos básicos:

a) La información sin imputar.

b) La información imputada (clasificada o comprometida).

Copias adicionales con la información imputada podrán ser guardadas en diferentes entidades, que garanticen el buen estado, existencia y veracidad de los archivos almacenados en medios magnéticos u ópticos.

Los lugares en donde se guarden los medios magnéticos y ópticos deben contar con una adecuada temperatura y no presentar humedad.

Los medios magnéticos y ópticos para almacenar la información deben ser nuevos (primer uso), verificándo su buen estado operacional.

Los medios magnéticos y ópticos donde está grabada la información deben recibir mantenimiento de limpieza con cierta periodicidad la cual debe ser al menos una vez al año.

Sólo el personal responsable de la integridad de la información tendrá acceso al ambiente donde se encuentren estos medios magnéticos previa autorización de la dependencia encargada por medio de un documento (nota informativa, oficio, requisición, vale, etc.), es decir sólo el personal encargado de la elaboración y procesamiento del sistema y el usuario responsable del mismo podrán acceder y usar la información que está almacenada en los medios magnéticos u ópticos.

El personal que elabora los sistemas de cómputo estimará la cantidad de medios magnéticos requeridos para las copias de los archivos de datos y de programas.

En el modo de trabajo monousuario, los usuarios son los responsables de hacer el respaldo de la información generada.

En el modo de trabajo multiusuario el responsable de hacer el respaldo de la información es el administrador de la red.

El disco duro es un medio de almacenamiento temporal de la información, el cual debe ser depurado permanentemente de los archivos que no volverán a ser utilizados en forma inmediata, así como efectuar un respaldo de toda la información útil que se encuentra almacenada en el disco duro, dicha actividad será realizada por el responsable designado para tal fin.

En caso de que se trabaje en red o en modo multiusuario, el administrador de la red hará un respaldo de la información útil del disco duro, con cierta periodicidad que depende directamente de la organización, según lo estipule por su importancia.

Los Funcionarios o Directivos, por escrito designarán al personal responsable de realizar el almacenamiento y respaldo, en medios magnéticos u ópticos de la información necesaria que procesa su Dirección.

Los Funcionarios o Directivos de las áreas de cómputo son responsables de cumplir y hacer cumplir las normas de seguridad informática de la organización.

5.3 TECNICAS PARA LA SEGURIDAD E INTEGRIDAD DE LA INFORMACIÓN

Artículo 44 bis.- La finalidad es mostrar la disponibilidad, autenticidad e integridad de la información del sector de la Federación, los Estados, el Distrito Federal y los Municipios que utiliza equipos de cómputo.

Se debe asegurar que sólo personal autorizado tenga acceso a la información clasificada como restringida o reservada, así como evitar la reproducción de la información sin la debida autorización y garantizar la integridad y autenticidad de la misma.

Acceso a la información

En los procedimientos administrativos será necesaria la identificación previa del personal que va a ingresar a las áreas de cómputo, verificando si cuenta con la autorización correspondiente y registrándo el ingreso y salida al área.

En los Sistemas Informáticos se considera necesario utilizar programas de cómputo, que cuenten con rutinas de control para el acceso de los usuarios.

Las rutinas de control, permiten que los usuarios ingresen al Sistema, previa identificación, mediante una palabra clave (password), la cual será única para cada uno de ellos; negando el acceso a las personas que no han sido definidos como usuarios del Sistema.

Las rutinas de control de acceso permitirán a los usuarios autorizados a usar determinados sistemas con su correspondiente nivel de acceso, el cual incluye la lectura o modificación en sus diferentes formas.

Modos de acceso

De forma general, un sistema de control de acceso relaciona los sujetos (usuario o proceso) que actúan en el sistema con cada uno de los recursos (archivos, dispositivos, ...). Los modos de acceso que suelen encontrarse en los sistemas son las siguientes:

Lectura: obtención por parte del sujeto de la información pasiva contenida en el recurso.

Escritura: modificación de los parámetros o el contenido del recurso (creación, borrado, modificación o concatenación de ficheros).

Ejecución: utilización activa de un recurso con comportamiento propio. El caso más típico es el de las aplicaciones y programas.

Borrado: eliminación (física o lógica) de un recurso. Puede ser especificado como modo de acceso distinto al de escritura, o estar incluido en esta.

Listado: acceso a los atributos del recurso. Al igual que ocurre con el modo anterior, puede ser especificado como modo de acceso distinto al de lectura, o estar incluido en esta.

Los dos últimos modos de acceso se presentan de forma separada con mucha menos frecuencia, pero ocasionalmente el permiso de listado puede ser bastante útil para implementar aspectos particulares de algunas políticas de seguridad.

Niveles de acceso a la información:

a) Nivel de consulta de la información no restringida o reservada.

b) Nivel de mantenimiento de la información no restringida o reservada.

c) Nivel de consulta de la información incluyendo la restringida o reservada.

d) Nivel de mantenimiento de la información incluyendo la restringida o reservada.

Para garantizar estos niveles cada palabra clave tendrá asignado uno de estos niveles de acceso.

Consecuentemente la información que se considere restringida o reservada estará debidamente identificada, así como a los usuarios que accedan a ella. Cada Unidad Orgánica de Informática cuenta para ello con un Administrador de la Información, quien es responsable de la asignación de las palabras claves, de los niveles de acceso y las fechas de expiración.

La Unidad Orgánica dispondrá de un procedimiento que posibilite que las palabras claves tengan o se generen bajo un periodo de vigencia con base en las normas de seguridad informática de la organización.

El Jefe de cada Unidad Orgánica es responsable del acceso a la información y será quien indique las directivas adecuadas al Administrador de la Información.

Los operadores de la información restringida o reservada realizarán estrictamente lo indicado en cada procedimiento establecido de procesamiento de la información, para lo cual éstos deberán estar claramente documentados.

En una base de datos se preverá en su desarrollo garantizar un límite máximo de instalaciones (licencias autorizadas), para su uso.

Se protegerá la información clasificada como restringida o reservada encriptándola.

El software de encriptación deberá cumplir las siguientes condiciones:

a) Ser portable, es decir que funcione en todos los ambientes: computadoras grandes, mini y microcomputadoras.

b) Podrá utilizarse en cualquier lenguaje de programación.

c) Ser de fácil entendimiento por el usuario, de tal manera que permita su uso sin necesidad que éste conozca las técnicas de encriptación. Estar debidamente documentado, para ser entendible por cualquier usuario.

La protección especial de la información incluye por parte de la empresa establecer procedimientos adecuados para el control y distribución de la información impresa, así como para la grabación de los medios magnéticos u ópticos y su respectivo almacenamiento.

La Integridad de la Información

Artículo 45 Bis.- Todo Sistema de Información diseñado por personal del sector de la Federación, los Estados, el Distrito Federal y los Municipios pertenecerá a ésta.

Los programas deberán estar autodocumentados y utilizarán nombres que permitan su fácil identificación.

El cambio que se haga a los sistemas informáticos debe ser inmediatamente documentado.

Las pruebas que se hagan a los sistemas de información y que para ello lo hagan con datos se deberán efectuar, primero con un volumen pequeño de ellos, seguidamente se probarán con un volumen de datos aproximado al real.

Para asegurar la calidad del Sistema es necesario efectuar pruebas de verificación y validación entre el analista y el usuario.

Debe existir la compatibilidad entre los módulos individuales integrantes de los sistemas.

Llevar un control de las licencias del software comprado al proveedor especificando si las actualizaciones son independientes de la compra de dicho software, así como aclarar si el servicio de instalación viene incluido o no.

Se deberá llevar un registro ordenado y clasificado de las actualizaciones del software tanto el diseñado internamente como el adquirido al proveedor con sus respectivas licencias originales.

Se proporcionará con anticipación los cursos necesarios a los operadores de las computadoras y con la debida documentación necesaria para la ejecución de trabajos de procesamiento automático de datos, de acuerdo a las prioridades de los mismos.

El responsable de un archivo debe adoptar las medidas de seguridad, que garanticen el cumplimiento de las normas. El usuario de sistemas informáticos que disponga de una palabra clave de acceso será responsable de su mal uso, así como por otras personas no autorizadas.

El Órgano de administración correspondiente debe proveer al personal, el mobiliario e instalaciones adecuadas para almacenar los datos clasificados.

Es recomendable constituir un comité de seguridad que velará por el cumplimiento de las normas y políticas de seguridad, y que estará presidido por el jefe de cómputo u otra persona de nivel equivalente y usuarios de la información clasificada como restringida o reservada.

La designación por escrito del personal encargado de la administración de los niveles de acceso a la información y del manejo de las palabras claves, deberá ser efectuado por los Funcionarios responsables de los órganos estructurados de sistemas de cómputo.

La Unidad Orgánica correspondiente deberá contar con toda información trabajada que se considere útil y de interés institucional, para que en caso de efectuarse una auditoría, está cuente con la documentación elaborada y se ubique rápidamente en los medios magnéticos.

5.4 PROTECCIÓN FÍSICA DE LOS EQUIPOS

Artículo 45 Bis-1.- La finalidad es mantener la seguridad de los equipos de cómputo y medios magnéticos u ópticos utilizados, para garantizar la seguridad de la información disponible en medios de almacenamiento, ante contingencias naturales, siniestros o sabotaje.

Evitar la destrucción de equipos, componentes e insumos informáticos.
Comprende a las áreas responsables de las instalaciones, mantenimiento y uso de equipos de cómputo, así como a todo el personal que hace uso de dichos equipos.

Realizar cálculos de la carga eléctrica requerida, de los tableros de distribución, así como de los circuitos y conexiones que deben soportar la carga adicional proyectada[21].

Disponer de circuitos alternos y tableros de distribución eléctrica independientes a cualquier otra conexión.

Deberá disponerse de un pozo a tierra, conectado al Sistema Eléctrico que alimenta los equipos de cómputo. Asimismo se etiquetará el cableado, las extensiones y los tableros de distribución eléctrica.

Reforzar la energía eléctrica de voltaje con la ayuda de sistemas de estabilización de voltaje, (UPS).

Tener en un lugar visible los procedimientos de maniobras de encendido de emergencia.

No dejar el cableado suelto o disperso[22].

Deben existir puntos centrales de corte de fluido eléctrico, a nivel edificio o piso.

Se deberán tener los sistemas de agua y desagüe a niveles inferiores al Centro de Cómputo.

El Centro de Cómputo deberá contar con servicio de aire acondicionado, no se encontrará próximo a material inflamable, asimismo contará con las instrucciones de operación visibles tanto del centro de cómputo como del aire acondicionado.

Asegurar que las tomas de aire de los equipos se encuentren ubicada en zonas no susceptibles de ser obstruidas.

[21] Catálogo de Normas Oficiales Mexicanas CONAE (Comisión Nacional para el Ahorro de Energía) Secretaría de Energía: http://www.conae.gob.mx/wb/distribuidor.jsp?seccion=1324
[22] Estándar Cableado Estructurado.- Estándar ANSI/TIA/EIA-568-A de alambrado de Telecomunicaciones para edificios Comerciales.

Se capacitará periódicamente al menos una vez al año al personal, en el uso y mantenimiento del equipo contra incendio, sistema de agua y electricidad.

Disponer de un plano que contenga todas las fuentes de suministros posibles de agua, instalación eléctrica con su capacidad estimada en cada caso.

Evitar que las paredes, pisos y techos contengan material inflamable, recomendándose instalar equipos de alarma detectores de humo.

Para combatir los incendios producidos por equipos eléctricos se deben utilizar extintores. Estos estarán al alcance inmediato, preservando la vigencia química del extintor, e identificando su localización en el respectivo plano.

Es recomendable que exista suficiente iluminación en los alrededores del edificio, las ventanas o mamparas y se protejan de manera que se evite el impacto de piedras o material incendiario.

El acceso a los centros de cómputo será restringido solo al personal autorizado, y contando con un registro de entradas y salidas de visitantes.

Las micro - computadoras y terminales tendrán un soporte logístico, que permita un apropiado mantenimiento preventivo.

El servicio de mantenimiento de los equipos de cómputo lo realizará personal especializada que garantice un buen servicio.

Contar con un plan de contingencia, así como con estrategias adecuadas para hacer frente a los desastres. Entre el área de cómputo y las demás áreas, se establecerán acuerdos acerca de las condiciones bajo las cuales el plan de contingencia ha de ser activado, considerándose la duración probable de la falta de servicio, y la pérdida (total o parcial) de la capacidad de procesamiento en una o varias instalaciones, etc.

Seleccionar organizaciones afines a la Institución y establecer con una o más de ellas convenios de mutuo apoyo, para los casos de desastres que inhabiliten el procesamiento de información. El principal criterio será la confiabilidad, también habrá que analizar la capacidad del centro de cómputo de la institución para efectuar el servicio recíproco, podría contemplar una entidad alterna espejo.

Deberá crearse un Comité de Seguridad a un nivel institucional, que vigile el cumplimiento de las normas y las políticas de seguridad de los equipos y medios de procesamiento de la información, el cual se recomienda que esté presidido por el Jefe de Cómputo u otro funcionario de nivel equivalente.

Los Funcionarios responsables, designarán por escrito, al personal custodio de la protección física de los equipos y medios de procesamiento de la información.

ANEXO IV

PROPUESTAS

La Propuesta que se anexa a continuación, es la que se obtuvo como resultado de la investigación llevada a cabo en el presente trabajo de Tesis y es una Propuesta de Reformas de Ley entregada en Oficialía de Partes del la Honorable Cámara de Diputados el 19 de Mayo de 2003.

NOTA ACLARATORIA:

Referente a la numeración de las hojas de la Propuesta que van consecutivamente del 1 al 11 está es debido a la presentación a la Honorable Cámara de Diputados así como también formarán parte de la numeración consecutiva de la Tesis.

México D.F. a 19 de Mayo de 2003

CIUDADANOS DE LA CÁMARA DE DIPUTADOS DE LA LVIII LEGISLATURA DEL HONORABLE CONGRESO DE LA UNIÓN

Griselda Pérez Osorio, mexicana por nacimiento, con credencial de elector expedida por el Instituto Federal Electoral número 059279763 y domicilio en calle Jarana 14 interior 2 Unidad Independencia, con fundamento en el artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, presentó a consideración del H. Congreso de la Unión, la iniciativa de decreto por el que se adicionan diversos artículos a la Ley General que Establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública, de conformidad con la siguiente:

EXPOSICIÓN DE MOTIVOS

Los artículos 21, y 73, fracción XIII, de la Constitución Política de los Estados Unidos Mexicanos, fueron reformados en el año de 1994, teniendo como objetivo establecer fundamentos jurídicos para aplicar en todo el país los principios sobre los cuales la Federación, los Estados, el Distrito Federal y los Municipios se coordinarían para combatir de manera la delincuencia.

Dicha reforma, estableció como un mandato Constitucional, la conformación de un Sistema Nacional de Seguridad Pública, mecanismo en dónde los tres órdenes de gobierno confluirían para hacer efectiva dicha coordinación en materia de seguridad pública, en los términos que la Ley respectiva señalaría.

Congruente con lo anterior, el H. Congreso de la Unión con fundamento en el artículo 73, fracción XIII expidió La Ley General que Establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública, misma que fue publicada en el Diario Oficial de la Federación el 11 de diciembre de 1995.

Esta Ley General señala en su artículo 2°, que el Sistema Nacional de Seguridad Pública, se integra con las instancias, instrumentos, políticas, servicios y acciones, tendientes a cumplir los objetivos y fines de la seguridad pública.

Como uno de los instrumentos más importantes del Sistema Nacional de Seguridad Pública se encuentra la obligación de la Federación, los Estados y los municipios de suministrar, intercambiar y sistematizar la información sobre seguridad pública. Esta información sobre seguridad pública integra los registros nacionales de personal de seguridad pública y de armamento y equipo, así como de la estadística de seguridad pública, de la información de apoyo a la procuración de justicia, entre otros.

Sin embargo la Ley General, no establece criterios claros de cómo deberá resguardarse la información a que se refiere su Capítulo IV, por lo que se hace necesario garantizar la seguridad de la información contenida en los medios electrónicos, equipos de cómputo e inclusive sus instalaciones.

Bajo ese esquema, se hace necesario formalizar la función de seguridad informática, con personal que cubra el perfil idóneo para involucrarse en las diferentes plataformas tecnológicas y sectores de negocios para la incorporación de las medidas de seguridad que deben regir el uso de los recursos informáticos en su organización, con el apoyo de las herramientas tecnológicas (hardware y software) disponibles en el mercado para tal fin, así como contar con un marco jurídico que permita que la falta de apego a las políticas, normas y procedimientos cubran a la Federación, los Estados, el Distrito Federal y los Municipios de las acciones fraudulentas, espionaje, violaciones, falta de honradez, etc., que pongan en riesgo la integridad, la confidencialidad y la confiabilidad de la información de la institución como parte primordial de su patrimonio.

Por lo anteriormente expuesto me permito someter a la elevada consideración del Honorable Congreso de la Unión, la siguiente iniciativa de:

"DECRETO POR EL QUE ADICIONAN LOS ARTÍCULOS 43-BIS, 43 BIS-I, 44 BIS, 45 BIS Y 45 BIS-I A LA LEY GENERAL QUE ESTABLECE LAS BASES DE COORDINACIÓN DEL SISTEMA NACIONAL DE SEGURIDAD PÚBLICA.

ARTÍCULO PRIMERO.- Se adicionan los artículos 43-bis, 43 bis-I, 44 bis, 45 bis y 45 bis-I de la Ley General que Establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública, para quedar como sigue:

TÍTULO SEGUNDO
DEL SISTEMA NACIONAL DE SEGURIDAD PÚBLICA

CAPÍTULO IV
De la Información Nacional sobre Seguridad Pública

25 a 43

.....

Artículo 43 bis.- El almacenamiento y respaldo de la información para el sector de la Federación, los Estados, el Distrito Federal y los Municipios que utilizan equipos de cómputo; protegerán la seguridad de los datos, con técnicas para su almacenamiento y recuperación, utilizando los recursos informáticos para garantizar la existencia y veracidad de la información en medios magnéticos u ópticos.

La información almacenada en medios magnéticos u ópticos debe contar con un documento donde se registre, si se trata de:

Archivo Maestro.- Aquél que contiene información que generalmente se toma como referencia para otros procesos.

Base de Datos.- Conjunto de datos organizados entre los cuales existe una correlación y que están almacenados con criterios independientes de los programas que los utilizan. La filosofía de las bases de datos es la de

almacenar grandes cantidades de información tal que permita las posibles consultas de acuerdo a los derechos de acceso y mediante una redundancia controlada.
Archivo Primario.- Archivo inicial o de partida que después de ser procesado generará archivos secundarios o complementarios.

Archivo Temporal.- Archivo intermedio que se genera en forma temporal que servirá para alimentar procesos intermedios y posteriores. Se trata de archivos eventuales o de corta duración.

Se Deberá Dejar especificado en el documento el nombre del sistema o aplicación, frecuencia de los procesos y la longitud del registro (tamaño del archivo).

Los medios magnéticos u ópticos (diskettes,CD's, cintas, y discos duros), deben tener etiquetas con el nombre de la aplicación, nombre del archivo, fecha de creación y si está empaquetado o no. Para el caso de las cintas magnéticas, las etiquetas deberán contener adicionalmente longitud del archivo, número de archivos, versión, nombre de la persona responsable, fecha de creación, así como especificar si es copia u original.

Artículo 43 bis I.- La información generada en un equipo de cómputo dentro de una entidad deberá ser almacenada en medios magnéticos u ópticos y por lo menos tendrán una copia de respaldo en diskettes o en otro medio de que disponga la entidad.

Deberá haber un lugar designado de manera específica por la organización para resguardar los respaldos.

La información almacenada debe ser verificada íntegramente, tanto el original como las copias (en caso de encontrarse empaquetada, desempaquetarla para su revisión), antes de ser guardada en algún lugar asignado, así como también se debe examinar que la información no esté contaminada con virus informático.

Deberá existir una copia de respaldo de los archivos, clasificandolos de acuerdo a su duración, importancia, frecuencia de actualización y función principal.

Los archivos que son textos, hojas de cálculo, gráficos, etc., mientras no se concluyan, serán guardados en una sola copia por cada actualización para facilitar su almacenamiento. Una vez concluidos se debe guardar una copia adicional de respaldo, en forma empaquetada o no, dependiendo del tamaño del archivo.

Cuando se quiera almacenar un archivo de respaldo éste deberá guardarse físicamente en otra unidad magnética (CD's, diskette, cinta o disco duro) diferente a la que contiene el archivo original, es decir, deben existir al menos dos medios magnéticos u ópticos de un mismo respaldo de información.

La información que se procesa periódicamente, se respaldará por períodos.

Entendiéndose por período, al tiempo (semanal, mensual, bimensual, trimestral, semestral, o anual) que transcurre para que se ejecute el procesamiento de la información.

En el caso de las Encuestas y Censos se deberá contar con las dos versiones de los archivos básicos:

a) La información sin imputar.

b) La información imputada (clasificada o comprometida).

Copias adicionales con la información imputada podrán ser guardadas en diferentes entidades, que garanticen el buen estado, existencia y veracidad de los archivos almacenados en medios magnéticos u ópticos.

Los lugares en donde se guarden los medios magnéticos y ópticos deben contar con una adecuada temperatura y no presentar humedad.

Los medios magnéticos y ópticos para almacenar la información deben ser nuevos (primer uso), verificándo su buen estado operacional.

Los medios magnéticos y ópticos donde está grabada la información deben recibir mantenimiento de limpieza con cierta periodicidad la cual debe ser al menos una vez al año.

Sólo el personal responsable de la integridad de la información tendrá acceso al ambiente donde se encuentren estos medios magnéticos previa autorización de la dependencia encargada por medio de un documento (nota informativa, oficio, requisición, vale, etc.), es decir sólo el personal encargado de la elaboración y procesamiento del sistema y el usuario responsable del mismo podrán acceder y usar la información que está almacenada en los medios magnéticos u ópticos.

El personal que elabora los sistemas de cómputo estimará la cantidad de medios magnéticos requeridos para las copias de los archivos de datos y de programas.

En el modo de trabajo monousuario, los usuarios son los responsables de hacer el respaldo de la información generada.

En el modo de trabajo multiusuario el responsable de hacer el respaldo de la información es el administrador de la red.

El disco duro es un medio de almacenamiento temporal de la información, el cual debe ser depurado permanentemente de los archivos que no volverán a ser utilizados en forma inmediata, así como efectuar un respaldo de toda la

información útil que se encuentra almacenada en el disco duro, dicha actividad será realizada por el responsable designado para tal fin.

En caso de que se trabaje en red o en modo multiusuario, el administrador de la red hará un respaldo de la información útil del disco duro, con cierta periodicidad que depende directamente de la organización, según lo estipule por su importancia.

Los Funcionarios o Directivos, por escrito designarán al personal responsable de realizar el almacenamiento y respaldo, en medios magnéticos u ópticos de la información necesaria que procesa su Dirección.

Los Funcionarios o Directivos de las áreas de cómputo son responsables de cumplir y hacer cumplir las normas de seguridad informática de la organización.

Artículo 44.- .....

Artículo 44 bis.- Los integrantes del Sistema Nacional de Seguridad Pública, deberán asegurar que sólo personal autorizado tenga acceso a la información clasificada como restringida o reservada, así como evitar la reproducción de la información sin la debida autorización y garantizar la integridad y autenticidad de la misma.

En los procedimientos administrativos será necesaria la identificación previa del personal que va a ingresar a las áreas de cómputo, verificando si cuenta con la autorización correspondiente y registrándo el ingreso y salida al área.

En los Sistemas Informáticos se considera necesario utilizar programas de cómputo, que cuenten con rutinas de control para el acceso de los usuarios.

Las rutinas de control, permiten que los usuarios ingresen al Sistema, previa identificación, mediante una palabra clave (password), la cual será única para cada uno de ellos; negando el acceso a las personas que no han sido definidos como usuarios del Sistema.

Las rutinas de control de acceso permitirán a los usuarios autorizados a usar determinados sistemas con su correspondiente nivel de acceso, el cual incluye la lectura o modificación en sus diferentes formas:

Lectura: obtención por parte del sujeto de la información pasiva contenida en el recurso.

Escritura: modificación de los parámetros o el contenido del recurso (creación, borrado, modificación o concatenación de ficheros).

Ejecución: utilización activa de un recurso con comportamiento propio. El caso más típico es el de las aplicaciones y programas.

Borrado: eliminación (física o lógica) de un recurso. Puede ser especificado como modo de acceso distinto al de escritura, o estar incluido en esta.

Listado: acceso a los atributos del recurso. Al igual que ocurre con el modo anterior, puede ser especificado como modo de acceso distinto al de lectura, o estar incluido en esta.

Los dos últimos modos de acceso se presentan de forma separada con mucha menos frecuencia, pero ocasionalmente el permiso de listado puede ser bastante útil para implementar aspectos particulares de algunas políticas de seguridad.

Niveles de acceso a la información:

a) Nivel de consulta de la información no restringida o reservada.

b) Nivel de mantenimiento de la información no restringida o reservada.

c) Nivel de consulta de la información incluyendo la restringida o reservada.

d) Nivel de mantenimiento de la información incluyendo la restringida o reservada.

Para garantizar estos niveles cada palabra clave tendrá asignado uno de estos niveles de acceso.

Consecuentemente la información que se considere restringida o reservada estará debidamente identificada, así como a los usuarios que accedan a ella. Cada Unidad Orgánica de Informática cuenta para ello con un Administrador de la Información, quien es responsable de la asignación de las palabras claves, de los niveles de acceso y las fechas de expiración.

La Unidad Orgánica dispondrá de un procedimiento que posibilite que las palabras claves tengan o se generen bajo un período de vigencia con base en las normas de seguridad informática de la organización.

El Jefe de cada Unidad Orgánica es responsable del acceso a la información y será quien indique las directivas adecuadas al Administrador de la Información.

Los operadores de la información restringida o reservada realizarán estrictamente lo indicado en cada procedimiento establecido de procesamiento de la información, para lo cual éstos deberán estar claramente documentados.

En una base de datos se preverá en su desarrollo garantizar un límite máximo de instalaciones (licencias autorizadas), para su uso.

Se protegerá la información clasificada como restringida o reservada encriptándola.

El software de encriptación deberá cumplir las siguientes condiciones:

a) Ser portable, es decir que funcione en todos los ambientes: computadoras grandes, mini y microcomputadoras.

b) Podrá utilizarse en cualquier lenguaje de programación.

c) Ser de fácil entendimiento por el usuario, de tal manera que permita su uso sin necesidad que éste conozca las técnicas de encriptación. Estar debidamente documentado, para ser entendible por cualquier usuario.

La protección especial de la información incluye por parte de la empresa establecer procedimientos adecuados para el control y distribución de la información impresa, así como para la grabación de los medios magnéticos u ópticos y su respectivo almacenamiento.

Artículo 45.- .....

Artículo 45 Bis.- Todo Sistema de Información diseñado por Federación, los Estados, el Distrito Federal y los Municipios pertenecerá a éstas.

Los programas deberán estar autodocumentados y utilizarán nombres que permitan su fácil identificación.

El cambio que se haga a los sistemas informáticos debe ser inmediatamente documentado.

Las pruebas que se hagan a los sistemas de información y que para ello lo hagan con datos se deberán efectuar, primero con un volumen pequeño de ellos, seguidamente se probarán con un volumen de datos aproximado al real.

Para asegurar la calidad del Sistema es necesario efectuar pruebas de verificación y validación entre el analista y el usuario.

Debe existir la compatibilidad entre los módulos individuales integrantes de los sistemas.

Llevar un control de las licencias del software comprado al proveedor especificando si las actualizaciones son independientes de la compra de dicho software, así como aclarar si el servicio de instalación viene incluido o no.

Se deberá llevar un registro ordenado y clasificado de las actualizaciones del software tanto el diseñado internamente como el adquirido al proveedor con sus respectivas licencias originales.

Se proporcionará con anticipación los cursos necesarios a los operadores de las computadoras y con la debida documentación necesaria para la ejecución de trabajos de procesamiento automático de datos, de acuerdo a las prioridades de los mismos.

El responsable de un archivo debe adoptar las medidas de seguridad, que garanticen el cumplimiento de las normas. El usuario de sistemas informáticos que disponga de una palabra clave de acceso será responsable de su mal uso, así como por otras personas no autorizadas.

El Órgano de administración correspondiente debe proveer al personal, el mobiliario e instalaciones adecuadas para almacenar los datos clasificados.

Es recomendable constituir un comité de seguridad que velará por el cumplimiento de las normas y políticas de seguridad, y que estará presidido por el jefe de cómputo u otra persona de nivel equivalente y usuarios de la información clasificada como restringida o reservada.

La designación por escrito del personal encargado de la administración de los niveles de acceso a la información y del manejo de las palabras claves, deberá ser efectuado por los Funcionarios responsables de los órganos estructurados de sistemas de cómputo.

La Unidad Orgánica correspondiente deberá contar con toda información trabajada que se considere útil y de interés institucional, para que en caso de efectuarse una auditoría, está cuente con la documentación elaborada y se ubique rápidamente en los medios magnéticos.

Artículo 45 BIS I.- Con el objeto de mantener la seguridad de los equipos de cómputo y medios magnéticos u ópticos utilizados, para garantizar la seguridad de la información disponible en medios de almacenamiento, ante contingencias naturales, siniestros o sabotaje.

Evitar la destrucción de equipos, componentes e insumos informáticos, comprende a las áreas responsables de las instalaciones, mantenimiento y uso de equipos de cómputo, así como a todo el personal que hace uso de dichos equipos.

Realizar cálculos de la carga eléctrica requerida, de los tableros de distribución, así como de los circuitos y conexiones que deben soportar la carga adicional proyectada.

Disponer de circuitos alternos y tableros de distribución eléctrica independientes a cualquier otra conexión.

Deberá disponerse de un pozo a tierra, conectado al Sistema Eléctrico que alimenta los equipos de cómputo. Asimismo se etiquetará el cableado, las extensiones y los tableros de distribución eléctrica.

Reforzar la energía eléctrica de voltaje con la ayuda de sistemas de estabilización de voltaje, (UPS).

Tener en un lugar visible los procedimientos de maniobras de encendido de emergencia.

No dejar el cableado suelto o disperso.

Deben existir puntos centrales de corte de fluido eléctrico, a nivel edificio o piso.

Se deberán tener los sistemas de agua y desagüe a niveles inferiores al Centro de Cómputo.

El Centro de Cómputo deberá contar con servicio de aire acondicionado, no se encontrará próximo a material inflamable, asimismo contará con las instrucciones de operación visibles tanto del centro de cómputo como del aire acondicionado.

Asegurar que las tomas de aire de los equipos se encuentren ubicada en zonas no susceptibles de ser obstruidas.

Se capacitará periódicamente al menos una vez al año al personal, en el uso y mantenimiento del equipo contra incendio, sistema de agua y electricidad.

Disponer de un plano que contenga todas las fuentes de suministros posibles de agua, instalación eléctrica con su capacidad estimada en cada caso.

Evitar que las paredes, pisos y techos contengan material inflamable, recomendándose instalar equipos de alarma detectores de humo.

Para combatir los incendios producidos por equipos eléctricos se deben utilizar extintores. Estos estarán al alcance inmediato, preservando la vigencia química del extintor, e identificando su localización en el respectivo plano.

Es recomendable que exista suficiente iluminación en los alrededores del edificio, las ventanas o mamparas y se protejan de manera que se evite el impacto de piedras o material incendiario.

El acceso a los centros de cómputo será restringido solo al personal autorizado, y contando con un registro de entradas y salidas de visitantes.

Las micro - computadoras y terminales tendrán un soporte logístico, que permita un apropiado mantenimiento preventivo.

El servicio de mantenimiento de los equipos de cómputo lo realizará personal especializado que garantice un buen servicio.

Contar con un plan de contingencia, así como con estrategias adecuadas para hacer frente a los desastres. Entre el área de cómputo y las demás áreas, se establecerán acuerdos acerca de las condiciones bajo las cuales el plan de contingencia ha de ser activado, considerándose la duración probable de la falta de servicio, y la pérdida (total o parcial) de la capacidad de procesamiento en una o varias instalaciones, etc.

Seleccionar organizaciones afines a la Institución y establecer con una o más de ellas convenios de mutuo apoyo, para los casos de desastres que inhabiliten el procesamiento de información. El principal criterio será la confiabilidad, también habrá que analizar la capacidad del centro de cómputo de la institución para efectuar el servicio recíproco, podría contemplar una entidad alterna espejo.

Deberá crearse un Comité de Seguridad a un nivel institucional, que vigile el cumplimiento de las normas y las políticas de seguridad de los equipos y medios de procesamiento de la información, el cual se recomienda que esté presidido por el Jefe de Cómputo u otro funcionario de nivel equivalente.

Los Funcionarios responsables, designarán por escrito, al personal custodio de la protección física de los equipos y medios de procesamiento de la información.

TRANSITORIOS

ÚNICO.- El presente Decreto entrará en vigor el siguiente día de su publicación en el Diario Oficial de la Federación."

CAPÍTULO VI

ÉTICA INFORMÁTICA

6.- ÉTICA INFORMÁTICA

Al hablar de ética necesariamente tenemos que hablar de filosofía, debido a que pertenece a esta esfera del conocimiento. La aceptación más conocida del vocablo *"ethos"* se presenta con Aristóteles donde se entendía con *"ethos"*: temperamento, carácter, hábito, modo de ser.

Algunas característica de la ética son:

- Es una disciplina filosófica.
- Su objetivo de estudio es la moral.
- Es normativa de la actividad humana en orden del bien.
- Es reflexiva, porque estudia los actos no como son, sino como deberían ser.
- Es práctica, es decir, se enfoca al campo de acción humano.

La ética tiene como objetivo de estudio la moral, esto no quiere decir que la ética crea la moral, solamente reflexiona sobre ella.

6.1 La Ética y Los Sistemas De Información

"Quizá es la tecnología, la dimensión empresarial, que despierta la conciencia ética con fuerza, en nuestros días". [Florman Informática Ética vs Competitividad http://www.geocities.com/Paris/Chateau/9164/papers/infoetica.htm].

Desde el inicio de las computadoras, cada vez más personas están relacionadas en su trabajo con las mismas, desde analistas, programadores, hasta ejecutivos y directores.

Esto nos da una muestra del impacto que ha tenido la tecnología de información en la sociedad y del papel que juega en las empresas. La tarea ética frente a las empresas es una continua tarea de rehumanización que puede realizarse a través de legislación, siempre empujada por una especial visión ética de la sociedad.

6.2 Algunas Definiciones De Ética Informática

Las personas con responsabilidades en el área de diseño o gestión de sistemas de información cada vez han de tomar más decisiones sobre problemas que no se

resuelven con lo legal y lo cuasi-legal (reglamentos, manuales de procedimiento de las empresas, etc.) sino que rozan lo ético mismo. La tarea de la EI es aportar guías de actuación cuando no hay reglamentación o cuando la existente es obsoleta. Al vacío de políticas se añade generalmente un problema de vacío conceptual. Por ello la EI también ha de analizar y proponer una marco conceptual que sea adecuado para entender los dilemas éticos que ocasiona la informática.

Otra definición la EI como la disciplina que identifica y analiza los impactos de las tecnologías de la información en los valores humanos y sociales. Estos valores afectados son la salud, la riqueza, el trabajo, la libertad, la democracia, el conocimiento, la privacidad, la seguridad o la autorrealización personal. En este concepto de EI se quieren incluir términos, teorías y métodos de disciplinas como la ética aplicada, la sociología de los ordenadores, la evaluación social de las tecnologías o el derecho informático.

Los que escriben sobre esta materia no tienen como objetivo adoctrinar o hacer proselitismo sobre una manera concreta de pensar tratando de transmitir un conjunto de valores concretos. La intención es incorporar una conciencia social relacionada con la tecnología informática y también ayudar a los informáticos a utilizar los ordenadores no-solo con eficiencia sino con criterios éticos. El objetivo es tomar decisiones sobre temas tecnológicos de manera consistente con la afirmación de los propios valores que uno profesa o con los derechos humanos en general.

El discurso ético no consiste en adoctrinar o trabajar la buena conciencia del lector o sus buenas y pías intenciones.

En conclusión, podemos afirmar que la ética en las TIC significa, en la teoría, atender a cuestiones de finalidad, cuestiones sobre la bondad de hechos y actividades, cuestiones sobre el deber ser de dichas acciones, cuestiones sobre el deber ejecutar o no ejecutar determinadas acciones en el campo de las TIC. Supone admitir como valiosas preguntas que van más allá de lo meramente técnico o instrumental. Son cuestiones muchas veces sobre los beneficiarios de las acciones. Supone tener por cierta la afirmación de que ***"el que algo sea técnicamente posible, el que algo pueda hacerse, no quiere decir que se deba hacer"***.

6.3 Algunas situaciones que presentan problemas de ética.

- Usar programas comerciales sin pagarlos.
- Usar recursos computacionales de una compañía para propósito personal.
- Hacer mal uso de la información en las compañías.

- Acceso público justo y relaciones entre los ordenadores y el poder en nuestra sociedad.
- En este apartado el problema consiste en el acceso a la información y en las cuestiones sobre justicia distributiva, igualdad y equidad. Hay que intentar definir con qué criterios podemos hablar de acceso justamente distribuido a la información, o de igualdad o inclusión en las sociedades de la información presentes y futuras.
- Intromisión no autorizada en los datos de la compañía o en los datos de la máquina de otro empleado.
- Recolectar datos de otra persona sin su autorización.
- Utilizar las computadoras para monitoreo en el desempeño de los empleados.
- Violar la primacía de software y base de datos.
- Crear virus.
- Mal uso del correo electrónico.
- Ciberpornografía.

- Amenazas a la privacidad y a la seguridad de las organizaciones.

Éste es uno de los temas más clásicos en la ética aplicada a la informática o a los sistemas de información. En este milenio que ahora comienza, uno de los elementos nuevos por medio de los cuales la intimidad de las personas estará en peligro será el motivado por el aumento de las técnicas de búsqueda o escarbo en la red (data-mining) o en las bases de datos, que va mucho más allá de las tradicionales búsquedas de información.

Toda esta serie de problemas y muchos otros más, son debido a la pérdida de valores[23] por parte de individuos, que conformamos la sociedad. Los profesionistas en informática estamos llamados a proceder con juicio recto y moral en la administración de los sistemas de información.

Los profesionales de la informática y las empresas del mundo de las TIC están desarrollando códigos deontológicos para garantizar la conducta ética en sus asociados o en sus organizaciones. Esto supone un constante reto. Elaborar un código

[23] Valores.- Se adquieren gracias a su relación con el hombre como sociedad. Desde el punto metafórico los valores según Emma Godoy, son como estrellas en el ancho firmamento de la libertad, hacia los cuales solo pueden caminar a ellas por senderos infinitos, como el arte, la ciencia y la moral; el arte se dirige hacia la belleza; la ciencia hacia la verdad; la moral hacia el bien y a estos se les denomina valores.

de ética es una tarea laboriosa y detallista. Lamentablemente muchas asociaciones profesionales y empresas creen que su tarea termina cuando consiguen presentar en sociedad un código ético propio bien elaborado mostrándose así ante sus propios países y ante la comunidad internacional como organizaciones responsables y preocupadas por la ética. Sin embargo, hoy en día hay también serios intentos de hacer ver a las asociaciones profesionales que es necesario apoyar activa y continuamente a sus asociados en sus deseos de actuar con justicia en su profesión

6.4 Ética Profesional

Todo profesionista debe contar con los siguientes conceptos:

Formación Profesional: Nuestra vida se rige por diferentes pasos que hacen de cada individuo lo que sería en el futuro, es decir, las distintas etapas de conocimiento: escuela primaria, secundaria y en último grado, la universidad, solo eso no basta, ya que esos conocimientos lo forman una generalidad de la vida y el profesional debe saber combinar esa generalidad con su formación profesional, entendiéndose por formación profesional un alto grado de conocimientos que se le inculca a un individuo de la sociedad, dotándolo de un interés particular en su profesión que se va a reflejar en su desempeño diario de la vida.

Carácter Profesional: El carácter para el individuo en su profesión se refleja desde tiempos antiguos, ellos han experimentado un progreso en todos los tipos de ciencias, han conquistado y desarrollado experimentos que tiempos atrás hubieran sido inimaginables de realizar. El profesional sin carácter puede tender a caer en un modelo usado por cientos de profesionales, puede llegar a caer en lo que sería la mediocridad, siendo éste último menos deseable para personas con aspiraciones en la vida.

El carácter no se forja con un título, se hace día a día experimentando cambios, ideas, experiencias, se hace enfrentándose a la vida; el título es como el adorno de la profesión, no importa si lo tienes lo importante es saberlo utilizar.

Vocación: La vocación es un deseo entrañable hacia lo que uno quiere convertirse en un futuro, lo que uno quiere hacer por el resto de su vida, es algo que va enlazado y determinado por tus conocimientos generales, un profesional que carezca de vocación, el proceso puede ser más tardío y difícil para poder desarrollar sus conocimientos, a diferencia de un profesional que sienta una verdadera vocación.

Orientación Profesional: Cuando una persona carezca del conocimiento o esté inseguro de la actividad que quiera realizar a nivel profesional puede solicitar ayuda a personal capacitado en orientación vocacional, que consiste en una serie de exámenes para que la persona se conozca a sí misma, para que conozca el medio social en que vive y poder indicarle de cierta forma la actividad profesional que más le conviene.

Costumbre: El código de ética de cada profesional enmarca una serie de reglas, derechos y deberes que lo limitan y mantienen al margen de caer en errores profesionales y morales, al mismo tiempo guiándolos por el buen desempeño profesional.

Un profesional conlleva consigo una serie de hábitos y costumbres que han adquirido durante toda su vida, no obstante a eso, no todo lo que uno realiza cotidianamente es correcto ante la sociedad, por lo que un profesionista debe tener la capacidad moral e intelectual para poder diferenciar lo correcto e incorrecto de su profesión, ya que ejemplos tales como: decir buenos días, tener una sonrisa en la cara, ser solidario, ser buen compañero, son puntos que no están especificados en un código y no por eso limitan al profesional a realizarlo.

Responsabilidad: El sentimiento de responsabilidad es un sentimiento personal que compromete a cada persona y le hace comprender que no puede simplemente abandonarse a sus conveniencias individuales. El concepto de responsabilidad, el sentimiento de responsabilidad nace y se desarrolla a través de los años, este sentimiento nos enseña la importancia de las cosas, a valorarlas y cuidarlas.

Un verdadero profesional es aquel que ejerce su competencia científico - técnica desde una profunda integridad personal y a la vez siempre consciente de su propia responsabilidad social. No es solo cuestión de comportarse correctamente como individuos, sino como una cuestión de justicia social.

BIBLIOGRAFÍA

Ética En Las Tecnologías De La Información Y Comunicaciones
http://paginaspersonales.deusto.es/guibert/1anales.html

Informática : Ética vs Competitividad
http://www.geocities.com/Paris/Chateau/9164/papers/infoetica.htm

Pontificio Consejo Para Las Comunicaciones Sociales Ética En Internet
http://www.vatican.va/roman_curia/pontifical_councils/pccs/documents/rc_pc_pccs_doc_20020228_ethics-internet_sp.html

Didier, C. & Dubreil, B.H. (eds) (1998), Éthique industrielle. Textes pour un débat, De Boeck Université, Bruxelles.

Johnson, D. (1997), "Is the Global Information Infraestructure a Democratic Technology?", Computers and Society, September, pp. 20-26.

Ladd, J. (1997), "Ethics and Computer World: A New Challenge for Philosophers", Computers and Society, September, pp. 8-13.

Mitcham, C. (1995), "Computers, Information and Ethics: A Review of Issues and Literature", Science and Engineering Ethics, vol. 1, pp. 113-132.

Rosenberg, R. (1998), "Beyond the Code of Ethics. The Responsibility of Professional Societies", Computers and Society, pp. 18-25.

Tavani, H.T. & Introna, L. D. (1999), "Computer Ethics: Philosophical Enquiry", Computers and Society, March, pp. 4-8.

Código de Ética de la Asociación Mexicana de la Industria Publicitaria y Comercial en Internet, A. C.(AMIPCI)
http://www.amipci.org.mx/amipci//codigo_de_ética.html

Código de Ética Profesional
http://www.cpic.or.cr/eticaf.jtm

Computer Security Management
Dennis Van Tassel
Prentice Hall, 1972

Magnaging Information Systems
Prentice Hall 1991
Mensching Adams

Ética laica y sociedad pluralista
Liga española de educación y cultura popular.
Editorial Popular. 1993

Información y Cambio
Humberto Lesca
Ediciones Gestión 2000, 1992

Ética un enfoque de procesos del pensamiento.
Rosa María Garza de Flores
Alhambra, 1993

Estrategia Competitiva
Michael Porter
CECSA, 1982

El Cambio del Poder
Alvin Toffler

CONCLUSIONES

CONCLUSIONES

El inicio de este proyecto fue a partir de la clase de Seminario llamada **"Fundamentos de Seguridad en Redes"** lo que despertó mi inquietud fue saber sobre la Legislación en nuestro México en la Protección de Datos en Tecnología de la Información y hacer referencia de la información internacional, por lo que nombré a mi tesis ***"Normatividad y Legislación Dirigida a la Protección de Datos en Tecnología de la Información"*** tema por el cual hay mucho que hacer.

De acuerdo a la recopilación de la información, me pareció importante mencionar en el trabajo de Tesis lo siguiente:

Los antecedentes de la Ley Modelo que considero de mucha importancia debido a que está dirigida a aquellos pueblos que desean unificar las políticas de Derecho Mercantil Internacional para dar valor jurídico a.los mensajes electrónicos y establecer relaciones económicas internacionales, en la que México participa.

Es importante saber y conocer quienes de las Instituciones de la Administración Pública Federal, así como las Normas en el país son atribuibles con la informática, por lo que menciono cada unas de las funciones al respecto.

De los Foros de Consulta sobre Derecho e Informática realizados en México son un paso importante, en los cuales se diagnosticaron y analizaron una serie de propuestas que se dirigieron a la Honorable Cámara de Diputados dando como resultado Reformas de Ley al Código Civil para el Distrito Federal en Materia Común y para toda la República Mexicana en Materia Federal, en el Código Federal de Procedimientos Civiles, al Código de Comercio y a la Ley Federal de Protección al Consumidor, lo que me permite manifestar que la lucha y participación en conjunto por los mismos intereses y preocupaciones en cuanto a la protección de Datos en Tecnología de la Información da como resultado avances de gran trascendencia para este país.

Por lo que es necesario un cambio cultural haciendo llegar a la sociedad en general la importancia que tiene la seguridad de la información en forma electrónica, para prevenir, impedir, detectar y corregir violaciones a la confidencialidad, autenticidad, integridad, no – repudio, control de acceso y disponibilidad de la información.

Esto se va logrando con nuestra participación en lugares estratégicos en la que de alguna manera podamos colaborar de forma más directa y manifestando de manera cotidiana en nuestro trabajo, nuestra casa y con la comunidad en general, así como también considero importante que debería existir una capacitación sobre aspectos relativos a las tecnologías de información a las autoridades que imparten la justicia.

Por lo que como mexicana, estudiante de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México y trabajadora del Secretariado Ejecutivo del Sistema

Nacional de Seguridad Pública órgano desconcentrado de la Secretaría de Seguridad Pública propongo Reformas a la "Ley General que Establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública" que se promulgó en noviembre de 1995, la cual fue entregada en Oficialia de Partes de la Honorable Cámara de Diputados el 19 de mayo de 2003, en la que manifiesto se anexen artículos referentes al Almacenamiento y Respaldo de la Información, Técnicas para la Seguridad e Integridad de la Información y Protección Física de los Equipos, esperando que sean consideradas en esta Ley, por que forman parte complementaria de la Información sobre Seguridad Pública.

Debido a la continua evolución tecnológica, se requiere de una revisión normativa para proporcionar una mayor protección a la información contenida en medios magnéticos, así como la transmisión de datos para proporcionar con mayor seguridad los servicios y prevenir los delitos cometidos a través de medios electrónicos.

Sobre esta necesidad que se tiene, me hace reflexionar que es necesario contar con leyes que nos marquen el camino correcto para un mejor desempeño en las tecnologías de la información.

Finalmente espero que mi propuesta sea considerada por los legisladores ya que es importante lograr mayor seguridad y certeza a la creación, procesamiento, almacenamiento y transmisión de datos en tecnologías de la información.

APÉNDICE A

GLOSARIO DE TÉRMINOS

APÉNDICE A

GLOSARIO DE TÉRMINOS

ACRÓNIMO.- Término formado por las primeras letras de las palabras de una expresión compuesta: OVNI Objeto Volador No Identificado.

ADMINISTRADOR DE LA RED.- Persona responsable que tiene a su cargo la gestión técnica, administrativa y operativa del sistema de redes.

ALMACENAMIENTO.- Cualquier dispositivo o medio, capaz de recibir información y retenerla durante un periodo de tiempo, permitiendo su extracción (recuperación) y empleo cuando sea necesario.

ARCHIVO.- Conjunto de registros que guardan relación. Al registro se le puede considerar como la información básica a la que se puede acceder en bloque y al archivo como una organización de los registros. Porción de memoria auxiliar normalmente en disco ocupada por un conjunto homogéneo de información (datos o programa).

ARCHIVO EMPAQUETADO.- Información (datos o programas) que ha sido comprimida a fin de obtener una óptima utilización de la memoria del ordenador.

ARCHIVO MAESTRO.- Es aquél que contiene información que permanece más o menos estable, la cual generalmente se toma como referencia para otros procesos.

ARCHIVO PRIMARIO.- Archivo inicial o de partida que después de ser procesada generará archivos secundarios o complementarios.

ARCHIVO TEMPORAL.- Archivos intermedios que se generan en forma temporal que servirán para alimentar procesos intermedios y posteriores. Son archivos eventuales o de corta duración.

ARQUITECTURA DE LA INFORMACIÓN.- Concepto que describe el conjunto de estructuras que modelan el manejo de la información dentro de una organización.

ARQUITECTURA FÍSICA.- Procesadores, CPU, dispositivos periféricos, estaciones de trabajo, capacidad de memoria, capacidad de disco, comunicaciones, velocidad de reloj.

ARQUITECTURA LÓGICA.- Formada por el software de sistemas (sistema operativo, programas de control de redes, generador de aplicaciones, administradores de bases de datos, herramientas CASE, procesadores de texto, hojas de cálculo, graficadores) y el software de aplicación (programas que procesan datos de acuerdo a los requerimientos del usuario).

BASE DE DATOS.- Conjunto de datos organizados entre los cuales existe una correlación y que están almacenados con criterios independientes de los programas que los utilizan. La filosofía de las bases de datos es la de almacenar grandes cantidades de información tal que permita las posibles consultas de acuerdo a los derechos de acceso y mediante una redundancia controlada.

CAMPO.- Espacio en la memoria para almacenar temporalmente un dato durante el proceso: su contenido varía durante la ejecución del programa. Un campo numérico sólo puede almacenar valores (dígitos) y un campo alfanumérico cualquier carácter (dígito,letra,símbolo especial). Una combinación de campos constituye un registro.

CONCERTAR.- Pactar, ajustar, acordar.

CONCILIAR.- Poner de acuerdo a dos doctrinas, a dos personas.

CONSISTENCIA.- Acción que permite detectar anomalías en los datos de un registro que se procesa y que generalmente se informa mediante impresión.

CRIMEN.- Acción punible que la Ley castiga o condena. Acto, Delito grave, o acción reprobable.

DELITO.- Crimen, quebrantamiento de la Ley. Acción u omisión prohibida bajo amenaza de una pena. Es un concepto que varía a través del tiempo. Según los países y en relación a las múltiples legislaciones vigentes. La acción delictuosa se considera voluntaria, a no ser que conste expresamente lo contrario. Los diferente tipos de delitos.

DEONTOLOGÍA.- (del gr. Deón, déontos significa obligación, deber, y lógos, logía expresa conocimiento, estudio, tratado). Ciencia o tratado de los deberes. Deontología hace referencia a la ciencia del deber o de los deberes. "Conjunto de reglas de carácter ético que una profesión se da a sí misma y que sus miembros deben respetar.

DERECHO.- Conjunto de normas sociales establecidas por la autoridad, que al mismo tiempo vela por su aplicación.

DIAGRAMA DE CONTEXTO.- Muestra la relación existente entre la Institución y su entorno (sectores públicos, privados, organismos internacionales, entre otros), así como los requerimientos de información (proporcionada por las fuentes) y la información producida por ésta (empleada por los usuarios).

ENTIDAD.- Es todo objeto sobre el cual la Institución pueda almacenar datos y cuyo propósito está claramente definido.

ESPECTRO RADIOELÉCTRICO.- Serie ordenada de todas las frecuencias o longitudes de onda utilizadas en radio, radar, televisión, teléfonos celulares, telecomunicaciones.

FOMENTO.- Disposición u oportunidad para hacer o lograr una cosa.

GLOBALIZACIÓN.- la "globalización" es una nueva fase del desarrollo del capitalismo.

La "globalización" no es un fenómeno abstracto, sino la concentracion de las comunicaciones, mercados financieros, culturales, sociales, etc, a nivel mundial.

HABEAS DATA.- De acuerdo al Derecho Comparado, el Hábeas Data es una garantía que protege derechos como la honra, buena reputación, intimidad y derecho a la información. "Es un remedio urgente para que las personas puedan obtener el conocimiento de los datos a ellos referidos, y de su finalidad, que conste en el registro o banco de datos públicos o privados y en su caso para exigir la supresión, rectificación, confidencialidad o actualización de aquellos", según la reglamentación en países donde ha empezado a funcionar.

INFORMACION HISTORICA.- Se refiere a información pasiva o de poco movimiento, que por lo general se almacena en medios magnéticos como por ejemplo, cintas magnéticas.

JURÍDICO.- que atañe al Derecho, justicia y a las leyes

LEGAL.- Verídico, puntual, fiel y recto en el cumplimiento de las funciones de su cargo.

LEY.- Regla y Norma constante e invariante de las cosas. Precepto dictado por la suprema autoridad, en que se manda o prohíbe una cosa. Reglamentación social del estado escrita y promulgada, cuyo incumplimiento lleva aparejada la posibilidad de una sanción o la ejecución obligatoria de lo señalado. La Ley es, pues, un mandato o prohibición de carácter exclusivamente normativo. Traza pautas en las conductas y relaciones sociales pero su cumplimiento no es automático ni ocurre necesariamente.

LONGITUD DE REGISTRO.- Número de bytes o de caracteres que forman un registro. Se tiene registros de longitud fija, cuyo tamaño en palabras o caracteres es constante, debido a las necesidades del equipo físico o a una programación especifica y, registros de longitud variable en las cuales la longitud puede variar dentro de ciertos límites prescritos de acuerdo con las necesidades de los datos.

MEDIOS MAGNETICOS.- Son dispositivos que permiten el almacenamiento de programas e información. En todos los dispositivos que componen este grupo, el soporte magnético tiene la misma estructura y composición. Están formados por una base de material y formas variables, sobre las que se ha depositado una delgada capa de material magnetizable.

El registro de información se realiza mediante equipos dotados de una cabeza de grabación, el cual dispone de una bobina que produce un campo electromagnético creando por inducción zonas puntuales magnetizables sobre el soporte utilizado. Los elementos más representativos de los medios magnéticos son los discos y cintas magnéticas, siendo el primero un medio de acceso seudoaleatorio y el segundo, un medio de acceso secuencial.

MEDIOS OPTICOS.- Son dispositivo de almacenamiento para grandes sistemas electrónicos de archivos (programas e información) . Dentro de ellos se encuentran el CD-ROM que son discos con información pregrabada y que sólo pueden ser leídas; WORM que permiten grabar información que se desee pudiendo ser leída cuantas veces sean necesario; y el EOD que son discos ópticos borrables o reescribibles y que son de reciente aparición.

MODELO CONCEPTUAL DE DATOS.- Se realiza con la finalidad de determinar las Bases de Datos corporativas que van a funcionar en la Institución, para ello se definirán en primer lugar las entidades, las cuales agrupadas darán origen a las Bases de Datos Corporativas.

MODELO DE DATOS.- Es la descripción de la organización de una Base de Datos, constituyéndose en una representación gráfica, orientada a la obtención de la estructura de datos mediante métodos. Representa las relaciones entre las entidades.

MODELO ENTIDAD – RELACIÓN.- Un modelo de datos que describe atributos (campos) de entidades y relaciones entre ellos.

MODELO GLOBAL DE DATOS.- Es la representación gráfica de las diferentes aplicaciones propuestas quienes a su vez, apoyarán funcionalmente al logro de los objetivos de la Institución. El modelo global de datos, permite la visualización de la interrelación de los sistemas, con las posibles Bases de Datos o grupos de entidades.

MÓDULO.- Es un componente autónomo de software o hardware que interactúa con un sistema mayor. Los módulo de programas se diseñan para manejar una tarea específica dentro de un programa mayor. Los módulos de hardware se hacen a menudo para incorporarlos al sistema principal.

MULTIUSUARIO.- Sistema de transmisión de datos que permite compartir recursos de información a través de un ordenador.

MONOUSUARIO.- Un solo usuario.

NORMA.- Regla general que pretende ordenar un grupo social según un determinado sistema de convivencia civil. La norma jurídica es obligatoria, y en muchos casos el poder político que rige la comunidad llega a imponerla por la fuerza. Pero la norma jurídica, en la práctica viva, puede además de ser transgredida caer en desuso, ser ignorada e incluso deformada como consecuencia de las transformaciones de la vida del Derecho y, concretamente de las leyes.

OBRANTE.- Ejecutar o realizar una cosa no material. Causar algún efecto.

PERITO.- El que, poseyendo especiales conocimientos teóricos o prácticos, informa, bajo juramento al juzgador sobre puntos litigiosos en cuanto se relacionan con su especial saber o experiencia.

PLAN ESTRATÉGICO.- Contempla la misión, políticas, objetivos y estrategias de la Institución, las cuales están orientadas a reducir costos y obtener ventaja competitiva.

POLÍTICA.- Arte, doctrina u opinión referente al gobierno de los Estados. Arte de conducir un asunto para alcanzar un fin. (cortesía, sinónimo de Urbanidad).

PUNIBLE.- Que merece castigo.

REFORMA.- Lo que se propone, proyecta o ejecuta como innovación o mejora en alguna cosa.

SISTEMA DE INFORMACIÓN.- Se denomina Sistema de Información, al conjunto de procedimientos manuales y/o automatizados, que están orientados a proporcionar información para la toma de decisiones.

TECNOLOGÍA.- Sistematización de los conocimientos y practicas aplicables a cualquier actividad, y más corrientemente a los procesos industriales. La tecnología es una disciplina relativamente moderna que utiliza los métodos de la Ciencia y la Ingeniería, en contraste con el conjunto de reglas empíricas que constituían las técnicas y oficios anteriores a la Revolución Industrial.

TELECOPIA.- correo electrónico o Telefacsímil.

TIPIFICAR.- Adaptar algo a un tipo o norma común.

USUARIO.- Cualquier persona que utiliza una computadora. Por lo general se refiere a las personas que no pertenecen al personal técnico y que proporcionan entradas y reciben salidas de la computadoras.

VALIDACION.- Verificación que ejecuta un programa para comprobar que la información procesada cumple ciertas condiciones. Comprobación que tiene por objeto asegurarse que los datos queden comprendidos dentro de ciertos límites prescritos.

Cualquier operación que se realice para comprobar la validez o la exactitud de un operando o de un resultado. El proceso de datos requiere comprobación de la máquina y la del personal de la oficina. Las comprobaciones por medio de la máquina pueden programarse especialmente o ser ejecutadas automáticamente por los componentes físicos.