“COMPENDIO LEGISLATIVO SOBRE SEGURIDAD INFORMÁTICA EN MÉXICO”

SEGURIDAD EN LAS TECNOLOGÍAS DE INFORMACIÓN

MAESTRIA EN TECNOLOGÍAS DE INFORMACIÓN

CATEDRÁTICO: MISAEL TORRES ALCANTARA

ALUMNO: MARTÍN ERNESTO TOVAR ORTIZ

CUARTO CUATRIMESTRE

DICIEMBRE 2007

ÍNDICE

RESUMEN

El uso de los medios electrónicos informáticos como la Internet y redes de comunicaciones es algo que se ha masificado en México en las diferentes áreas de Gobierno, Educación, Investigación, Salud, Comercio e Industria.

En cualquier sociedad un pequeño porcentaje de la gente es maliciosa. Se estima que Internet tiene 40 millones de usuarios. Aún si el porcentaje de usuarios maliciosos es menor al 1% de esta sociedad, el número de usuarios maliciosos es tan grande que debería ser preocupante.

La aparición y expansión de Internet conjuntamente con los sistemas informáticos, han hecho posible la realización de tareas impensables hasta hace unos años: transacciones bancarias, resolución de problemas complejos, control, docencia, comercio electrónico, etc.

A medida que los sistemas de información son más complejos, han puesto de manifiesto una mayor cantidad de puntos vulnerables debido a que el número de posibles atacantes crece muy rápidamente, los medios disponibles para efectuar ataques siguen una evolución tan rápida como los propios sistemas y la generalización de Internet hace que los ataques puedan provenir de cualquier lugar.

Por lo anterior, es importante, y por demás urgente, contar con un esquema jurídico informático para implantar esquemas de seguridad robustos, para que la seguridad se concrete a mecanismos tecnológicos vulnerables en menor o mayor grado a los riesgos inherentes al uso de tecnología informática.

Se requiere promover el reconocimiento jurídico en temas como la confidencialidad de la información, la protección de la intimidad de las personas usuarias de la tecnología y la validez de documentos electrónicos, entre otros.

En este compendio se analiza hasta donde hemos llegado en México en materia legislativa informática y lo que nos falta por hacer, cabe mencionar que la información estará disponible en Internet en algunos foros y sitios web colaborativos

ABSTRACT

Use of computer electronic means like internet and local communication nets is a topic set in México in several government, education, researching, health, commerce and industry areas.

In any society, there is a little portion of malicious people. It is estimated internet has forty millions of users. Even if the percentage of malicious user is less than 1% in this portion; talking about numbers, that kind of users is so big, which should be a preoccupation.

Apparition and expansion of internet, in joint with data processing systems, have made possible the reachment of unimaginables jobs even till some little years ago: banking movements, complex trouble resolutions, control, teaching-learning, electronic trade, etc.

A measure that data processing systems are more complex, they have put in knowledegement a growing number of vulerable points due to the hackers are increasing fastly, available means to attack are having a quick evolution like the systems by themself do it and the wide use of internet makes the attacks may come from any place.

For that reason, it is important and urgent; to get a data processing legal scheme to implement hard safety systems and asure, against inherent risks to its use, to the vulnerable technological mechanisms, rather in minor or major grade they can be.

It is mandatory to promote the juridical recognition over confidentiality, and privac y of people uses this technology and the true certification of electronic documents, among others.

In this context, it is analyzed till where we have arrived in mexico into data processing legal matter and we have to do even more; it is necesary to mention this information will be available in internet in some forums and colaborating web sites.

INTRODUCCIÓN

Los delitos informáticos constituyen una gran laguna en nuestras leyes penales, existe una gran lista de los delitos que no están contemplados en el Código Penal y que requieren análisis urgente en donde se involucre a penalistas, académicos, legisladores, especialistas, medios de comunicación, instituciones educativas, iniciativa privada, etc.

En México el Internet no se ha regulado de manera expresa, como tampoco en el resto de los países latinoamericanos, su uso gira en torno a cierto Código Ético.

En cualquier sociedad, un pequeño porcentaje de la gente es maliciosa. Se estima que Internet tiene 40 millones de usuarios. Aún si el porcentaje de usuarios maliciosos es menor al 1% de esta sociedad, el número de usuarios maliciosos es tan grande que debería ser preocupante.

A pesar de los índices de crecimiento del uso de la computadora y de Internet, México enfrenta un problema social consistente en el llamado analfabetismo informático, del cual el Poder Legislativo y el gobierno en general no están exentos, por lo que muchos congresistas y funcionarios públicos no entienden el concepto y la estructura de Internet. En igual circunstancia se encuentra el poder Judicial, tanto los jueces como los magistrados tienen la misma carencia, por lo cual no se tiene conocimiento de la existencia de tesis ni jurisprudencia alguna que se refieran a los medios electrónicos en general y a Internet en especial.

Como se mencionó es un Código Ético el que actualmente regula la conducta de los usuarios, mas sin embargo, existe en nuestro país una regulación administrativa sobre las conductas ilícitas relacionadas con la informática, pero que aún no contemplan en sí los delitos informáticos.

Es un hecho innegable que el avance desbordante de la tecnología en materia informática y el desarrollo de las nuevas Tecnologías de Información y Comunicación (TIC) han excedido con mucho las expectativas más ambiciosas, pero sobretodo y como consecuencia de ello, han propiciado una serie de conductas, actos y hechos que inciden de manera trascendente en la vida social, económica, familiar, comercial, laboral, profesional, política, científica, y en general en todos los ámbitos sociales. Y es ahí donde el Derecho, como regulador de las conductas del hombre en sociedad, debe intervenir en tiempo y forma para evitar que los delitos informáticos escapen de control legal manteniéndose al margen del

Derecho mientras generan una serie de situaciones que necesariamente afectan de manera importante la vida de las personas y del Estado.

El desarrollo y aplicación de los avances informáticos llevan una inercia y una velocidad que los han hecho casi inalcanzables, en donde el sistema jurídico mantiene un proceso legislativo demasiado lento.

Dado el creciente uso de medios electrónicos informáticos como lo es Internet y redes de comunicaciones, es importante conocer el panorama jurídico actual y el desarrollo en otros países con realidades tecnológicas o tendencias a las que se acerca México, incluyendo los delitos a través de estos medios.

OBJETIVO

El presente trabajo pretende realizar una recopilación de varios autores con respecto al tema poco explorado sobre la legislación informática en México y el mundo, el cual presenta un rezago considerable, así como proponer a grandes rasgos las políticas de seguridad a implementar y que hoy por hoy resultan inaplazables, además de poderla transcribir en un concepto integral, a diversos foros y sitios web colaborativos para que quede a disposición de todos los usuarios interesados en el tema.

MARCO TEÓRICO

- **SEGURIDAD INFORMÁTICA**

La seguridad informática es un conjunto de procesos, procedimientos, tareas y actividades implementados conjuntamente con elementos de computación y telecomunicaciones para controlar y proteger contra amenazas que pongan en riesgo los recursos informáticos (información, equipos, etc.) ubicados en un sitio específico, durante su estadía en un medio de almacenamiento o durante su transmisión, en sus aspectos de integridad, disponibilidad, confidencialidad y autenticidad.

En seguridad informática, se pueden pensar en tres momentos diferentes para realizarla:

Prevenir. Consiste en evitar que un ataque tenga éxito, a esta categoría pertenecen todas las acciones que se realicen en la organización tendientes a no permitir que ocurra un incidente de seguridad.

Detectar. Cuando no es posible o no se desea prevenir un ataque, es posible que lo que se busque sea darse cuenta de que está recibiendo un ataque durante el mismo momento en el que se está presentado, en este caso lo que se desea es detectar el ataque para así tomar acciones al respecto.

Recuperar. La tercera y última alternativa es recuperar, en este caso, ya se ha realizado el ataque. Lo que se debe realizar es una revisión de lo que aconteció y tratar de poner en producción nuevamente todos los sistemas afectados, para lo cual se cuenta con dos alternativas:

- Parar el ataque (evitar que continúe) y entrar a reparar cualquier daño causado por el ataque
- Continuar la operación normal e ir defendiéndose del ataque.

Los requerimientos básicos de seguridad son disponibilidad, integridad, confidencialidad o privacidad y autenticidad.

Disponibilidad: Es la garantía de que la información será accesible por los usuarios a los servicios de la red según su perfil en el momento requerido y sin degradaciones.

Integridad: Tiene que ver con la protección que se da a los activos informáticos para que solo puedan ser modificados por las personas autorizadas.

Confidencialidad o Privacidad: Propiedad o requerimiento de la seguridad que exige que la información sea accedida por cada usuario en razón de su área del negocio.

Autenticidad: Propiedad fundamental de la información de ser confrontada en cualquier momento de su ciclo de vida contra su origen real (Verdadero/falso).

- DELITOS INFORMÁTICOS

Los delitos informáticos constituyen una gran laguna en nuestras leyes penales, así pues, el derecho comparado nos permite hacer una lista de los delitos que no están contemplados en el Código Penal y que requieren análisis urgente por parte de nuestros académicos, penalistas y legisladores.

Delito informático lo podemos definir como todo ilícito penal llevado a cabo a través de la utilización de medios informáticos y que está estrechamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes.

Los delitos informáticos son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)"[1]. Por su parte, el tratadista penal italiano Carlos Sarzana, sostiene que los delitos informáticos son "cualquier

[1] Julio Tellez Valdez

comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo".

Según Téllez Valdez, este tipo de acciones presentan las siguientes características:

- Son conductas criminales de cuello blanco, 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, este autor clasifica a estos delitos, de acuerdo a dos criterios:

1. Como instrumento o medio y
2. Como fin u objetivo.

- POLITÍCAS DE SEGURIDAD

Podemos definirlo como el conjunto de normas, reglas y principios que gobiernan una identidad u organismo, en donde cada regla define una acción, mecanismo y/o procedimiento con el objetivo de lograr la seguridad, orden y buen uso de los sistemas de

información, especifican también las condiciones, derechos y obligaciones sobre el uso de los sistemas de cómputo.

Las Políticas de Seguridad nos ayudan a prevenir la pérdida de la información, tener un uso adecuado y eficiente de los sistemas de cómputo y de las telecomunicaciones, así como una forma de poder ir a la par con la tecnología y una respuesta a la falta de legislación informática.

Ventajas de las Políticas de Seguridad:

- Ayudan a la adquisición del HW y del SW.
- Permiten actuar a las autoridades en el caso de una violación de la seguridad.
- Permite tener procedimientos para eventualidades y para llevar acabo una auditoria
- Evitar la excusa llamada ignorancia

Para desarrollar políticas de manera integral debemos primeramente detectar claramente la problemática para estar en posición de sensibilizar a todos los involucrados, para esto debemos responder a las siguientes preguntas:

¿Qué se debe de proteger?¿Contra qué se debe de proteger?¿Qué tipo de usuarios se tienen? ¿Quién debe de poder usar los recursos?¿Quién debe tener privilegios de administrador? ¿Cómo debe de manejarse la información sensible?

- **DEFINICIÓN DE LEGISLACIÓN INFORMÁTICA**

Se define como el "conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática"[2].

Su aplicación en los campos actuales del derecho en la Informática se da en la protección jurídica de la información personal, la protección jurídica del software, el flujo de datos fronterizo, los convenios y/o contratos informáticos, los delitos informáticos y el valor probatorio de los documentos electromagnéticos entre otros.

Es preciso mencionar también el siguiente concepto: "Es el conjunto de estudios e instrumentos derivados de la aplicación de la Informática al Derecho, o más precisamente, a los procesos de creación, aplicación y conocimiento del Derecho"[3].

[2] Dr. Julio Tellez
[3] Dr. Hector Fix Fierro

- **TIPOS DE DELITOS INFORMÁTICOS RECONOCIDOS POR LA ORGANIZACIÓN DE LAS NACIONES UNIDAS**

Las conductas o acciones que considera las Naciones Unidas como delitos informáticos son las siguientes:

1) Los Fraudes cometidos mediante manipulación de computadoras
2) La manipulación de programas
3) La Manipulación de datos de salida
4) Fraude efectuado por manipulación informáticas de los procesos de cómputo.
5) Falsificaciones informáticas
6) Como instrumentos
7) Sabotaje Informático
8) Los Virus
9) Los Gusanos
10) La Bomba lógica o cronológica
11) Acceso no autorizado a servicios u sistemas informáticos
12) Piratas Informáticos o Hackers
13) Reproducción no autorizada de programas informáticos de protección legal

- **LA OMPI (ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL) COMO ORGANISMO RECTOR**

La Organización Mundial de la Propiedad Intelectual (OMPI) es un organismo especializado del sistema de organizaciones de las Naciones Unidas. Su objetivo es desarrollar un sistema de propiedad intelectual (P.I.) internacional, que sea equilibrado y accesible y recompense la creatividad, estimule la innovación y contribuya al desarrollo económico, salvaguardando a la vez el interés público.

Se estableció en 1967 en virtud el Convenio de la OMPI, con el mandato de los Estados miembros de fomentar la protección de la propiedad intelectual en todo el mundo mediante la cooperación de los Estados y la colaboración con otras organizaciones internacionales. Su Sede se encuentra en Ginebra (Suiza).

El Comité Permanente de Tecnologías de la Información (SCIT), creado por los Estados miembros de la OMPI en 1998, constituye el foro que brinda orientación de política y asesoramiento técnico en todo lo relacionado con la estrategia de la OMPI en materia de tecnologías de la información, con inclusión de las normas técnicas de la OMPI y los

aspectos relativos a la documentación sobre propiedad intelectual. El Comité está compuesto por todos los Estados miembros de la OMPI y por observadores.

Tras la adopción de la nueva estructura en su reunión de enero de 2001, el SCIT cuenta ahora con dos grupos de trabajo subsidiarios, el Grupo de Trabajo sobre Proyectos de Tecnologías de la Información y el Grupo de Trabajo sobre Normas y Documentación.

El sector del sitio Web de la OMPI correspondiente al SCIT no solamente contiene enlaces a toda la documentación de las reuniones, sino que también proporciona acceso a información relacionada con los informes anuales técnicos.

- **COMPARATIVA LEGISLATIVA CON OTROS PAÍSES**

LEGISLACION EN OTROS PAISES.

ALEMANIA. Para hacer frente a la delincuencia relacionado con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos:

Espionaje de datos, estafa Informática, falsificación de datos probatorios, alteración de Datos, sabotaje Informático, utilización abusiva de cheques o tarjetas de crédito.

Alemania también cuenta con una Ley de Protección de Datos, promulgada el 27 de enero de 1977.

AUSTRIA. Ley de reforma del Código Penal del 22 de diciembre de 1987, la cual contempla los siguientes delitos:

Destrucción de Datos (126). Estafa Informática.(148).

CHILE. Cuenta con una ley relativa a Delitos Informáticos, promulgada en Santiago de Chile el 28 de mayo de 1993.

ESTADOS UNIDOS. Cabe mencionar, la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030). Dicha acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año de prisión.

ITALIA. En un país con importante tradición criminalista, como Italia, nos encontramos tipificados en su Código Penal los siguientes delitos:

Acceso Abusivo. Se configura exclusivamente en caso de sistemas informáticos y telemáticos protegidos por dispositivos de seguridad (contraseñas o llaves de hardware). La comisión de este delito se castiga con reclusión de hasta tres años, previendo agravantes.
Abuso de la calidad de operador de sistemas. Introducción de virus informáticos. Fraude Informático. Falsificación informática.
Así también tenemos:
Abuso fraudulento en el procesamiento de información (Austria, Japón). Daño de equipo de cómputo y uso ilegal de equipo de cómputo (Japón). Lucrar utilizando inadecuadamente bases de datos (Japón, Nueva Zelanda). Sabotear negocios ajenos (Japón). Piratería y adquisición ilegal de programas (Francia, Alemania, Japón, Escocia, Gran Bretaña, El Salvador). Fraude o robo de información confidencial y programas (Francia, Gran Bretaña, Austria, Suiza, Japón, Estados Unidos). Alteración de programas (Japón, Gran Bretaña). Regulación de delitos informáticos (Chile LEY 19223, y como proyecto en El Salvador). Proyecto de legislación para proteger la intimidad, dignidad y autodeterminación de los ciudadanos frente a los retos que ofrece el procesamiento automatizado de datos personales (Costa Rica).

- **LEGISLACIÓN EN MÉXICO**

Las Instituciones de la Administración Pública Federal con atribuciones vinculadas con la informática son:
• Secretaría de Gobernación
• Secretaría de Relaciones Exteriores
• Secretaría de Hacienda y Crédito Público
• Secretaría de Economía
• Secretaría de Comunicaciones y Transportes
• Secretaría de Contraloría y Desarrollo Administrativo
• Secretaría de Educación Pública
• Comisión Federal de Telecomunicaciones
• Consejo Nacional de Ciencia y Tecnología
Las Leyes relacionadas con la seguridad informática se enumeran a continuación:
• Ley Federal del Derecho de Autor
• Ley de la Propiedad Industrial

• Ley Federal de Telecomunicaciones

• Ley de Información Estadística y Geográfica

• Código Penal Federal

• Código Federal de Procedimientos Civiles

• Código de Comercio

• Ley Federal Contra la Delincuencia Organizada

• Código Civil Federal

• Ley Federal del Trabajo

• Código Fiscal de la Federación

• Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental

• Ley del Mercado de Valores

• Ley Federal de Protección al Consumidor

Las principales iniciativas jurídicas en México a la fecha son:

- En materia informática

22 de marzo del 2000 en Materia de delito informático

- En materia de correo electrónico

28 de abril de 1999

15 de diciembre de 1999

22 de marzo del 2000

Proyecto Norma Oficial Mexicana

PROY-NOM-151-SCFI-2001

- Protección de datos personales

14 de febrero del 2001: Ley Federa de Protección de Datos Personales

Reformas al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.

- **TENDENCIAS INTERNACIONALES DE LA INFORMÁTICA Y EL DERECHO**

Dentro de la evolución que ha tenido en los últimos años la materia, podemos establecer claramente tendencias en el ámbito internacional, que se tienen en los distintos países del mundo, respecto del desarrollo de la informática y el derecho; de esta manera podemos enumerar las siguientes tendencias: inicial o básica, progresiva o creciente, avanzada o próspera y culminante o innovadora.

A) Tendencia Inicial o Básica: 1) Poco avance y desarrollo de la informática jurídica y del derecho informático, debido a la escasa importancia dada a la materia por los profesores de derecho de las Universidades y también por los funcionarios del Gobierno. 2) Se empieza a promover que se incluya la materia de informática jurídica en los planes de estudio de las facultades de derecho, (se estudia al derecho informático, dentro de la informática jurídica).

B) Tendencia Creciente o Progresiva: 1) Distinción clara entre informática jurídica y derecho informático, como ramas totalmente independientes una de la otra, pero relacionadas entre sí. 2) Consideración del derecho informático como rama autónoma del derecho; incluyéndose en los planes de estudio de las principales facultades de derecho del país, de manera separada a la materia de informática jurídica.

C) Tendencia Avanzada o Próspera: 1) Destaca la necesidad e importancia de desarrollar la labor legislativa respecto al derecho informático. 2) Desarrollo y consolidación importante de la legislación.

D) Tendencia Culminante o Innovadora: 1) Avances importantes en respecto de la informática jurídica meta documental, auge de centros de investigación para la utilización de sistemas de inteligencia artificial aplicados al derecho, desarrollo de tesis doctórales relativas a la inteligencia artificial y el derecho. 2) Desarrollo de proyectos prácticos y específicos de utilización de la inteligencia artificial aplicados al derecho.

- **TENDENCIA ACTUAL DE LA INFORMÁTICA Y EL DERECHO EN MÉXICO**

En este orden de ideas, pudiéramos establecer que México, se encuentra actualmente pasando de la tendencia inicial o básica a la tendencia creciente o progresiva, debido a que se empieza a incluir en las Facultades de Derecho del país, a la informática jurídica y se empieza a analizar, aunque de manera incipiente, la conveniencia de separar en el plan de estudios de las facultades de derecho, a ambas materias, es decir, la informática jurídica y el derecho informático como ramas independiente y se empieza a desarrollar la doctrina nacional sobre la materia.

- **CONCLUSIONES Y RECOMENDACIONES**

Una legislación informática permite implantar esquemas de seguridad robustos y eficientes. Es verdad que existen adaptaciones de algunas leyes al ámbito computacional y tecnológico como Derechos de autor, Protección industrial y Regulación de las comunicaciones entre otros, pero también la inexistencia de legislación en cuanto a: Tipificación de delitos

informáticos, uso ilícito del equipo de cómputo y de Telecomunicaciones, seguridad jurídica en el uso de medios electrónicos, reconocimiento legal de las transacciones, electrónicas, etc.

La seguridad en cómputo no es un lujo, es un esfuerzo en conjunto donde deben de participar diversos actores, especialistas, empresarios, legisladores, funcionarios públicos e instituciones de los tres órganos de gobierno. Cabe hacer mención que el 50% de los incidentes son internos por eso, las políticas es una manera de ir un paso adelante de la legislación, son únicas por cada organización y garantizan una enorme reducción del riego de la información.

Es por todo esto que se hace urgente que el poder legislativo en México redacte e implemente leyes en materia de seguridad informática, asimismo, es necesario que a la seguridad informática en México se le de la importancia que se requiere, por lo cual es conveniente que existan más escuela en nuestro país a nivel profesional que formen y capaciten al alumnado en materia de seguridad informática. Falta mucho por hacer es cierto, pero los avances son significativos y todos los que de una forma u otra nos vemos involucrados día con día en materia de informática, debemos hacer un esfuerzo extra para impulsar una legislación integral que nos garantice la salvaguarda de la información y el respeto a la privacidad, el no hacerlo podría ocasionar un nuevo tipo de impunidad, "La impunidad Informática".

- **CREACIÓN DE LA FIGURA DEL OSI(Oficial de Seguridad Informática)**

Por último haremos la recomendación de la creación de la figura del OSI bajo el siguiente esquema.

Definición

El Oficial de seguridad informática (OSI), es la persona responsable de planear, coordinar y administrar los procesos de seguridad informática en una organización.

Misión

El Oficial de seguridad informática tiene la función de brindar los servicios de seguridad en la organización, a través de la planeación, coordinación y administración de los procesos de seguridad informática, así como difundir la cultura de seguridad informática entre todos los miembros de la organización.

Objetivos

- Definir la misión de seguridad informática de la organización en conjunto con las autoridades de la misma.
- Aplicar una metodología de análisis de riesgo para evaluar la seguridad informática en la organización.
- Definir la Política de seguridad informática de la organización.
- Definir los procedimientos para aplicar la Política de seguridad informática.
- Seleccionar los mecanismos y herramientas adecuadas que permitan aplicar las políticas dentro de la misión establecida.
- Crear un grupo de respuesta a incidentes de seguridad, para atender los problemas relacionados a la seguridad informática dentro de la organización.
- Promover la aplicación de auditorias enfocadas a la seguridad, para evaluar las prácticas de seguridad informática dentro de la organización.
- Crear y vigilar los lineamientos necesarios que coadyuven a tener los servicios de seguridad en la organización.
- Crear un grupo de seguridad informática en la organización.

REFERENCIAS Y ENLACES

Internet y Derecho en México Edit. Mc Graw Hill, México 1997.
Barrios Garrido, Gabriela

Derecho Informático, Edit. Mc Graw-Hill Segunda Edicion/1996

Ingeniera Claudia Santiago C. *Centro de Estudios de Telemática. Escuela Colombiana de Ingeniería Julio Garavito. 2005*
http://www.citel.oas.org/newsletter/2005/septiembre/seguridad_e.asp

Delitos informáticos. 2004
http://www.wikilearning.com/delitos_informaticos-wkccp-2204-1.htm

Legislación de la Informática. Delitos Informáticos.
Universidad Autónoma de Chihuahua, Facultad de Ingeniería. 2001.
http://www.fing.uach.mx/MatDidactico/Legislacion/desarrolla.htm

La Importancia de la Seguridad Informática: Las políticas y la Legislación.
M. Farias-Elinos. Lab. de Investigación y Desarrollo de Tecnología Avanzada (LIDETEA)
Universidad La Salle. México. 2004.

Organización Mundial de la Propiedad Intelectual (OMPI). ONU. 2007.
http://www.wipo.int/about-wipo/es/what_is_wipo.html

Fuentes: Sria. Gobernación, SFP, Derechos de Autor, Profeco, IFAI, ONU