EL REGIMEN JURIDICO DE LA SEGURIDAD INFORMATICA EN EL SISTEMA EMPRESARIAL CUBANO. UNA VISION ACTUAL

MSc. Rogelio Meléndez Carballido

MSc. Manuel José Pérez Calderón

ABSTRACT

One of the main juridical goals of some improving- system enterprises is the application of diferent software security control rules held by some institutions of the province.

This work focuses on a comparative analysis between Cuban and international software security rules, as well as on the consequences of its application.

Some empiric and theorical methods were applied to deepen on the Topic (dialectic, juridical, critical analysis and through interviewing some experts).

The lack of stricted laws together with the non-experienced staff in charge of controlling the software security rules has brought about violation of the legal regulations.

INTRODUCCION.

La comunicación desde el mismo inicio del desarrollo de la humanidad ha resultado ser, un factor indispensable para todas las relaciones de intercambio económico, político y social, elemento este perdurable en el tiempo desde la

comunidad primitiva hasta nuestros días, pasando en su evolución por diferentes estadios y niveles de desarrollo en correspondencia a cada etapa en particular.

Contando entre sus fines directos, el intercambio de información, elemento este determinante para el desarrollo sociopolítico, comercial y económico de un país, en tal sentido, debemos considerar el derecho como el complemento de la misma, toda vez que le proporciona forma y carácter y la nutre de los elementos más representativos de la sociedad, de sus costumbres y sus valores.

El desarrollo de las comunicaciones, aparejado a los avances de la electrónica en la segunda mitad del pasado siglo, propicio el aumento progresivo del intercambio de información así como el necesario desarrollo de las técnicas para su protección.

EL siglo XX, también llamado el siglo de la electrónica por sus invenciones, fue la época que gestó el mayor adelanto tecnológico en función del comercio, las telecomunicaciones y posteriormente de la informática como herramientas que hoy en día son casi indispensables para cometer actos sociopolíticos, económicos y de comercio en su total expresión en una sociedad inmersa en el conocimiento y la información.

A raíz del impetuoso avance de este tipo de tecnologías y de algunos sucesos sociopolíticos y económicos a nivel mundial, la información, va sufriendo una

transformación cualitativa y cuantitativa, que permite no solo mirarla como una cuestión interna del desarrollo de cada país, sino como un fenómeno internacional con normas reguladoras, encaminadas hacia la búsqueda de uniformidad en las relaciones entre los países desarrollados y en vías de desarrollo.

La electrónica en sentido general y la informática en lo particular, han modificado sustancialmente la vida económica y social en muchos países y aparejadamente han hecho que el derecho se vea obligado e emitir nuevas concepciones, la mayoría de la documentación ha pasado a ser intangible y extraterritorial, las fronteras, limitadoras físicas del territorio de cada país, dejan de serlo al utilizar las vías electrónicas, por consiguiente la sociedad ha cambiado drásticamente, se ha nutrido de nuevas percepciones de conceptos y valores nuevos. Por tanto van cambiando los conceptos económicos y la forma en que la sociedad no solo encara la manera de negociar, sino de gobernar, entretenerse, educar y trabajar.

Ya hoy en día se reconoce expresamente por organismos internacionales como la OMC que la gran mayoría de los países pasarán de la era industrial basada en la transformación de materias primas a una nueva economía basada en el manejo de información a través de las computadoras, de la inteligencia artificial, de los recursos intangibles y de la comunicación.

La llamada “era de la información” transformará radicalmente las bases sobre las que descansa la economía mundial, al igual que la de nuestro país. Cambiará

dogmas, reglas, conceptos, cuestiones tales, que el Derecho no quedara inmune a ellos.

Dentro de este indetenible desarrollo de la informática y las comunicaciones, juega un papel preponderante el uso de Internet, concebida en sus inicios como una aplicación de uso militar en Estados Unidos, Internet fue un conglomerado de ordenadores enlazados entre si con protocolos de comunicación mas actuales y eficientes que el conocido IDE, esta red, al irse expandiendo, conectando centros universitarios, empresas públicas y privadas, perdió su carácter militar para convertirse en una red de alcance global, una vez que traspasó las fronteras nacionales, por lo que el carácter aterritorial es su principal característica.

Lo que propició que estas tecnologías fueran usadas para el desarrollo del comercio, las telecomunicaciones y el intercambio de información, agudizándose así los problemas legales, ya que lo que sucedía antiguamente en formato papel, con medios tangibles, se sucede en un espectro intangible, donde muchos productos también lo son.

Así pues se hace necesario un marco general de regulación de aspectos tan vitales como el control y seguridad de las transacciones internacionales, el cobro de impuestos, la protección de los derechos de propiedad intelectual, la protección de los consumidores en cuanto a publicidad engañosa o no deseada, el fraude, los

contenidos ilegales e ilícitos y el uso abusivo de datos personales; así mismo obliga a generar altos niveles de seguridad de la información.

La masiva utilización de las computadoras y redes como medios para almacenar, transferir y procesar información se ha incrementado espectacularmente en los últimos años, al grado de convertirse en un elemento indispensable para el funcionamiento de la sociedad actual. Como consecuencia, la información en todas sus formas y estados se ha convertido en un activo de altísimo valor, el cual se debe proteger y asegurar para garantizar su integridad, confidencialidad y disponibilidad, entre otros servicios de seguridad.

De igual modo que se protegen los otros activos de la empresa, los requerimientos de calidad y seguridad de la información se hacen indispensables. La dirección de la empresa debe establecer un sistema de seguridad adecuado que soporte y garantice el correcto funcionamiento de los procesos informáticos.

La forma más simple de proteger a una red de computadoras de peligros externos es aislándola físicamente y sin que exista posibilidad alguna de conectarse a ellas de manera remota.

Sin embargo, el desarrollo de las nuevas tecnologías de información y comunicaciones han propiciado formas más modernas y eficientes de desarrollar la gestión socio política, económica y comercial de un país, basado

fundamentalmente en las técnicas de trabajo en grupo sobre medios electrónicos y tomando como centro del análisis, el procesamiento, generación y protección de la información.

Desdichadamente un porciento significativo de la información con que se requiere trabajar en cualquiera de las tareas antes mencionadas, no se genera o está disponible en la organización en cuestión, y por tanto es inevitable el acceso a entidades externas, que en términos de seguridad informática pueden definirse como entidades no confiables.

Lograr que las personas que precisan de una información determinada en un momento dado puedan obtenerla directamente desde la fuente que la ha generado u otra designada por esta para su publicación, es una tarea bien difícil para las organizaciones en la actualidad, y no es posible tener éxito sin conexiones a redes de área amplia de carácter nacional o a redes de alcance global como Internet, por todo esto toma una gran importancia la necesidad del aprendizaje de los nuevos conceptos de Seguridad Informática.

En Cuba, no somos ajenos a este modelo de desarrollo, a mediados de la década del 90 del pasado siglo, Internet llega, y en el contexto en que se desenvuelve nuestro país ha visto transitar a paso acelerado un proceso de informatización de la sociedad que a vertiginosa velocidad en tan solo unos 15 años ha llevado a cuba a estar a la altura de muchos países del área con mayor tiempo en la aplicación de los logros tecnológicos.

Se toman iniciativas a manera experimental para desarrollar esta actividad, se crea el Instituto Latinoamericano de Protección contra Virus Informáticos con sede en Ciudad de la Habana, hoy devenido SEGURMATICA, sentando las pautas para el enfrentamiento al terrible desafió que representa el uso de las tecnologías de la información y las comunicaciones en el ámbito de su regulación jurídica**.**

Actualmente se ha incrementado en cuba el uso de aplicaciones electrónicas que abarcan: correo, comercio, transacciones y dinero electrónicos, firmas y certificados digitales, acceso seguro a bancos de información, comunicaciones seguras, entre otras. Por tal motivo, los requerimientos de seguridad son cada vez mayores, presentándose así un problema que la Seguridad Informática, haciendo uso fundamentalmente de técnicas criptográficas, trata de resolver implementando diversas herramientas.

No obstante los esfuerzos realizados con esta finalidad, nuestro sistema empresarial en general y las empresas en Perfeccionamiento Empresarial en lo particular, afrontan un conjunto de dificultades que van más allá de la mera acción de piratas, hackers y las estela de delitos informáticos que se comenten mediante el uso de los medios técnicos, todo lo que de una forma directa, inciden negativamente en el desarrollo de un sistema de seguridad informática.

Analizado el Decreto-Ley 187 del 98 sobre las Bases Generales del Perfeccionamiento Empresarial, se puede comprobar que se pronuncia en torno a la innovación tecnológica, la preparación del personal, el uso de medios técnicos de computación, al establecimiento de métodos y procedimientos que validen la información, no obstante lo cual el mismo no incluye dentro de su cuerpo, aspectos relacionados a la seguridad informática, a pesar de promulgarse con posterioridad a cuerpos legales como la Resolución 6 del 96 que puso en vigor el Reglamento sobre la Seguridad Informática.

De la misma forma, se pudo comprobar que no forma parte del presupuesto de las empresas lo referido a seguridad informática, lo que unido al escaso nivel del personal en cuanto a sus términos generales, el incumplimiento de las normas de acceso y permanencia, el descontrol en los registros establecidos y otras dificultades, hacen peligrar la correcta utilización de los planes de seguridad informática en las empresas inmersas en el perfeccionamiento empresarial en nuestra provincia.

Sobre la base de lo analizado, los principales aspectos concernientes a la seguridad informática, la normativa legal vigente y la situacion actual de esta en las empresas en perfeccionamiento empresarial en nuestra provincia, se determina como problema científico**.**

¿En que medida la legislación cubana vigente, sobre Seguridad Informática ofrece respuestas a los problemas actuales de esta materia para el sistema empresarial cubano?

A partir de esta problemática objetiva, determinamos como objeto de estudio. El Régimen Jurídico actual y los problemas de desarrollo de la seguridad informática para el empresariado cubano.

Estableciendo a su vez como campo de investigación**.** La normativa legal vigente, referente a la seguridad informática en cuba, la aplicación práctica de la norma, y los efectos derivados de ello.

Definidos estos elementos (problema científico, objeto de estudio y campo de investigación) proponemos como objetivo. Caracterizar la situación que presenta la Seguridad Informática en el entorno empresarial cubano a través del estudio del derecho comparado, la legislación vigente, y los problemas que se generan en su instrumentación dentro de nuestro entorno empresarial, con la finalidad de atemperarla a las exigencias actuales de nuestro sistema.

Resultado de todo lo anteriormente expresado, se formula la siguiente pregunta científica**. ¿**Responden las normas legales del ordenamiento jurídico cubano, a las necesidades actuales de la seguridad informática para el sistema empresarial cubano?

A fin de brindar solución al problema planteado, determinar el punto de vista a defender y dar cumplimiento al objetivo especificado, nos proponemos las siguientes Tareas Científicas.

1. Analizar la evolución legislativa de la seguridad informática en el mundo y en Cuba.

2. Análisis comparado de la normativa legal, relativa a la seguridad informática.

3. Estudio del régimen jurídico cubano, sobre la seguridad informática y los principales problemas s que soporta un sistema de seguridad informática.

4. Valorar las dificultades que se presentan en el ámbito empresarial para la correcta implementación del sistema de seguridad informática.

5. Proponer los elementos indispensables para la creación e instrumentación de un sistema de seguridad informática.

Los Métodos Teóricos de la Investigación Científica que se han utilizado en nuestra investigación, han sido.

- Método del análisis dialéctico. Encaminado a establecer la interrelación entre la seguridad informática y los demás fenómenos de la superestructura empresarial, a fin de precisar sus fundamentos y antecedentes históricos y legislativos.

- Método del análisis-síntesis. A los efectos de establecer los fundamentos teóricos de la investigación que permitan precisar conceptos y teorías generalmente aceptados, sobre el tema que se plantea.

- Método del análisis exegético-jurídico de las normas. Que nos permita caracterizar las deficiencias fundamentales en la normativa legal reguladora de la seguridad informática en Cuba.

Métodos Empíricos de la investigación utilizados.

- La observación en su variante del análisis de documento, teniendo como objeto planes de seguridad informática, resultados de auditoria informática, informes, legislaciones y, trabajos independientes realizados por estudiosos del tema.

- La observación participante. Se realiza de forma que permita observar las acciones, situaciones del campo de investigación así

como explorar la información existente en el tema, el modo en como se enfoca la actividad y que conocimientos teóricos y prácticos existen en las personas jurídicas y naturales que lo llevan a cabo.

- Del análisis histórico jurídico de la norma. Nos permite a partir del estudio, identificar los orígenes y momentos más importantes del tema así como su evolución.

- Del análisis comparado de la norma. Nos posibilita a partir del estudio, identificar diferencias y semejanzas en las normas jurídicas reguladoras de este tema en particular.

- Del análisis critico. Nos permitió conocer a profundidad el dominio que se posee en torno a los conceptos básicos elementales y el grado de especialización alcanzado por los encargados de la aplicación de la seguridad informática en el sistema empresarial cubano.

- La entrevista a expertos, contribuyo a una mejor percepción del panorama actual y futuro, las proyecciones existentes, así como las diferentes opiniones en torno al contenido y forma de los sistemas destinados al cumplimiento de todo lo relacionado a la seguridad informática dentro del entrono empresarial cubano.

La importancia del tema, será indiscutible, si lo valoramos desde una perspectiva de desarrollo necesario, al resultar imprescindible la implementación y perfeccionamiento de todo el sistema de seguridad informática en el sistema empresarial cubano, como vía para evitar las perdidas derivadas de su inexistencia como lo son la perdida de cliente, de imagen, de ingresos etc. desde una óptica generalizadora que abarque todas las esferas vinculadas a la misma, desde los simples trabajadores, estudiantes, hasta los mas altos niveles de todo nuestro sistema empresarial.

La relevancia de este tema se tiene también por la necesidad de evitar por una parte las afectaciones e incongruencias derivadas de la inobservancia de tales normas, así como por la indispensable urgencia de atemperar el sistema empresarial cubano a los acelerados avances del mundo contemporáneo en esta esfera del acelerado desarrollo tecnológico.

Este trabajo está diseñado de la siguiente manera.

Tema: EL REGIMEN JURIDICO DE LA SEGURIDAD INFORMATICA EN EL SISTEMA EMPRESARIAL CUBANO.

- Introducción.

CAPITULO I. LA SEGURIDAD INFORMÁTICA GENERALIDADES.

I.1- Principios, enfoques y fundamentos de la Seguridad Informática.

I.2- Sistemas de clasificación de los Criptosistemas. Medidas, criterios y normativas de seguridad en el derecho comparado.

I.3- Internet. El Icono Emblemático.

I.4- Estado Actual de la Seguridad Informática.

CAPITULO II. CONSIDERACIONES SOBRE EL TRATAMIENTO LEGAL DE LA SEGURIDAD INFORMÁTICA EN EL SISTEMA EMPRESARIAL CUBANO.

II.1 Antecedentes históricos- legislativos.

II.2 Legislación Actual.

II.3 Principales problemas del entorno jurídico y empresarial.

II.4 La instrumentación interna de la seguridad informática en el sistema empresarial cubano. Elementos y consideraciones generales al respecto.

- Conclusiones.
- Recomendaciones.
- Bibliografía.
- Anexos

CAPITULO I. LA SEGURIDAD INFORMÁTICA GENERALIDADES.

El incremento en el uso de ordenadores y sistemas de comunicación que permiten almacenar, procesar e intercambiar grandes cantidades de información está siendo espectacular en los últimos años. Este hecho provoca, que cada vez, un mayor número de organizaciones considere a su información y a la tecnología a ella asociada, como uno de sus activos más importantes.

A lo largo de la historia, incluso desde tiempos en los que no existía la electricidad, el hombre siempre ha querido simplificar su modo de vida, por esta razón los grandes pensadores de todos los tiempos, han dedicado gran parte de su vida a desarrollar teorías matemáticas para construir máquinas que simplifiquen las tareas de la vida diaria.

Sin lugar a dudas el siglo XX es considerado el siglo de la electrónica y de la informática, dejando al entrante siglo XXI innumerables adelantos tecnológicos capaces de modificar en gran medida el comportamiento de la humanidad en muchos sentidos, en lo social, en lo económico y porque no, en lo político.

Resultando ser el plano económico el más beneficiado, haciéndose extensivo incluso para los países en vías de desarrollo. Por ser precisamente en el ámbito del comercio donde las tecnologías electrónicas e informáticas irrumpieron para quedarse de una vez por todas y para bien del comercio este se hizo cada vez más dinámico y ágil al hacer uso de una infraestructura nunca vista que no iba a respetar barreras geográficas, idiomas y culturas. Prueba de la rapidez del avance informático, es tangible en cosas fáciles de encontrar como un artículo de revista de computación, paginas de Internet, libros antiguos de computación, entre otros.

En sus inicios los medios técnicos de computación, eran medios relativamente seguros, tomando en consideración que los mismos estaban dedicados a procesar volúmenes de datos importantes, tales como información contable, datos

estadísticos, en el orden interno de una empresa por lo cual era relativamente fácil su control, de la misma forma que el numero de empresas beneficiarias de su uso, era limitado.

I.1- Principios, fundamentos y enfoques de la Seguridad Informática

La definición puramente lingüística del concepto “seguridad” es actualmente inaplicable al tema que abordamos en este trabajo. Se concibe como seguro a aquello que resultare infalible, inatacable, libre y exento de todo peligro, daño o riesgo.

Hay autores tontos que sugieren que un sistema informático seguro es aquel que carece de red, y que se encuentra desconectado de la corriente. Estamos seguros que esta analogía tiene sus raíces en las palabras del famoso conquistador norteamericano de tierras indias y asesino de tribus, quien enunció su famosa frase “el único indio bueno es el indio muerto”.

La seguridad en los sistemas de cómputo existe, pero a diferencia del significado que la Real Academia de la Lengua le otorga, no puede ser absoluta. Eso sí: puede ser elevada a niveles insospechados, y para ello partimos de cinco elementos esenciales a tener en cuenta:

1. ¿Cuáles son los puntos débiles del sistema informático a proteger?

2. ¿Cuánto tiempo deberá protegerse un dato?
3. Las medidas de control se implementan para que tengan un comportamiento efectivo, eficiente, sean fáciles de usar y apropiadas al medio.
4. Ningún sistema de control resulta efectivo hasta que surge la necesidad de aplicarlo.
5. Los usuarios deben estar concientizados de las posibles fallas de los sistemas y de la necesidad de asegurarlos.

Como vemos, los cuatro primeros puntos que representan los principios clásicos de la seguridad informática son meramente técnicos. Pero el quinto, que con razón se reputa como el más importante, es de índole social.

En el primero de los caso (principio del Acceso más fácil) debemos considerar lo siguiente.

- “El intruso al sistema utilizará cualquier artilugio que haga más fácil su acceso y posterior ataque”.
- Existirá una diversidad de frentes desde los que puede producirse un ataque. Esto dificulta el análisis de riesgos porque el delincuente aplica la filosofía de ataque hacia el punto más débil.

En el segundo elemento (principio de La Caducidad del secreto) se debe tener presente que.

- “Los datos confidenciales deben protegerse sólo hasta ese secreto pierda su valor”.
- Se habla, por tanto, de la caducidad del sistema de protección: tiempo en el que debe mantenerse la confidencialidad o secreto del dato.
- Esto nos llevará a la fortaleza del sistema de cifra.

El tercer y cuarto elemento (principio de la Eficiencia de las medidas tomadas) se ha de considerar que.

- “Las medidas de control se implementan para ser utilizadas de forma efectiva. Deben ser eficientes, fáciles de usar y apropiadas al medio”.
  - Que funcionen en el momento oportuno.
  - Que lo hagan optimizando los recursos del sistema.
  - Que pasen desapercibidas para el usuario.

Y lo más importante: ningún sistema de control resulta efectivo hasta que es utilizado al surgir la necesidad de aplicarlo. Este es uno de los grandes problemas de la Seguridad Informática.

Analizados los principios de la seguridad informática, consideramos oportuno hacer referencia a los fundamentos sobre los que descansa la misma así como los diferentes enfoques que hacen posible o facilitan su estudio.

Fundamentos de la seguridad informática.

- La teoría de la información
  - Estudio de la cantidad de información y entropía.
- La teoría de los números
  - Estudio de las matemáticas discretas y cuerpos finitos.
- La teoría de la complejidad de los algoritmos
  - Clasificación de los problemas.

Teoría de la información

- Información:
  - Conjunto de datos o mensajes inteligibles creados con un lenguaje de representación y que debemos proteger ante las amenazas del entorno, durante su transmisión o almacenamiento, usando entre otras cosas, las técnicas criptográficas.
  - La teoría de la información mide la cantidad de información que contiene un mensaje a través del número medio de bits necesario para codificar todos los posibles mensajes con un codificador óptimo.

Teoría de los Números

- Es la base matemática (matemáticas discretas) en la que se sustentan las operaciones de cifra.

Teoría de la Complejidad Algorítmica

- La teoría de la complejidad de los algoritmos nos permitirá conocer si un algoritmo tiene fortaleza y tener así una idea de su vulnerabilidad computacional.

Para su estudio la seguridad informática, podemos dividirla en.

- Seguridad Física. Incluye la protección del sistema ante las amenazas físicas, planes de contingencias, control de acceso físico, políticas de seguridad, normativas, etc.
- Seguridad Lógica. Incluye la protección de la información en su propio medio mediante el enmascaramiento de la misma usando técnicas de criptografía, protocolos de autenticidad entre el cliente y el servidor.

De esta forma y analizados los elementos que a nuestro juicio resultan indispensable entre otros, para el estudio de la problemática que se nos presenta, resulta necesario, adentrarnos en el campo jurídico propiamente dicho o sea en el Derecho como una de las tres cúspides de la actividad social, conjuntamente con la política y la religión.

Particularmente interesante resulta el hecho de que como rama científica solamente en los últimos años se haya comenzado a hablar acerca del Derecho y

la Informática, cuando es evidente que en su papel de regulador de las relaciones sociales el Derecho juega su papel en el proceso de concientización de los individuos antes mencionado.

He aquí como el Derecho se entrelaza con esta ciencia de aparición relativamente reciente, dando paso a diversas interrogantes como son las siguientes:

1. ¿Existe una clara identificación del bien jurídico a proteger por la norma legal cuando este está relacionado con las TICs?
2. ¿Debe optarse por la flexibilidad o por la austeridad de las definiciones legales ante el impetuoso avance de las TICs?
3. ¿Qué ámbito de aplicación debe tener la norma que regule las relaciones en el ámbito de la informática: Penal, Administrativo, Civil o mixto?
4. ¿Está preparado el personal que imparte justicia para apreciar en su verdadero sentido la responsabilidad del infractor de la seguridad informática?
5. En nuestro país, ¿existe una política gubernamental de carácter normativo uniforme, centralizado y eficaz que prevenga la ocurrencia de hechos que atenten contra la seguridad informática?

Son muchas las interrogantes que en torno al tema pudiéramos formular en estas líneas. Sin embargo, en estas pocas se resumen los objetos de discusión más

candentes entre teóricos y especialistas, no sólo del país, sino también de la arena internacional.

Como siempre que surge una figura novedosa en el actuar social, el Derecho pronto capturó a la Informática como su centro de atención. Bien pronto los grandes teóricos enarbolaron clasificaciones en cuanto al software-de gestión, documental, etc. Y como era de esperar, las diferentes ramas del Derecho “se apresuraron” a tutelar a la recién nacida.

El Derecho de Propiedad Intelectual pronto vio en esta actividad un fruto de la creación humana, susceptible por tanto de ser regulada en este ámbito. Y para este fin, se revisaron los Convenios de Berna, el TRIPPS y demás instrumentos jurídicos internacionales de la materia. El software quedó, por esta vía, incluido y justamente por demás como una creación más del intelecto.

La creciente importancia del uso de las PCs fue elevando la significación de las mismas. Ya no eran simplemente dos o tres juguetes caros en un laboratorio de una institución científica o en manos de un millonario. Ahora estaban en manos de cualquier persona, y todos nos habíamos convertido en usuarios potenciales de esos cada vez más potentes adminículos electrónicos. Y para cuando surgió la idea de conectar varias PCs, el confuso

Era hora de que hiciera su entrada el Derecho Penal: la rama coercitiva por excelencia del Derecho. Máxima expresión de la tutela del Estado sobre un bien que a partir de ese momento reviste interés social por sobre el particular, o que al menos queda garantizado tutelarmente por sobre los demás, los penalistas se apresuraron a identificar como una nueva serie de delitos a conductas delictivas tradicionales que ahora pasaron a llamarse, pintorescamente, “delitos informáticos”.

El punto en común que tienen todas estas conductas antisociales –fraude, robo, estafa, daños- es que atacan solamente a un bien: la información. Un bien por demás intangible, que asimila esta clase de “delitos” a los cometidos contra la moral y las buenas costumbres, por citar un ejemplo.

Aún con repercusión en el ámbito moral, queda claro, no obstante, que los delitos informáticos, por aplicar la denominación ya cotidiana, atentan sobre todo contra la información. De ahí lo difícil que resulta tipificar y cuantificar sus resultados, por cuanto la información es difícil de cuantificar, evaluar, tasar y en general de apreciar en sus distintas facetas.

El otro punto que debemos tener en cuenta es en lo concerniente a la flexibilidad de la norma legal que regule el tema de la seguridad informática.

En efecto: la mayor parte de los legisladores prefiere hacer un uso gramatical restringido en la redacción de los textos legales, ante el temor de que la flexibilización excesiva conduzca a una aplicación extensiva de los mismos.

Por otro lado, el Derecho ha demostrado ir siempre más despacio que los cambios sociales que respaldan la emisión de instrumentos jurídicos. ¡Qué decir de aquellos que se dictaren amparando actividades relacionadas con la informática, una de las ramas del desenvolvimiento humano de mayor complejidad y velocidad de desarrollo actuales.

Por sólo poner un ejemplo: los virus informáticos atacaban hace 10 años solamente a programas ejecutables. Hace nueve años comenzaron a infectar documentos, algo que nunca se pensó fuera posible. Hace siete años infectaron hojas de cálculo y actualmente se les encuentra alojados hasta en el interior de archivos multimedia.

Cualquier norma que hubiera catalogado a un virus como “segmento de código ejecutable que se copia y reproduce a sí mismo dentro de programas ejecutables” hubiera quedado obsoleta en poco tiempo a causa de una definición incorrecta.

Con problemas semánticos y de redacción de este tipo el legislador debe enfrentarse a diario, razón por la cual, se hace necesario, realizar un análisis en torno al origen y evolución de la seguridad informática.

Resulta innegable que Internet se ha transformado en una inmensa fuente de información de acceso universal que ejerce una importante influencia en la educación y en el ámbito sociocultural, a la vez que presenta buenas perspectivas en el ámbito del comercio. Se trata de un importante foro donde se desarrollan numerosas actividades, la mayoría de las cuales son realizadas con fines legítimos y provechosos; pero, obviamente, también se llevan a cabo actividades ilícitas y conductas socialmente no aceptables. Es por ello que el tema de la seguridad informática, resulta un tema fundamental en los ámbitos académicos internacionales, tanto tecnológicos como jurídicos.

Como es conocido, la primera respuesta a las necesidades de protección de las redes fueron las técnicas criptográficas que, permiten proteger la información e impiden que los sistemas sean utilizados o accedidos por personas no autorizadas o con fines lícitos. Pero por otra parte ello facilita las actividades delictivas en las redes al transformar las comunicaciones en inexpugnables. No debemos perder de vista que, en todos los casos, esta presente el interés legitimo de los estados de velar por la seguridad y el orden publico y resguardo de las naciones.

En tal sentido podemos definir y las primeras aproximaciones históricas a estas técnicas criptográficas así como realizar una clasificación de las mismas.

- La criptografía es casi tan antigua como las primeras civilizaciones de nuestro planeta.
- Ya en el siglo V antes de J.C. se usaban técnicas de cifra para proteger a la información.
- Se pretendía garantizar sólo la confidencialidad y la autenticidad de los mensajes.

I.2 Clasificación de los Criptosistemas. Medidas, Criterios y Normativas de Seguridad en el derecho comparado.

Históricamente los criptosistemas o sistemas criptográficos para la protección de la información se clasifican según su relación con la historia en sistemas clásicos y sistemas modernos, sin analizar esta como la mejor clasificación desde el punto de vista de la informática, consideramos que la misma permite comprobar el desarrollo de estas técnicas de cifra hoy en día rudimentarias y en algunos casos simples, desde una perspectiva histórica.

Desde el punto de vista clásico los mismos se han dividido de la siguiente forma

- Cifrado por transposición:
- Escítala. Era usada en el siglo V a.d.C. por el pueblo griego de los lacedemonios. Consistía en un bastón en el que se enrollaba una cinta de cuero y luego se escribía en ella el mensaje de forma longitudinal.

- Al desenrollar la cinta, las letras aparecen desordenadas.

- La única posibilidad de recuperar el texto en claro pasaba por enrollar dicha cinta en un bastón con el mismo diámetro que el usado en el extremo emisor y leer el mensaje de forma longitudinal. La clave del sistema está en el diámetro del bastón. Se trata de una cifra por transposición pues los caracteres del criptograma son los mismos que en el texto en claro distribuidos de otra forma.

➢ Cifrado por sustitución.

  - Polybios. Es el cifrador por sustitución de caracteres más antiguo que se conoce (siglo II a.d.C.) pero como duplica el tamaño del texto en claro, con letras o números.
  - En 1917 Gilbert Vernam (MIT) propone un cifrador por sustitución binaria con clave de un solo uso
  - El cifrador de matrices de Hill. En 1929 Lester Hill propone un sistema de cifra usando una matriz como clave.

No obstante de todo lo anterior podemos afirmar que los mayores avances se lograron en la Segunda Guerra Mundial, los países en conflicto tenían un gran

número de técnicos encargados de romper los mensajes cifrados de los teletipos (criptografía moderna).

Esta nace al mismo tiempo que las computadoras. Durante la Segunda Guerra Mundial, en un lugar llamado Bletchley Park, un grupo de científicos entre los que se encontraba Alan Turing, trabajaba en el proyecto ULTRA tratando de descifrar los mensajes enviados por el ejercito alemán con el mas sofisticado ingenio de codificación ideado hasta entonces: la máquina ENIGMA. Este grupo de científicos empleaba el que hoy se considera el primer computador aunque esta información permaneció en secreto hasta mediados de los 70. Su uso y la llegada del polaco Marian Rejewski tras la invasión de su país natal cambiaran para siempre el curso de la Historia.

Desde entonces hasta hoy ha habido un crecimiento espectacular de la tecnología criptográfica, si bien la mayor parte de estos avances se mantenían y se siguen manteniendo, según algunos en secreto. Financiadas fundamentalmente por la NSA (Agencia Nacional de Seguridad de los EE.UU.), la mayor parte de las investigaciones hasta hace relativamente poco tiempo han sido tratadas como secretos militares. Sin embargo en los últimos anos investigaciones serias llevadas a cabo en universidades de todo el mundo han logrado que la criptografía sea una ciencia al alcance de todos, y que se convierta en la piedra angular de asuntos tan importantes como el comercio en Internet.

De forma generalizadora podemos definir los hitos históricos de la criptografía de la siguiente forma.

- La criptografía clásica abarca desde tiempos inmemoriales hasta la mitad del siglo XX.
- El punto de inflexión en esta clasificación la marcan tres hechos relevantes:
  - En el año 1948 se publica el estudio de Claude Shannon sobre la Teoría de la Información.

Cifrado Digital

  - En 1974 aparece el estándar de cifra DES.
  - En el año 1976 se publica el estudio realizado por W. Diffie y M. Hellman sobre la aplicación de funciones matemáticas de un solo sentido a un modelo de cifra, denominado cifrado con clave pública.

A partir de lo cual los criptosistemas poseen una clasificación actual que podemos definir de la siguiente forma.

- En dependencia del tratamiento de la información a cifrar en:
  - Cifrado en Bloque y Cifrado en Flujo
- En dependencia del tipo de clave utilizada en la cifra en:
  - Sistema con Clave Secreta y Sistema con Clave Pública

Calcificación esta a partir de la cual se han desarrollado diferentes modelos, criterios y normativas de seguridad que entre los principales podemos mencionar los siguientes.

- Modelo de Bell LaPadula (BLP)
- Modelo de Take-Grant (TG)
- Modelo de Clark-Wilson (CW)
- Modelo de Goguen-Meseguer (GM)
- Modelo de Matriz de Accesos (MA)

Criterios y normativas de seguridad

- Criterio de evaluación TSEC. Trusted Computer System Evaluation Criteria, también conocido como Orange Book.
- Criterio de evaluación ITSEC Information Technology Security Evaluation Criteria.
- Criterio de evaluación CC. Common Criteria: incluye los dos anteriores.

Existen legislaciones específicas encaminadas a regular este tipo de actividad, aunque por el momento no han demostrado ser suficientemente efectivas en el control de actividades ilícitas tales como violación de secretos, la propaganda o competencia desleal, los delitos contra la libertad de prensa, los accesos indebidos a sistemas, donde aparecen como preponderantes las figura de los Hackers, los Crackers y los Phreakers.

En el mejor de los casos las previsiones han demostrado ser adecuadas dentro de los límites fronterizos de las naciones, mas no así cuando se intenta reprimir mas allá de los bordes geográficos, siendo esta la característica definitiva de tales actos. Algunos ejemplos de ellos mostraremos a continuación.

- Reino Unido: Hasta 1990, la única legislación vigente que podía otorgar algún tipo de protección, que por supuesto, era muy deficiente para el amplio espectro de delitos de esta naturaleza, era la Ley de Protección de Datos de 1984 (Data Protection Act), según la cual solo había delito si se verificaba un elemento esencial, la existencia de daños o destrozos materiales. No obstante ese requisito material, las cortes habían comenzado a considerar delito a los daños efectuados ala propiedad intangible. En 1990, el parlamento británico sanciono la Ley de Utilización Indebida de Computadoras (Computer Misuse Act) que con el objetivo de brindar seguridad material al contenido en una computadora contra los accesos no autorizados, introduce los tipos de conductas punibles siguientes.
    - Provocar en una computadora determinado funcionamiento con la intención de asegurarse el acceso a cualquier programa o información contenida en ella.

- Realizar el mismo hecho mencionado anteriormente, pero con la intención de cometer o facilitar la comisión posterior del delito.
- Causar la modificación, la alteración o la eliminación total o parcial no autorizada de los contenidos de una computadora.

De este modo esta ley, introduce las necesarias modificaciones, entre las que podemos destacar, además de las mencionadas, las contenidas en las ultimas seis secciones, en la que se trata la jurisdicción de la ley y que incluyen previsiones sobre extradición, en las cuales se considera de jurisdicción británica al delito que, sin importar donde fue cometido físicamente, haya tenido sus repercusiones o efectos dentro del territorio de ese país.

- Canadá: Los delitos realizados por medio de computadoras fueron incorporados al Codigo Penal (Canadian Criminal Code) y básicamente están contemplados en las secciones 342 y 430. Las sanciones, están previstas para quien de forma fraudulenta e ilegitima tenga acceso, directa o indirectamente a una computadora, o intercepte o cause que se intercepte a un sistema. Asimismo, se prevén penas de hasta diez años de prisión para quienes alteren datos, intercepten u obstruyan su transmisión o imposibiliten el acceso a quienes están autorizados a hacerlo. Uno de los aspectos a destacar de la legislación canadiense, es que otorga una jurisdicción especial para los delitos cometidos por medio de computadoras,

que en caen bajo la orbita de Royal Canadian Mountain Police Y la Information Technology Security Branco, que son los organismos encargados de la seguridad en tecnología de la información en Canadá.

- Israel: Posee legislación sobre delitos realizados por medio de computadoras, incluso existe un organismo con jurisdicción para entender tales delitos, que es el Escuadrón Nacional de Fraudes. No obstante en dicho país, no se ha advertido aun la gravedad de estos tipos de delitos y en consecuencia, resulta común que los hackers, sean empleados por las industrias o las corporaciones.

- España: En este caso, la comisión de delitos por medio de instrumentos informáticos ha sido incorporada al Código Penal (modificación aprobada por Ley Orgánica 10/95, de 23/11/1995), que introduce cambios que permiten la tipificación de delitos cometidos por accesos no autorizados a redes de computadoras o telecomunicaciones , difusión de datos personales reservados, alteración de información, revelación de secretos ajenos, utilización indebida de claves personales, destrucción de programas o datos, plagio de software, estafa con medios informáticos etc. Muchos de los artículos contienen previsiones respecto a la protección de datos personales, otros tratan lo referente a datos reservados a personas jurídicas y se disponen sanciones similares para quienes divulgaren, revelaren o cedieren datos personales o reservados de personas jurídicas.

Por lo general, las penas oscilan entre uno y siete años de prisión y días multa. Otras de las normas introducidas, son las prescripciones de los artículos 211 y 212 que hacen responsables en forma solidaria por calumnias e injurias a los proveedores de servicios de Internet. Previsiones estas similares a las dispuestas por la Communications decency Act de los Estados Unidos de América.

De la misma forma, resultan ser de referencia obligada, otros cuerpos o normativas legales dictadas en este país, enfocadas directamente hacia la actividad de protección y seguridad de la información, como lo son.

- ✓ Ley Orgánica de Protección de Datos LOPD (1999) (Ley de seguridad Informática en España
  - Establece un conjunto de medidas de seguridad de debido cumplimiento por parte de empresas y organismos.
  - Ley Orgánica de Protección de Datos LOPD se desarrolla en España en el año 1999 y comienza a aplicarse ya en el siglo XXI.
  - Se crea una Agencia de Protección de datos APD que debe velar por el cumplimiento de esta ley mediante la realización de auditorías, al menos cada dos años. La APD la forman 9 personas.
  - Se definen las funciones del Responsable de Fichero y del Encargado de Tratamiento.

- Las faltas se clasifican como leves, graves y muy graves con multas de 60.000, 300.000 y 600.000 €.
- En el Real Decreto 994/1999 sobre “Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal” se definen las funciones del Responsable de Seguridad.
- Establece un conjunto de procedimientos de obligado cumplimiento de forma que además de proteger la privacidad de las personas, se cumplan los principios de la seguridad informática física y lógica.

✓ La normativa 17799 (Código de buenas prácticas para la Gestión de la Seguridad de la Información: PNE-ISO/IEC 17799 Proyecto de Norma Española)

– Desarrolla un protocolo de condiciones mínimas de seguridad informática de amplio espectro.

- Antecedentes
- Introducción
- Objeto y campo de la aplicación
- Términos y definiciones
- Política de seguridad
- Aspectos organizativos para la seguridad
- Clasificación y control de los archivos
- Seguridad ligada al personal

- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos
- Desarrollo y mantenimiento de sistemas
- Gestión de continuidad del negocio
- Conformidad

En 70 páginas y diez apartados, presenta unas normas, recomendaciones y criterios básicos para establecer unas políticas de seguridad. Éstas van desde los conceptos de seguridad física hasta los de seguridad lógica. Parte de la norma elaborada por la British Standards Institution BSI, adoptada por International Standards Organization ISO y la International Electronic Commission IEC.

1.3 Internet. El Icono Emblemático.

Las nuevas tecnologías digitales, que han irrumpido en redes abiertas de telecomunicaciones, han permitido el desarrollo y rápido crecimiento de Internet como el ícono representativo de esas redes, y de numerosos servicios disponibles a través de ellas. El surgimiento de esta “tecnología” no se debe a descubrimientos casuales, ni a movimientos sociales, ni a compañías telefónicas haciendo presión por una alternativa de comunicación nueva y más barata.

Internet se ha convertido en un fenómeno que involucra a millones de personas, por lo que resulta indispensable conocer sus antecedentes, origen, evolución, estado actual y las tendencias que genera, para poder tomar una reflexión más cabal sobre el tema.

En el periodo comprendido de la llamada Guerra Fría entre los años 1960 y 1985, el Departamento de Defensa de los EE.UU ordenaron la creación de un sistema de computación por paquetes desarrollado por la Advanced Research Projects Agency a finales de1960 (red denominada ARPANET), de tal manera que los sitios de investigación de ARPA pudieron compartir información y dar acceso a computadores de todo el mundo. Esta fue la reacción norteamericana al lanzamiento del primer satélite artificial de la Tierra, llevado a cabo por la entonces URSS, en el año 1957, ya que este suceso, presuponía un nivel investigación y desarrollo nunca antes visto, no solo desde el punto de vista coheteril, sino de las comunicaciones, al lograr la comunicación con una entidad artificial sobrevolando la esfera terrestre.

Por lo que en el año 1962 surge el proyecto denominado Internet, diseñado con fines militares. A partir de entonces los científicos a cargo del proyecto desarrollaron una tecnología denominada conmutación de paquetes (Packet Switching), que fuera capaz de enviar o recibir datos procedentes de dos puntos situados a gran distancia, incluso en medio de una guerra termonuclear y

sobrevivir a ella. A esta nueva tecnología se le asignó el nombre TCP/IP, siglas que corresponden a Transmission Control Protocol e Internet Protocol.

En noviembre de 1967, *Larry Roberts* formó el Network Working Group integrantes se reunieron el mismo mes. Dicho grupo estaba compuesto que tomarían parte en las primeras conexiones, como eran la University University of Utah, la UCLA, así como de la Rand Corporation. El NWG trabajó durante el invierno que siguió a noviembre de 1967. El 1 de marzo de 1961 se encontraban listas las especificaciones para la construcción de la red.

Durante el transcurso del año 1969, el diseño de los programas acompañó el trabajo en el hardware. El primer modelo que apareció fue el denominado cliente-servidor, un modelo familiar por la omnipresencia de terminales que empleaban las computadoras a tiempo compartido.

Esto condujo a la creación del Network Control Program (NCP), el primer programa de control de redes que después se denominó Network Control Protocol. La expresión "protocolo" se deriva de la tradición diplomática; aparentemente surgió de una metáfora que se utilizó en una conversación entre *Vint Cerf*, *Jon Postel* y *Stephen Crocker* en fecha no determinada. En el RFC (Requests for Comments) número 33 de *Crocker* y *Cerf* con fecha 12 de febrero de 1970, se empleó el término en su título ("New Host-to-Host Protocol).

Los protocolos de comunicación son conjuntos de reglas que permiten que diferentes computadoras con distintos sistemas operativos se comuniquen y compartan recursos. Los más importantes son: IP (Internet Protocol), TCP (Transmission Control Protocol), FTP (File Transfer Protocol), TelNet (Network Terminal Protocol), y SMTP (Simple Mail Transmission Protocol).

A partir de entonces los científicos a cargo del proyecto desarrollaron una tecnología denominada conmutación de paquetes (Packet Switching), que fuera capaz de enviar o recibir datos procedentes de dos puntos situados a gran distancia, incluso en medio de una guerra termonuclear y sobrevivir a ella. A esta nueva tecnología se le asignó el nombre TCP/IP, siglas que corresponden a Transmission Control Protocol e Internet Protocol.

A diferencia del procedimiento militar común, jerárquico, el modelo de la red fue ampliamente distribuido para permitir un fácil redireccionamiento de las comunicaciones en caso de un ataque. Hoy en día es el protocolo por excelencia de la comunicación de Internet.

En abril de 1971, el ARPANET estaba compuesta por 15 nodos. En aquel momento, ARPANET era una verdadera red de conmutación de paquetes. Sin embargo, sus diseñadores percibían que los especialistas que laboraban en el sector de las comunicaciones por medio de computadoras no habían tomado conciencia de la significación de este hecho. La idea de la red como un medio

nunca se comprendió completamente en los inicios de ARPANET. En1972, *S. D. Crocker* y otros publicaron una de las primeras descripciones acerca de un protocolo de aplicación relacionado con el trabajo remoto y la transferencia de ficheros donde se subrayó el punto de vista del usuario en lugar de la tecnología para la conmutación de paquetes. La mayoría de sus trabajos estaban dedicados al protocolo Telnet, para el uso de sistemas interactivos remotos.

Por otra parte, a inicios de los años 70, los franceses y los ingleses comenzaron sus propios proyectos.

En Francia, el Cyclades y su subred el CIGALE, fueron el resultado de estudios que comenzaron en 1970. El proyecto Cyclades experimentó con rapidez recortes en su presupuesto un año después debido posiblemente a que en 1974, el sistema de correo francés comenzó a trabajar en una red propia de conmutación de paquetes que finalmente se convirtió en Transpac, el servicio francés que se basado en el protocolo X.25.

En 1977, Gran Bretaña adoptó el protocolo X.25.

La creación del X.25 proporcionó una alternativa a la utilización del TCP/IP como una solución para la interconexión de redes. Mientras que TCP/IP era un protocolo de uso probado, disponible libremente y sin propietario, los portadores públicos deseaban un protocolo que estuviera diseñado para satisfacer sus necesidades e intereses específicos que no eran necesariamente los mismos que los de los

usuarios académicos y militares, quienes apoyaban los protocolos de ARPA. El X.25 es una norma que desarrolló CCITT, (una rama de la ITU - la International Telecommunications Union).

A mediados de los años ochenta, la National Science Foundation (NSF) se interesó en el proyecto, ya que se había desarrollado lo suficiente como para que las redes fueran utilizadas por los investigadores, colaborando así con el crecimiento de Internet.

Entre finales de los años 80 y principios de los 90, ocurrió una explosión de nuevas aplicaciones que transformaron completamente la visión de Internet. En 1989, tuvo lugar un suceso imperceptible en el CERN(Conseil Européen pour la Recherche Nucléaire) (Organización Europea para la Investigación Nuclear), un centro europeo de investigación en la rama de la física situado cerca de la frontera franco -suiza. *Tim Berners*-Lee y *Robert Cailiaux* comenzaron a concebir un sistema distribuido de documentosque se estructuraría en forma de hipertexto. En aquel entonces, la idea tuvo solo un alcance local.

La NSF y otros organismos, tal como la NASA, empezaron a desarrollar sus propias redes. A finales de la década de los ochenta, Internet empezó a alcanzar a otros países del mundo y la red ARPANET original fue abandonada en 1990. A partir de esa fecha la backbone de NSF (una red de alto rendimiento a la que se conectan otras redes) empezó a jugar su papel como el núcleo o superautopista

de Internet. En mayo de 1990, se celebró la primera conferencia sobre ciberespacio en la Universidad de Texas en Austin, que abordó no solo temas tecnológicos sino que previó el impacto legal de estas tecnologías.

Hoy Internet es una gigantesca red, un conglomerado de millones de ordenadores conectados, buscando y compartiendo información, situados en distintos países. Su principal característica es su carácter aterritorial, no conoce fronteras, y representa al mismo tiempo el mayor intercambio social de todos los tiempos prácticamente sin restricciones y por mucho tiempo a sido inmune a las leyes territoriales, al punto que muchas ha tenido que obligatoriamente someterse a revisión. Es la principal herramienta en la búsqueda y distribución de informaciones diversas, desde un planteamiento científico hasta la receta de puré de niños, esto hace a la sociedad más eficiente, el eliminar las restricciones geográficas de intercambio de conocimientos

Por otra parte lo que conocemos como autopista de la información, o sea la WWW (World Wide Web o “la Web”), que da soporte a Internet, se desarrolló en el European Particle Physics Lab como vehículo mediante el cual había científicos que trabajaban en diferentes lugares en el ámbito internacional y que compartían información sobre la física de alta energía. Encabezados por Tim Berners-Lee, hoy llamado el padre de la Web, los desarrolladores concluyeron en forma correcta que llegar a producir estándares para hardware o software representaba una pérdida de tiempo. Por el contrario, desarrollaron un estándar de comunicación

para representar los datos. Este se llamó el Hypertext Markup Language, o lenguaje de hipertexto HTML el cual es la base de toda publicación que se haga en Internet hoy en día, que da soporte a la vez al XML o eXtensive Markup Language

Este lenguaje, bastante sencillo en sus inicios, propicia la vinculación de documentos entre si y dentro del mismo documento, a lo que llamamos hipervínculos. Al utilizarlo sencillamente se adhiere una etiqueta apropiada para una frase o palabra ocasionando que ésta se convierta en un enlace con otra página. Este enlace puede ser para un documento en la misma máquina o en una máquina diferente en cualquier parte del mundo, explotando la otra importante innovación de la Web, un sistema universal de direcciones. Con este sistema se puede tener acceso a cualquier documento Web, que puede incluir opcionalmente sonido, imagen e incluso video; de igual manera, se puede entrar y ver con mucha facilidad, sin volver a ingresar otro número, conociendo cualquier dirección del computador o digitando una identificación específica.

Una de las herramientas más populares que agregaba este sistema era el correo electrónico, que permitía a los investigadores el envió de mensajes de datos. Otros avances significativos eran la facilidad de las conferencias y la conversación interactiva al alcance de los que estuvieran conectados entre si, dando el nombre de ciberespacio a ese tiempo en el que se encontraban enlazados los sistemas computacionales.

1.4 Estado actual de la Seguridad Informática.

Analizado el estado actual del desarrollo de las tecnologías informáticas, resulta procedente remarcar nuevamente que en esta sociedad global de la información, estas resultan ser uno de los bienes mas preciados, con relación a ella se ha expresado que, actualmente, la creación de nuevas riquezas depende mas de la información que de otros recursos, existiendo predicciones, según las cuales para el año 2020 el 80 % del valor económico surgirá de la tecnología de la información.

El hecho de llamársele, era de la información, sociedad global o era del conocimiento, es una señal que advierte en torno a su creciente valor, resulta innegable que en esta nueva y competitiva era, las riquezas han pasado a provenir del suelo y la naturaleza en general , a ser un producto de nuestras mentes. De manera creciente las economías están basadas en el conocimiento y, por tanto son más dependientes de la habilidad humana de crear, vender explicar y solucionar problemas.

Cada vez en mayor medida la información juega un papel preponderante en las economías, circunstancia que es mas notoria en los países industrializados, en donde la producción y distribución de información ha pasado a ser una de las mayores fuentes de recursos, como consecuencia de ello han comenzado a emerger nuevas divisiones sociales entre quienes poseen información y quienes no la poseen.

No obstante la preocupación fundamental de las instituciones, es en la actualidad, brindar la mayor seguridad a sus sistemas automatizados de información, pues en la mediad de la dependencia tecnológica de las mismas obtendrán por un lado, mayor agilidad y dinamismo y por otro como contrapartida, quedan expuestas a grandes riesgos de vulneración.

Básicamente le problema de la seguridad en las redes es un tema, que por la magnitud de sus consecuencias y las proyecciones que se preveen en el futuro desarrollo de las mismas, se ha tornado estratégico para los gobiernos de todo el mundo. Estas proyecciones pronostican que el crecimiento y evolución de la sociedad de la información globalizada tendrá características exponenciales en virtud del sostenido abaratamiento de los costos del hardware y el software y del desarrollo de Internet II (que posibilitara la conexión a 100 veces mayor velocidad que en la actualidad), todo lo cual significara un aumento desmedido en la cantidad de usuarios conectados a la red. A esto debemos sumarles los esfuerzos internacionales para promover el crecimiento del comercio electrónico y sus derivaciones (firma digital, contratos instrumentados digitalmente, moneda digital).

Con este objetivo, los estados han tomado decisiones estratégicas a fin de otorgar mayor seguridad a las redes, fundamentalmente tratando de delinear un marco normativo adecuado que brinde seguridad jurídica, con el fin de fomentar el desarrollo de actividades a través de redes.

En tal sentido, cabe destacar que todas aquellas acciones que se lleven adelante en el desarrollo de sistemas de seguridad y de normas específicas para regular la administración, acceso y control de los sistemas informatizados, se traducirán tanto en la promoción del comercio electrónico como en la seguridad de las naciones.

CAPITULO II. CONSIDERACIONES SOBRE EL TRATAMIENTO LEGAL DE LA SEGURIDAD INFORMÁTICA EN CUBA.

II.1 Antecedentes históricos- legislativos y su comportamiento actual

En nuestro país se puede hablar de un desarrollo de las tecnologías de la información y las comunicaciones caracterizado por una curva ascendente, que sin embargo alcanza una elevación más significativa a inicios del año 1995. No obstante consideramos oportuno hacer mención a lo que a nuestro juicio, resultan ser los principales antecedentes históricos y legislativos relativos a la protección de la información, como sin lugar a dudas resultan ser.

- Ley número 1246 del Secreto Estatal de fecha 14 de Mayo de 1973, sobre la protección del secreto estatal y su reglamento, puesto en vigor por el decreto número 3753 de 17 de enero de 1974.
- El decreto número 3787 de 23 de septiembre de 1974, que puso en vigor los Reglamentos Gubernamentales para el Servicio de Cifrado Nacional y, para el Servicio de Cifrado Exterior.
- Ley número 1321 del 27 de Noviembre de 1976, Ley de Protección Física.

Las cuales indistintamente, facultan al Ministerio del Interior para dirigir, ejecutar y controlar la política del Estado y el Gobierno en cuanto a la Protección de la Información, la política Criptográfica y la Protección Física.

En efecto se puede hablar del uso extensivo de las primeras PCs solamente alrededor del año 1987. En esos tiempos el tema de la seguridad informática no era uno de los más sensibles, aún cuando en el año 1988 se detectó en el país el primer virus informático: el Vienna 648, también conocido como Ping Pong o de la "pelotica".

En esos tiempos las computadoras eran medios relativamente seguros, ya que al ser medios escasos y de relativamente alto valor, las normas de protección física –léase acceso- a las mismas eran severas. Como habitualmente estaban dedicadas a procesar volúmenes de datos importantes, tales como información contable, datos estadísticos, información de la defensa, etc. poseían salvas y era, en resumen, relativamente fácil el control de las mismas.

La fundación de los primeros Joven Club de Computación y Electrónica, aparejado a la introducción en la enseñanza de los primeros equipos personales de cómputo, popularizaron el papel de las PC. Muy pronto la cifra inicial de ocho virus a nivel nacional se duplicó. Los virus se convirtieron en la amenaza más severa por entonces debido al intercambio indiscriminado de disquetes y a la inexistencia de discos duros en las PCs que posibilitaran la instalación de antivirus en las mismas.

Instituciones como el Instituto Latinoamericano de Protección Contra Virus Informáticos, con sede en Ciudad de la Habana, hoy devenido Segurmática, sentaron pautas para la lucha contra estas amenazas. Grupos independientes

como Merchise, de la Universidad de las Villas, contribuyeron asimismo a este proyecto.

En 1992, la Isla abrió sus puertas a Internet. Hasta ese entonces el tráfico de datos hacia el exterior se efectuaba a través de un backbone o enlace arrendado a Canadá, que solamente amparaba el uso del correo electrónico. La entrada de Cuba a Internet planteó un desafío considerable a los responsables de la seguridad informática en el país.

A pesar de los años transcurridos, nuestro país, al igual que el mundo, se enfrenta al terrible desafío que representa el uso de las tecnologías de la información y las comunicaciones en el ámbito de su regulación jurídica. Se trata de hacer frente a un fenómeno social, que como siempre tendrá su contrapartida de manera tardía en el ordenamiento jurídico.

Pero por si fuera poco, debemos enfrentarnos a cambios cotidianos, elevar la preparación técnica del personal que opera las PCs, cambiar la mentalidad de jueces y fiscales…todo ello en medio de una discusión sin frutos aparentes donde aún algunos debaten si existen o no delitos informáticos, quizás cerrando los ojos a la realidad patente de que la acción dañina se produce ante nuestros ojos y ya Cuba es objeto de hechos que, delitos o no, tienen como patrón común la existencia o utilización de una PC para cometerlos.

II.2 Legislación Actual

A partir de la llegada de Internet, y a pesar de lo reducido de su presencia en el ámbito nacional, se tomaron medidas de índole legal para ordenar y regular su uso, así como los medios de trabajo que se utilizan, enfocado principalmente a las computadoras personales de trabajo. La mayoría de estas legislaciones, dan tratamiento al tema de la seguridad informática en las empresas, así como de los medios físicos que elaboran información, entre ellas se destacan las siguientes**:**

- En el Decreto 209 del 96, se establecen regulaciones para el desarrollo adecuado y armónico, así como los intereses de la defensa y seguridad del país, para el acceso desde la República de Cuba a redes Informáticas de alcance global y en él se define que el Ministerio del Interior será el responsable de dirigir, controlar y aplicar, en el marco de su competencia, la política de Seguridad Informática.

- L a Resolución número 204 de 20 de noviembre de 1996 del Ministerio de la Industria Sideromécanica y Electrónica, que pone en vigor el reglamento Sobre la Protección y Seguridad Técnica de los Sistemas Informáticos.

- La Resolución número 6 del 96. La misma, dictada por el Ministerio del Interior como máximo responsable del estado para dirigir, controlar y aplicar, en el marco de su competencia, la política de Seguridad Informática, pone en vigor el Reglamento sobre la Seguridad informática,

> dado a cumplimentar las medidas establecidas para la protección y seguridad del Secreto Estatal y la Protección Física y, basado en la necesidad de que esta (La Seguridad Informática) requiere de una disposición que contenga las normas básicas que implementen un sistema de medidas administrativas, organizativas, físicas, técnicas y legales que garanticen la confidencialidad, integridad y disponibilidad de la información que se procese, intercambie, reproduzca y conserve mediante el uso de las tecnologías de información.

Dicho cuerpo legal, consta de seis Títulos, definiendo en el número uno, los objetivos y alcance de dicho sistema, enmarcando como objeto del mismo, establecer los principios, criterios y requerimientos de Seguridad Informática que garanticen la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce y conserva mediante el uso de las tecnologías de información, siendo el Jefe máximo de cada entidad el responsable del cumplimiento de todo lo que en él se dispone, haciendo extensivo su alcance a todos los Organos y Organismos de la Administración Central del Estado y sus dependencias, otras entidades estatales, empresas mixtas, sociedades y asociaciones económicas que se constituyan conforme a la Ley, (en lo adelante entidad), siendo de obligatorio cumplimiento por todas las personas que participen en el uso, aplicación, explotación y mantenimiento de las tecnologías de información.

De la misma forma define la seguridad informática como el conjunto de medidas administrativas, organizativas, físicas, técnicas, legales y educativas dirigidas a prevenir, detectar y responder a acciones que pongan en riesgo la confidencialidad, integridad y disponibilidad de la información que se procese, intercambie, reproduzca y conserve a través de las tecnologías de información. Considerando a su vez como bien perteneciente a cada entidad, toda la información que se procese, intercambie, reproduzca y conserve a través de los medios técnicos de computación.

Fijando en su titulo segundo entre otros contenidos, el establecimiento de las medidas administrativas sobre la seguridad informática, incluyendo en los mismos las políticas y planes de seguridad y de contingencia, estipulando que el Plan de Seguridad Informática se instituye como una exigencia para todas las entidades, en el cual deben reflejar las políticas, estructura de gestión y el sistema de medidas, para la Seguridad Informática, teniendo en cuenta los resultados obtenidos en los análisis de riesgos y vulnerabilidad realizados. El máximo dirigente de cada entidad garantizará, según corresponda a la actividad informática que se desarrolle, que se elabore, ponga en vigor, cumpla y actualice periódicamente. Por su parte el Plan de Contingencia para la Seguridad Informática se instituye como una exigencia para todas las entidades, con el fin de garantizar la continuidad de los procesos informáticos ante cualquier desastre que pueda ocurrir.

Igualmente se definen las áreas vitales, los requerimientos de protección física y tecnológica de los soportes, la identificación de las tecnologías de información que posean, la designación y funciones del responsable de la seguridad informática.

Se establece o definen las entidades autorizadas a brindar servicios de Seguridad Informática a terceros estipulando que las mismas deben contar con el correspondiente certificado de autorización emitido por el Ministerio del Interior sin perjuicio de las que puedan conceder otros organismos así mismo estipula que la persona responsabilizada con el control de la información clasificada, en coordinación con el Responsable de Seguridad Informática, comprobará si las tecnologías de información y sus soportes que se trasladen al extranjero, contienen solo la información que se autoriza para ello, así como que estén libres de virus informáticos.

Por ultimo dicho texto define el proceder necesario para el enfrentamiento a las violaciones detectadas en el funcionamiento y uso de las tecnologías de información.

- Decreto Ley 199 de 25/11 de 1999. Sobre la Seguridad y Protección de la Información Oficial. Sin lugar a dudas, resulta ser este, el máximo esfuerzo por ordenar de alguna forma el ámbito normativo cubano en materia de seguridad informática, constituyendo la principal razón que motiva la

emisión de esta norma, la necesidad de proteger al país ante la actitud agresiva y de constante acecho de las agencias de inteligencia enemigas.

La misma estructurada en ocho capítulos, define en su articulo numero uno como objetivo fundamental de la misma, establecer y regular el Sistema para la Seguridad y Protección de la Información Oficial, estableciendo además que dichas normas deben ser cumplimentadas tanto los órganos, organismos, entidades o cualquier otra persona natural o jurídica residente en el territorio nacional, como las representaciones cubanas en el exterior. Para dar paso en su artículo numero dos al contenido de la misma, dentro del cual encontramos precisamente y entre otros lo referido a la seguridad informática, para dar paso en su artículo numero tres a una serie de definiciones sobre términos que a nuestro juicio consideramos oportuno dejar plasmado, de forma tal que permitan una rápida adaptación al contenido de los mismos, en aras de facilitar la comprensión generalizada del tema en cuestión.

- **Acceso**: Facultad o autorización que se otorga a una persona y que le permite conocer información oficial clasificada para el ejercicio de sus funciones.
- **Auditoría a la Seguridad Informática**: Es el proceso de verificación y control mediante la investigación, análisis, comprobación y dictamen del conjunto de medidas dirigidas a prevenir, detectar y responder a acciones que pongan en riesgo la confidencialidad,

integridad y disponibilidad de la información que se procese, intercambie, reproduzca y conserve por medio de las tecnologías de información.

- **Compartimentación:** Acción de dar a conocer lo que competa a cada persona, de acuerdo al acceso a la información oficial que le sea otorgado.
- **Documento**: Cualquier objeto físico capaz de proporcionar información o datos que pueden ser transferidos del conocimiento de una persona a otra.
- **Entidad**: Toda organización administrativa, comercial, económica, productiva o de servicios de carácter estatal, cooperativo, privado o mixto, residente en el territorio nacional, así como las organizaciones sociales y de masas del país.
- **OCIC**: Oficina para el Control de la Información Oficial Clasificada.
- **Plan de Contingencia**: Documento básico contenido dentro del Plan de Seguridad Informática, mediante el que se establecen las medidas para restablecer y dar continuidad a los procesos informáticos ante una eventualidad o desastre.
- **Plan de Evacuación, Conservación y Destrucción de la Información Oficial**: Documento básico que establece las medidas organizativas y funcionales para la evacuación, conservación o destrucción de la información oficial, que por sus características es

necesario preservar o destruir al declararse una situación excepcional o producirse una catástrofe.

- **Plan de Seguridad Informática**: Documento básico que establece los principios organizativos y funcionales de la actividad de Seguridad Informática en un órgano, organismo o entidad, a partir de las políticas y conjunto de medidas aprobadas sobre la base de los resultados obtenidos en el análisis de riesgo previamente realizado.
- **Plan de Seguridad y Protección de Información Oficial Clasificada**: Es el documento básico que establece el conjunto de medidas organizativas, administrativas, operativas, preventivas y de control dirigidas a garantizar la seguridad y protección de la información oficial clasificada e impedir su conocimiento u obtención por personas no autorizadas o por los servicios especiales extranjeros.
- **Protección Criptográfica**: Proceso de transformación de información abierta en información cifrada mediante funciones, algoritmos matemáticos o sucesiones lógicas de instrucciones, con el objetivo de su protección ante personas sin acceso a ella.
- **Seguridad Informática**: Conjunto de medidas administrativas, organizativas, físicas, técnicas, legales y educativas dirigidas a prevenir, detectar y responder a las acciones que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de la

información que se procesa, intercambia, reproduce o conserva por medio de las tecnologías de información.

- **Señalización**: Acción de consignar de forma visible y expresa la categoría de clasificación o término que le corresponde a la información oficial.
- **Servicio Cifrado**: Actividad que se realiza mediante un conjunto de regulaciones, medidas organizativas y técnicas y medios para la protección criptográfica de la información oficial clasificada que se tramita o almacena a través de las tecnologías de información.
- **Tecnologías de Información**: Medios técnicos de computación o comunicación y sus soportes de información, que pueden ser empleados para el procesamiento, intercambio, reproducción o conservación de la información oficial.

Continuando con el análisis de dicho cuerpo legal, observamos como el mismo establece y define al Ministerio del Interior, como el organismo encargado de regular, dirigir y controlar todo lo concerniente a la política gubernamental, referente la seguridad y protección de la información, a la vez que hace referencia a las funciones y atribuciones del mismo

En su capitulo siete, dedicado exclusivamente a la seguridad informática, establece entre otros aspectos, la obligación de los órganos, organismos y

entidades, donde se procesa, intercambia, reproduce o conserva Información Oficial por medio de las tecnologías de información, a.

- Cumplir las medidas que se requieran para su seguridad y protección, en correspondencia con las normas y regulaciones emitidas por el Ministerio del Interior.
- Elaborar, aplicar y mantener actualizados permanentemente los Planes de Seguridad Informática y de Contingencia, acorde con lo establecido por el Ministerio del Interior para la seguridad informática y por el de la Industria Sidero Mecánica y la Electrónica para la seguridad técnica de los sistemas informáticos.
- Designar una o más personas en su caso, con la idoneidad requerida para que supervise y controle el cumplimiento de las medidas de Seguridad Informática establecidas.

A la vez que prohíbe. Procesar, reproducir o conservar Información Oficial Clasificada con la categoría Secreto de Estado en las tecnologías de información conectadas en redes de datos, crear o diseminar programas malignos, el acceso no autorizado a redes de datos y conectar tecnologías de información que procesen Información Oficial Clasificada a las redes de datos de alcance global. Concediendo a la autoridad administrativa, la facultad para, conocer y aplicar la

medida correspondiente ante la inobservancia de tales prohibiciones, sin perjuicio de cualquier otra responsabilidad derivado de ello.

No obstante, en lo concerniente a la seguridad informática el Decreto Ley adolece de las siguientes deficiencias:

1. Subordina la importancia de las TICs a que las mismas procesen, conserven, intercambien o reproduzcan **información confidencial**, dando competencia al MININT y al SIME (hoy MIC) para regular estos procesos.
2. Delegó en el MININT la facultad de realizar y autorizar la realización de las auditorías de Seguridad Informática, existiendo en la actualidad dualidad de funciones con el MAC.
3. Carece de apartado que implique sanciones o demás acciones coercitivas.

En general, se dedican solamente 7 de 53 artículos al tema de la Seguridad Informática.

Las disposiciones complementarias del Decreto Ley se dirigieron a fomentar en todas las entidades nacionales la elaboración de Planes de Seguridad Informática y de Contingencias. Como era de esperar, los Planes constan de una estructura

esquemática, y solo adaptan a las necesidades particulares ciertos aspectos de la actividad.

En muchos casos el Plan de Seguridad Informática y el de Contingencias revisten carácter clasificado, y no son del conocimiento de los usuarios, que no saben que conducta adoptar ante la ocurrencia de hechos que atenten contra la seguridad informática.

Entre estas disposiciones complementarias podemos mencionar las siguientes.

- Res. 4/96 de fecha 22/4/96 del MIC Establece que las operaciones de los servicios de INTERNET dentro del país se regirán por las Resoluciones y Disposiciones vigentes de los Organismos de la Administración Central de Estado correspondiente y de las que a este fin emita el Ministerio de Comunicaciones para el tratamiento de las Redes de Datos.

- Res.57/96 CITMA de fecha 26/6/96 Crea el Registro Nacional de los distribuidores y productores de bienes y servicios de información electrónica para redes de datos, el que se conocerá indistintamente y a todos los efectos como “REGISTRO NACIONAL DE INFORMACION ELECTRONICA PARA REDES DE DATOS”.

- Res56 del 99 de 16/6/1999 del Ministerio de Cultura Establecer que toda publicación seriada cubana que pretenda circularse, imprimirse o difundirse por INTERNET deberá contar con la aprobación específica del Registro Nacional de Publicaciones Seriadas para ese fin, independientemente del nodo, institución o país que utilice como vía de ingreso a dicha red.

- Res.1/2000 de fecha 26/12/2000 del Ministerio del Interior que pone en vigor EL REGLAMENTO SOBRE LA SEGURIDAD Y PROTECCION DE LA NFORMACION OFICIAL

- Res No. 2/01 de 5/3/2001 del Ministro del Interior que pone en vigor el REGLAMENTO SOBRE EL SISTEMA DE SEGURIDAD Y PROTECCION FISICA.
- Res. 188/01 de fecha 15/11/01 MIC Aprobar y poner en vigor la Metodología para el acceso de entidades cubanas a Internet o a otras redes de datos externas a las mismas.

- Res. 269/2002 SIME 23/12/02 Poner en vigor el REGLAMENTO SOBRE LA POLÍTICA DE SEGURIDAD INFORMÁTICA en el Ministerio de la Industria Sidero-Mecánica

- Res. 39/02 de fecha 3/4/02 del MIC Poner en vigor las Políticas de Seguridad Informática del Ministerio de la Informática y las Comunicaciones.

- Res. 65/03 MIC fecha 5/6/03 Toda Red Privada de Datos establecida en el territorio nacional deberá ser inscrita en el registro existente a esos efectos en la Agencia de Control y Supervisión del Ministerio de la Informática y las Comunicaciones, en lo adelante la Agencia.

- Res 180/03 MIC de fecha 31/12/03 Disponer que la Empresa de Telecomunicaciones de Cuba S.A. (ETECSA), emplee todos los medios técnicos necesarios que permitan detectar e impedir el acceso al servicio de navegación por Internet, desde líneas telefónicas que operan en moneda nacional no convertible a partir del 1ro. De enero del 2004.

- INSTRUCCIÓN No.1-04 de 8/7/2004 del SIME Requisitos y Procedimiento a tener en cuenta para el acceso a Internet en las Entidades del SIME.

- Res. 85/04 de 13/12/2004 del MIC Toda “Area de Internet” que brinde los Servicios de Navegación por Internet y/o Correo Electrónico Nacional e Internacional en cualquier tipo de entidad del territorio nacional, deberá estar debidamente registrada a esos efectos en la Agencia de Control y

Supervisión del Ministerio de la Informática y las Comunicaciones, en lo adelante Agencia

- Res. 12/05 de 24/1/05 del MIC Poner en vigor los “Requisitos informáticos adicionales para los Sistemas Contables–Financieros soportados sobre las Tecnologías de la Información

Toda esta legislación antes mencionada, como bien se observa, está destinada a proteger cuestiones referentes a la seguridad de informaciones oficiales, medios físicos, a la estrategias de seguridad informática en relación a presencia de virus, accesos no autorizados, desastres y contingencias de diversos ordenes.

No podíamos concluir este análisis sin hacer referencia a nuestro marco penal, como vía idónea para cuestionar y en su caso reprimir las innumerables violaciones que se acontecen en el marco de las TICs, podemos observar como en nuestro país, al igual que en otros muchos países, estas conductas violatorias, no han sido aún objeto de tipificación por parte de nuestra legislación penal o sea en nuestro código penal.

Por tal razón, coincido con los que consideran que la vía más adecuada para enfrentar estas conductas es la revisión de los delitos convencionales previstos en el Código Penal Cubano y atemperar su formulación a las nuevas condiciones en que puede materializarse la acción a través de medios informáticos y en los casos

en que esto no sea posible, agruparlas dentro de un nuevo Título dedicado a tutelar como bien jurídico la Seguridad Informática.

II.3 Principales problemas del entorno jurídico

La Seguridad Informática es uno de los elementos técnico-jurídico más vinculados a la Era de la Información y por ende constituye una de las piedras angulares de toda realización informática que vaya a tener una incidencia social. Las disposiciones de Seguridad Informática son las que permiten contar con sistemas automatizados que cuenten con los requisitos de confidencialidad, integralidad y disponibilidad de la información digitalizada. Por eso un régimen jurídico de Seguridad Informática debe contener las normas que establezcan.

- Las garantías para la confidencialidad.
- Disponibilidad e integridad de los sistemas informáticos.
- La información digitalizada tanto la que se guarda en soportes magnéticos como la que circula por las redes.
- Programas, Datos e Información.
- Servicios de procesamientos de datos.
- Equipos e instalaciones de procesamiento electrónico de datos e información.
- Las principales debilidades y amenazas de los sistemas informáticos.

Por otra parte consideramos que la Seguridad Informática debe ser reconocida legalmente como

- medio de prevención de delitos en el entorno informático, por tal razón es necesario establecer las normas que rigen para el registro contable de los medios y recursos informáticos a proteger o medidas de seguridad informática, así como aquellas disposiciones que permitan delimitar el valor patrimonial de los activos protegidos.

No debe faltar en esta previsión legislativa las normas que fijen las medidas de Seguridad Informática que rigen para diversos ámbitos de aplicación:

- Administrativo y de organización
- Personal.
- Entorno físico.
- Sistemas electrónicos utilizados en telecomunicaciones.
- Equipos y programas de computación.

Asociado a éstos presupuestos enunciados están las normas que establezcan las reglas para la delimitación de los riesgos asociados a los recursos protegibles.

También hay que establecer las disposiciones legales que fijen los parámetros para evaluar la vulnerabilidad del sistema de procesamiento de datos identificados como sujetos de seguridad informática. Especial relevancia tienen las normas para

el reconocimiento y otorgamiento de las licencias de Seguridad y las Certificaciones de Seguridad Informática, ya que las certificaciones efectuadas hoy en día por las entidades autorizadas, véase Cámara de Comercio, si bien disponen de autorización para la actividad, la validez del documento electrónico, que se emite, no dispone aún de un sistema integral de reconocimiento legal a diversas instancias, no solo judicial.

Los planes de estudio actuales son omisos en gran medida en cuanto al conocimiento específico de la informática por los juristas. El aprendizaje de la informática va dirigido más bien a formar operadores de equipos, que se dejan mistificar por los conceptos sobre virus, hackers y seguridad informática.

Ante los jueces y fiscales se plantea una interrogante: ¿será culpable el individuo realmente de lo que se le acusa? ¿Qué figura delictiva cometió realmente? ¿Se podía haber concretado la acción delictiva mediante el uso de los medios empleados? ¿Son aceptables los medios de prueba propuestos?

Está claro que aún ni la más vasta preparación podría preparar a los profesionales del derecho para asumir tarea de índole técnica tan compleja. Para ello se auxiliarán asimismo de los peritos judiciales, y en general de los medios generalmente utilizados para ello.

Pero lo que obviamente resulta claro es que sin profesionales preparados, poco tendremos que esperar en el futuro inmediato a la hora de aplicar una norma novedosa.

Aún cuando podemos catalogar de fuerte la política del Estado cubano ante los infractores de la seguridad informática, al adoptarse medidas severas ante hechos relevantes, podemos citar aspectos que propician la ocurrencia de estos:

1. Escasa o nula educación de los jóvenes en aspectos de la ética informática. Esto es de especial peligrosidad en los nuevos Institutos Politécnicos de Informática y en la UCI. Debemos crear gurus y hackers, no piratas ni prehackers.
2. Irresponsables reportes sensacionalistas en los medios de difusión masiva de incidentes que atentan contra la seguridad informática internacional. En el caso de los hechos ocurridos en el país, se les silencia o atenúa, aún cuando servirían de ejemplos típicos de fallas comunes en los sistemas nacionales.
3. A pesar de que la política es fuerte, los esfuerzos se encuentran dispersos entre el MININT, el CITMA y el MIC. Solamente un actuar organizado de estas instituciones y una norma uniforme y extensa sobre seguridad informática sentará las bases para un marco legal satisfactorio.

4. Normas emitidas por el MININT como las relacionadas con el cifrado de datos limitan la posibilidad de que las personas naturales y jurídicas protejan la confidencialidad de la información intercambiada.

II.4 Instrumentación interna de la seguridad informática en el sistema empresarial cubano.

No obstante los esfuerzos realizados y que se continúan realizando, y los años transcurridos, nuestro país en general y nuestro sistema empresarial en lo particular, enfrentan el terrible desafío que representa el uso de las tecnologías de la información y las comunicaciones así como el universo infinito de violaciones, en sus mas diversas formas de manifestación que se materializan a través o mediante el uso de estas avanzadas tecnologías, todo lo cual representa sin lugar a dudas y, a nuestro juicio uno de los mayores retos para el empresariado cubano en la lucha por el perfeccionamiento del mismo, a fin de lograr la competitividad requerida ante los embates presentes y futuros de este mundo globalizado. Mundo este en el cual, la Seguridad Informática, juega un papel preponderante y definitorio.

Todo lo cual requiere sin lugar a dudas del perfeccionamiento de todas las infraestructuras de nuestro sistema, para enfrentar los cambios cotidianos, elevar los niveles de preparación técnica no solo del personal directamente vinculado al

uso de estas tecnologías, sino a todos los que de una forma u otra posean o puedan poseer relación con las mismas, pero enfocados en primer orden hacia la importancia vital que desempeña y desempeñará en el futuro , la seguridad informática para nuestro empresariado y para nuestro país.

En este contexto, consideramos oportuno proponer, los elementos y estructura que a nuestro juicio y derivados de la experiencia practica del autor, han de tomarse como punto de partida para la implementación de un sistema de seguridad informática en nuestro sistema empresarial, a partir de las disposiciones legales vigentes para tales fines. El mismo deberá contener**.**

1. Alcance. El mismo se hará extensivo a cada una de las personas con acceso a los medios informáticos que se relacionen en dicho plan.

2. Caracterización del Sistema Informático. Donde se definirán las Características de las Computadoras haciendo énfasis en las que se conectarán a INTERNET así como el Software y el hardware de cada una de ellas.

3. Resultado del análisis de Riesgo Para realizar este Plan de Seguridad Informática se deberá llevar a cabo el estudio y análisis de los riesgos que implicaría la conexión a Internet con el objetivo de identificar los recursos que se afectarían por las violaciones de seguridad y las amenazas a las que están

expuestos dichos recursos, de forma tal que dicho análisis nos brinde la información siguiente.

- Determinación precisa de los recursos sensibles de la organización.
- Identificación de las amenazas del sistema.
- Identificación de las vulnerabilidades específicas del sistema.
- Identificación de posibles pérdidas.
- Identificación de la probabilidad de ocurrencia de una pérdida.
- Derivación de contramedidas efectivas.
- Identificación de herramientas de seguridad.
- Implementación de un sistema de seguridad eficiente en costes y tiempo.

4. Las políticas de Seguridad. Resultara indispensable, establecer claramente una política de seguridad que garantice.

- La confidencialidad, integridad y disponibilidad de la información.
- La seguridad requerida de las tecnologías de información de la entidad.
- Neutralizar la recepción o transmisión de informaciones de carácter nocivo.
- Que ningún trabajador operará máquinas o equipos sin estar previamente adiestrado de acuerdo a los planes de adiestramiento vigente y autorizado

- Que el activo informático estará a disposición del personal que esté debidamente autorizado para realizar las auditorias informáticas.

De la misma forma dicha política deberá definir entre otros aspectos.

- La obligación de los trabajadores, respecto al uso de dichos medios técnicos.
- Las prohibiciones relativas al uso de los medios técnicos.
- El o los procedimientos para la implantación de toda nueva versión de un sistema.
- La especificación de no colocar información clasificada en las maquinas con acceso a Internet.

5. Sistema de seguridad informática, En este aspecto, se definirán las áreas a proteger y dentro de estas una especial atención a aquella destinada a la navegación de Internet. De la misma forma se ha de incluir en este acápite el tratamiento a:

- Los Recursos Humanos, donde se establecerán como requisitos previos el adiestramiento, la evaluación y la autorización del personal, para el uso de las tecnologías informáticas. De igual forma la obligación del Responsable de Seguridad Informática de elaborar y mantener actualizado el Registro de Software Autorizado (Registro**)** para las máquinas de Internet, el listado nominal de los trabajadores con acceso a internet así como las responsabilidades tanto de los

encargados del control de todo lo concerniente a la seguridad informática en la entidad (Comisión de Seguridad Informática) como los trabajadores con acceso a internet.

- Los Recursos o Medios Técnicos, se realizara un análisis detallado y de la misma forma se establecerá el control de cada uno de los medios técnicos de la entidad.
- Medidas y Procesamientos de Seguridad Informática y dentro de estas.
    - De Protección Física. Dirigidas a las áreas con tecnología instaladas, a las tecnologías de la información, y a los soportes de información Por tales motivos, se debe tener en cuenta los siguientes aspectos.
        - ✓ Anclajes a mesas de trabajo.
        - ✓ Cerraduras.
        - ✓ Tarjetas con alarma.
        - ✓ Etiquetas con adhesivos especiales.
        - ✓ Bloqueo de portadiscos.
        - ✓ Protectores de teclado.
        - ✓ Tarjeta de control de acceso al hardware.
        - ✓ Suministro ininterrumpido de corriente.
        - ✓ Toma de tierra
        - ✓ Eliminación de estática.

- De Protección Técnica o Lógica. Entendiendo como tal al conjunto de medidas que se implementen mediante el empleo de programas o medios tecnológicos encaminados a proteger las tecnologías informáticas, y sus soportes tecnológicos de información. Entre las cuales tenemos
    - Identificación de Usuarios.
    - Autenticación de Usuarios.
    - Control de Acceso a los Activos y Recursos.
    - Integridad de los Ficheros y Datos.
    - Auditorias y alarmas.

- De Seguridad de las Operaciones**.** Aquí se definirán los criterios para la selección de os mecanismos de seguridad

    - Sistemas de salva de respaldo**.** En este caso se debe establecer la obligatoriedad de todos de la realización de salvas diarias de la información obtenida, que permita la actualización del banco de datos, y por ende la restauración del sistema ante posibles daños.

    - Mantenimiento y reparación de las tecnologías de información. El Responsable de Seguridad Informática, deberá establecer un plan de mantenimiento de los medios técnicos, exigiendo

por su cumplimiento, enfatizando que la realización de los mismos, siempre se hará en presencia del administrador de la Red.

- Control del uso, traslado y entrada de tecnologías de información. Deberá garantizarse el cumplimiento de las medidas de seguridad, así como las salvas de las informaciones, de la misma forma ha de mantenerse actualizado el control de los medios, y los componentes.

- Pruebas de inspección. Las mismas se realizaran periódicamente, para comprobar los registros especiales, listado de usuarios conectados, cumplimiento de las medidas de seguridad.

- Registros. Como sistemas de registros para el control de los diferentes procesos que se realicen, se han de establecer para el obligatorio cumplimiento los siguientes:
    - Registro de Software de nueva adquisición.
    - Registro de inspecciones:
    - Registro y control de los soportes:
    - Registro de incidencias de la Seguridad Informática:

Este registro es muy importante porque nos permitirá tener un control de todas las incidencias más relevantes ocurridas durante el día, ya que se registran hechos como: Traslado de los medios, roturas, trabajo de personal ajeno a la entidad, visitas, violaciones, existencia de virus, salvas, etc. Se establece con carácter obligatorio la anotación en el "Libro de Incidencias" por el Responsable de Seguridad Informática e INTERNET.

- Registro de Control de los Medios Técnicos de Computación:

- De Recuperación ante Contingencias

Planes de contingencia. Análisis pormenorizado de las áreas que componen la organización que nos servirá para establecer una política de recuperación ante un desastre, lo que además de aumentar la seguridad, permitirá un conocimiento mayor de las fortalezas y debilidades del sistema. El mismo, se referirá exclusivamente al activo informático que se posea y al grupo encargado de ejecutar dicho plan.

En el mismo se realizara una determinación de las vulnerabilidades, entre las que estarán.

- Contaminación con virus informáticos.
- Destrucción o modificación del Sistema Operativo.
- Publicación de información Clasificada o Sensible.
- Fallas del fluido eléctrico.

- Fallas de las comunicaciones.
- Fallas del Hardware.
- Roturas de los Equipos de climatización.
- Denegación del Servicio.

Definiendo para cada caso en particular las acciones a realizar para el enfrentamiento a cada una de estas vulnerabilidades en el caso de ocurrencia de alguna de ellas así como los responsables y las responsabilidades de cada uno de ellos.

Además de lo cual se incluirán medidas educativas y de concientizacion, encaminadas a divulgar los aspectos claves que permitan garantizar la seguridad informática, los programas de preparación, las sanciones a aplicar por la violación o inobservancia de lo contenido en el plan en correspondencia a la legislación vigente en materia de disciplina laboral, con independencia a cualquier otra responsabilidad derivada del caso.

Concluida esta exposición de los elementos que de forma general y a nuestro criterio, deberá contener un plan de Seguridad Informática. Haremos referencia a una estructura lógica del mismo.

1. Alcance.
2. Característica del Sistema Informático.
3. Resultados del Análisis de Riesgo.
4. Políticas de Seguridad.
5. Sistema de Seguridad Informática

Medios Humanos.

Medios Técnicos.

Medidas y Procesamientos de Seguridad Informática.

Medidas de Protección Física.

A las Áreas con Tecnología Instaladas

A las Tecnologías de Información.

A los Soportes de Información.

Medidas Técnicas o Lógicas.

Identificacion de Usuarios.

Autenticación de Usuarios.

Control de Acceso a los Activos y Recursos.

Integridad de los Ficheros y Datos.

Auditorias y Alarmas.

Medidas de Seguridad de las Operaciones.

Medidas de Recuperación ante Contingencias.

6. Anexos

Programa de Seguridad.

Listado Nominal de Usuarios con Acceso a Redes de Alcance Global (Internet).

Registros.

Código de Etica

Con esta estructura, consideramos que se da cumplimiento al propósito inicial de poner en manos de nuestro empresariado, una herramienta útil de trabajo, que permita facilitar en cierta medida, la implementación de un sistema de seguridad informática, abarcador de los postulados fundamentales y de las necesidades reales de protección y enfrentamiento a las disímiles violaciones que en este campo se generan y puedan generarse en medio del progresivo avance de las tecnologías de la información .

CONCLUSIONES:

Con el trabajo que se presenta, hemos pretendido aglutinar un abarcador conjunto de elementos, del acontecer internacional y nacional referente a la normativa en materia de seguridad informática.

Razón por la cual, hemos arribado a las siguientes conclusiones.

1. El marco legal normativo que establece el Estado Cubano relativo a la seguridad informática en el Decreto Ley 199/99 es insuficiente en la práctica, por tanto no ofrece las respuestas necesarias a nuestro entorno empresarial.
2. A pesar de los enormes esfuerzos que se realizan tanto en el orden internacional como nacional para desarrollar políticas de seguridad que permitan una mejor gestión de la seguridad informática, inevitablemente tanto la doctrina como la practica, han evolucionado mas despacio que la informática, por demás una de las ramas del desenvolvimiento humano de mayor complejidad y velocidad en su desarrollo.
3. Una buena parte del empresariado cubano reconocen la importancia de las tecnologías informáticas y dentro de estas, la necesaria implementación de un sistema de seguridad informática, en contraposición a esto, el grado de capacitación de los recursos humanos resulta insuficiente a tales fines.

4. Existe desconocimiento y desacuerdo entre los profesionales del Derecho en lo que a normatividad se refiere. Incluso, en lugar de adoptar acciones concretas, muchos siguen imbuidos en la batalla sobre si existen los delitos informáticos o no, cuestión que, a nuestro juicio, no es el aspecto más relevante de la discusión.
5. La existencia de normas legalmente establecidas que regulen el funcionamiento y control del Ciberespacio y su seguridad requieren de manera ineludible de normas penales que complementen el ordenamiento jurídico y establezcan sanciones que permitan enfrentar la comisión de conductas que violen la Seguridad Informática.
6. Por el desarrollo y vulnerabilidad que actualmente han alcanzado las TIC, la auditoría informática ha de convertirse en una herramienta vital para garantizar el cumplimiento de los controles internos en todas las entidades del país que utilicen sistemas informáticos.
7. Los planes de estudio actuales son omisos en gran medida en cuanto al conocimiento específico de la informática y dentro de esta a la seguridad informática.

8. El aprendizaje de la informática va dirigido más bien a formar operadores de equipos, que se dejan mistificar por los conceptos sobre virus, hackers y seguridad informática.

RECOMENDACIONES:

1. Resulta indispensable la promulgación de normativas legales que amparen la seguridad informática en toda la magnitud de su impetuoso desarrollo
2. Proveer al empresariado cubano, de los recursos materiales, humanos y financieros indispensables que permitan implementar y a su vez enfrentar las más disímiles conductas violatorias de la seguridad informática.
3. Implementar en nuestro sistema educacional medio y superior, programas de estudio contentivos de la seguridad informática como vía indispensable para el desarrollo ulterior de nuestro sistema empresarial.

4. Ofrecer una mayor divulgación especializada en el tema de la seguridad informática, que contemple no solo los principales aspectos del ámbito internacional, sino también del entorno cubano

5. Potenciar los cursos de superación en nuestro sistema empresarial, dirigido específicamente a esta temática.

6. Trabajar en la promulgación de una norma jurídica uniforme, bajo los principios de nuestro ordenamiento jurídico, pero atemperada con la legislación internacional, y con el grado de flexibilidad suficiente que permita su adaptación a las diversas variantes derivadas del acelerado avance de las tecnologías informáticas.

Anexo I: Entrevista

Guía de entrevista a personas relacionadas directamente con el tema

El criterio para seleccionar a los expertos, se estableció por los siguientes aspectos.

1. Tiempo de desempeño en la actividad. (7 años)
2. Calificación profesional y estudios de postgrado, especializados en el tema. .
3. Reconocimiento y prestigio derivado de sus conocimientos en torno al tema.

Pregunta 1: ¿Considera usted que las normas legales vigentes, relativas a la seguridad informática, responden a las crecientes necesidades del sistema empresarial cubano en esta área?

Pregunta 2: ¿Cuáles son las principales dificultades detectadas en materia de seguridad informática, en las inspecciones realizadas a las empresas en perfeccionamiento empresarial de nuestra provincia?

Pregunta 3: ¿Cuál es el criterio de selección utilizado para definir las empresas a inspeccionar?

Pregunta 4: ¿Cuáles son las principales dificultades detectadas en dichas inspecciones, tanto en el orden de tratamiento legal como en la utilización de las normativas internas para el control de esta actividad?

Pregunta: 5 ¿Cuál es el nivel de preparación de los especialista que atienden la seguridad informática en las empresas visitadas, así como los trabajadores y dirigentes, acerca de esta actividad?

Pregunta: 6 ¿Cómo se comporta el cumplimiento por parte de las entidades en perfeccionamiento empresarial, respecto a la legislación en materia de seguridad informática?

BIBLIOGRAFIA:

- Aguirre, Jorge Ramiro Seguridad Informática y Criptografía Versión 4.1., Universidad Politécnica de Madrid, 01/03/2006.
- Alonso, Fernando Benito. Construyendo una Intranet, http://www.interplanet.es/enterprise/welcome.htm
- Bases generales del perfeccionamiento empresarial en la empresa estatal cubana. 1998.
- Castell, Manuel. La Sociedad Red. Alianza Editorial. 1996.
- Colectivo de autores. El impacto de las nuevas tecnologías en la vida de la empresa. Cuadernos Cinco Días. Ibermática 2000.
- Colectivo de autores. El mundo en hechos y cifras. La industria de la información. Consultoría BIOMUNDI. IDICT. 1998.
- Drucker, Peter. La información que importa. Los ejecutivos y los datos. Revista Gestión. Enero - Febrero 1996.
- Gil Pechúan, Ignacio. Sistemas y tecnologías de la información para la gestión. Mc. Graw-Hill. España.1997.
- Mansfield,,www.madrimasd.org/informacion/publicacion/doc/inovtec1.pdf. 1984.
- Microsoft TelchNet. 2000.
- Miret Biosca, Josep María “Curso de Seguridad Informática y Criptografía” Universidad Politécnica de Madrid.

- Morant Ramón, J.L.; Ribagorda Garnacho, A.; Sancho Rodríguez J. SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN. Colección de Informática, Editorial Centro de Estudios Ramón Areces, S.A., Madrid, Año 1994 (388 páginas)
- Navas López, José Emilio. Organización de la empresa y nuevas tecnologías. Ediciones Pirámides S.A. Madrid. 1994.
- Ordiz Fuertes, Mónica, Pérez - Bustamante, Ilander. Creación de valor en la empresa a través de las tecnologías de la información y comunicación. ESIC Market. Enero-Febrero 2000.
- Pastor, José; Sarasa, Miguel Angel- CRIPTOGRAFÍA DIGITAL. FUNDAMENTOS Y APLICACIONES, Prensas Universitarias de Zaragoza, Año 1998 (597 páginas)
- Quesada, Jorge. 3INTERNET. Facultad de Economía. U.H. 2001.
- Seguridad y protección de la información, Colección de Informática, Editorial Centro de Estudios Ramón Areces, S.A., Madrid. Año 1994 (388 páginas)
- Scott, George M. Principios de Sistemas de Información. Mc. Graw-Hill. 1994.
- Tapscott, Don, Caston, Art. Cambios de paradigmas empresariales. Mc. Graw-Hill. 1995. (Best Seller International).
- TECNOLOGIA EMPRESARIAL Año 1 No. 2.

- TI Magazine. Cómo obtener ventajas competitivas por medio de la información. Diciembre 1998.
- TI Magazine. Data Warehouse. Diciembre 1999.
- Zaldívar, Daniel Austin. Comercio Electrónico y Derecho en Cuba. Una Visión del Entorno 2007.
- Zeleny, M. The IEBM Handbook of Information Technology in Business. Thomson Learning. UK. 1999.

Legislación Nacional

- Ley número 1246 del Secreto Estatal de fecha 14 de Mayo de 1973
- Ley número 1321 del 27 de Noviembre de 1976, Ley de Protección Física.
- Decreto - Ley no. 186 / 98 “Sobre el sistema de seguridad y protección física”
- Decreto Ley 199 de 25/11 de 1999. Sobre la Seguridad y Protección de la Información Oficial
- Decreto 299 del Consejo de Ministros, que establece el acceso desde cuba a redes informa ticas de alcance global.
- Decreto número 3753 de 17 de enero de 1974.
- Decreto número 3787 de 23 de septiembre de 1974
- Decreto 209 del 96,
- Resolución número 204 de 20 de noviembre de 1996 del Ministerio de la Industria Sideromecánica y Electrónica

- Resolución número 6 del 96. del Ministerio del Interior
- Res. 4/96 de fecha 22/4/96 del MIC.
- Res.57/96 CITMA de fecha 26/6/96
- Res56 del 99 de 16/6/1999 del Ministerio de Cultura
- Res.1/2000 de fecha 26/12/2000 del Ministerio del Interior
- Res No. 2/01 de 5/3/2001 del Ministro del Interior
- Res. 188/01 de fecha 15/11/01 MIC
- Res. 269/2002 SIME 23/12/02
- Res. 39/02 de fecha 3/4/02 del MIC.
- Res. 65/03 MIC fecha 5/6/03
- Res 180/03 MIC de fecha 31/12/03
- Res. 85/04 de 13/12/2004 del MIC
- Res. 12/05 de 24/1/05 del MIC
- INSTRUCCIÓN No.1-04 de 8/7/2004 del SIME

Legislación Internacional:

- Directiva 2000/31/Unión Europea sobre “Sociedad de la Información y Comercio Electrónico”
- Ley de Protección de Datos de 1984 (Data Protection Act) Inglaterra

- Ley de Utilización Indebida de Computadoras (Computer Misuse Act) 1990, Inglaterra
- (Canadian Criminal Code)
- (Canadian Criminal Code)
- Ley Orgánica de Protección de Datos LOPD (1999) (Ley de seguridad Informática en España
- La normativa 17799 (Código de buenas prácticas para la Gestión de la Seguridad de la Información: PNE-ISO/IEC 17799 Proyecto de Norma Española)