UNIVERSIDAD LATINA, S.C.

INCORPORADA A LA U.N.A.M.
FECULTAD DE DERECHO

"LA PRIVACIDAD PARTICULAR EN INTERNET POR NAVEGANTE, Y SU FALTA DE LEGISLACION ESPECIFICA"

T E S I S

QUE PARA OBTENER EL TITULO DE:
LICENCIADO EN DERECHO
P R E S E N T A :
CLEMENTE TREJO ESTRADA

ASESOR: LIC. MARTIN FUENTES GARCIA

MEXICO, D.F. 2004

UNIVERSIDAD LATINA, S.C.

INCORPORADA A LA U.N.A.M.

Coyoacán México 03 de Junio de 2004

C. DIRECTOR GENERAL DE REVALIDACIÓN
INCORPORACIÓN Y DE ESTUDIOS, UNAM
P R E S E N T E:

El **C. TREJO ESTRADA CLEMENTE** ha elaborado la tesis profesional titulada **"La privacidad particular en internet por navegante, y su falta de legislación especifica"** bajo la dirección de la **LIC. MARTIN FUENTES GARCIA** para obtener el Titulo de Licenciado en Derecho.

El alumno ha concluido la tesis de referencia, misma que llena a mi juicio los requisitos marcados en la Legislación Universitaria y en la normatividad escolar de la Universidad Latina para las tesis profesionales, por lo que otorgo la aprobación correspondiente para todos los efectos académicos correspondientes.

ATENTAMENTE
"LUX VIA SAPIENTIAS"

LIC. SANDRA LUZ HERNÁNDEZ ESTÉVEZ
DIRECTORA TECNICA DE LA
LICENCIATURA EN DERECHO.
CAMPUS SUR

Autorizo a la Dirección General de Bibliotecas de la UNAM a difundir en formato electrónico e impreso el contenido de mi trabajo recepcional.
NOMBRE: Clemente Trejo Estrada
FECHA: 21-JUNIO-04
FIRMA:

En la ciudad de México, D.F. 19 de marzo de 2004.

UNIVERSIDAD LATINA, S.C.
ESCUELA DE DERECHO.

LIC. SANDRA LUZ HERNÁNDEZ ESTEVEZ.
DIRECTORA TÉCNICA
DE LA LICIENCIATURA EN DERECHO.
P R E S E N T E.

Por medio de la presente, me dirijo a Usted, para hacer de su conocimiento que he concluido la revisión del Trabajo de Tesis realizado por el alumno; **Clemente Trejo Estrada,** que curso en esta Institución la Licenciatura en Derecho, la cual lleva por titulo **"La Privacidad Particular en Internet por Navegantes, y su Falta de Legislación Específica."**Misma de la cual funjo como asesor y a mi consideración, reúne los requisitos de fondo y forma conforme a la Legislación Universitaria y al Reglamento de Titulación de la Universidad Latina.

Por lo anterior expuesto solicito a Usted, que turne el presente Trabajo para continuar los trámites que establece el manual de Titulación de la Universidad Latina.

Agradezco su valioso apoyo

Sin otro particular le envío un cordial saludo, y me permito asimismo felicitarla a usted por su atinada Dirección y a la Institución a la que orgullosamente pertenezco, por la formación de profesionistas, plenos de valores y conocimientos.

Respetuosamente, quedo de usted.

A T E N T A M E N T E

LIC. MARTÍN FUENTES GARCÍA

Agradecimiento

A Díos gracias por permitirme concluir una etapa más en mi vida, por estar con migo siempre y brindarme la gracia de la vida.

A mis Padres, quienes han estado con migo en todos los momentos importantes de mi vida, aquellos que me dieron la vida, me llevaron de la mano, me dieron su confianza y me brindaron todo su apoyo, a ellos dedico mis logros y agradezco por ser quien soy. Que Díos los Bendiga y Cuide.
Francisco Trejo S. y Eufemia Estrada L.

A aquellos que siempre estuvieron con migo en las buenas y en las malas, sin importar más, que quien soy, aquellos que siempre tenían una mano extendida para ayudar, apoyar incondicional, así como para aquellos momentos de alegría.
Gracias Amigos

A quien siempre está en mi corazón y me ha brindado apoyo en todo, así como aliento para seguir adelante a pesar de lo adverso de la vida. G. S. F. (T. A).
A quien me dio el coraje de emprender esta carrera O. C. M. Gracias.

A aquellos que me dieron un voto de confianza para poder concluir con este trabajo y poder cerrar el último paso de un gran periodo de mi vida, a mis Asesores Gracias.

Índice General

Introducción

La tecnología, va de la mano con todo lo que podemos ver alrededor de nuestras vidas, desde una simple calculadora que puede realizar cálculos científicos hasta una sencilla suma. Muchos estudiosos desde la invención del teléfono, habían soñado con el concepto de un programa o medio de comunicación universal, tal vez, sin pensar que sus sueños llegarían en nuestros días más haya de esta simple comunicación de dos personas.

Fuera de este sueño que se convirtió en realidad, se creó algo más, un sistema de comunicación que aparte de mantener a sus usuarios comunicados a grandes distancias, es también un medio por el cual se puede tener acceso a cualquier tipo de información, este sistema se llama Internet, este medio nos va proporcionar información y conocimientos que van desde los más sencillos hasta los más complejos dirigida a personas especializadas, es un sistema que cualquier persona puede utilizarlo sin mayor complicación, simplemente se requiere de tener conocimientos básicos de manejo de computadoras, y la información que el usuario requiere la obtiene sin mas movimientos que un "clic" en un botos de su equipo de computo el cual se encargará de obtener toda la información requerida.

El uso de la Red de la Información de Internet hasta hace algunos años estuvo exclusivamente en manos de los expertos, científicos y mandatarios, y este sistema de información no era como actualmente es, sino que para su funcionamiento se debería conocer una gran cantidad de conceptos y comandos para poder entrar al mundo cibernético, el cual era exclusivo y sin lo que hoy conocemos como "Chat de diversión" o simples páginas de ocio. De unos años para nuestros días, los expertos en informática y en este medio comenzaron a desarrollar sistemas computacionales que pudieran ser usados por personas con pocos conocimientos y experiencia en sistemas de cómputo, es decir personas comunes. La creación de estos sistemas han hecho más fácil su uso, por ejemplo se ha incorporado el uso del ratón ("mouse") y pantallas gráficas, que reducen al mínimo el uso de comandos, eliminando el sistema operativo, haciendo una computadora más, accesible, para todos. Gracias a este desarrollo de tecnología y la preocupación por los expertos, se aumentó en la vida diaria los sistemas computacionales, así como al tratar de hacer una comunicación y envió de materiales de trabajo más rápida y directa, dejando a un lado el concepto de exclusividad del Internet y ampliándolo en primer término a las universidades y después abrir esta maravilla al mundo en general.

Gracias a esto en nuestros días podemos tener acceso a el "World Wide Web" que si hacemos la traducción al español es "Red de Alcance Mundial o la Red que Abarca el Mundo", el cual no es más que un sistema que permite tener acceso a un sin fin de información de una red de máquinas conectadas a ella que se conoce como Internet.

En base a esto de la misma forma se fueron creando más valores en este sistema como fue la extensión de la comunicación, tanto vía E-mail, Chat y las reglas comerciales, es aquí en donde las empresas comerciales como tecnológicas, rápidamente incorporaron sus innovaciones a la competencia económica y se unen a las empresas del sector de telecomunicaciones y de los medios de comunicación, creando un mercado virtual en el cual los usuarios ya no tienen necesidad de salir a los centros comerciales, esto al inicio de la Internet era muy distantes, pero en la actualidad a tomado nuevas vías hacia ese nuevo mercado en la medida que se desarrolla la economía digital, de la misma manera, el Estado, que en un principio no lo tomó en cuenta y se mantuvo alejado de Internet, y empieza a intervenir progresivamente conforme la Red de Redes de la Información de Internet se convierte en un medio social, cultural y político con una importante expresión de conflictos y poderes, por que de la misma forma en que nacen los colonos de esta cibersociedad como son los usuarios o cibernavegantes, y los comerciantes virtuales, así como las empresas digitales, hay quien trata de regularlo como son las policías virtuales, los centinelas del futuro, se crean nuevas leyes para la Red Mundial de Información, pero de la misma forma con este nacimiento de cultura nacen delincuentes, nacen lo que podemos decir de manera intangible Giros Negros Virtuales, Hackers, Crackers, y muchos otros individuos que se esconden detrás de esta Red de Comunicaciones parea hacer los fechorías.

Es como si habláramos de personajes sacados de una película de ciencia ficción, los centinelas o policía cibernética se enfrentan a sus enemigos en la red electrónica, los Hackers quienes son especialistas en informática, los cuales que utilizan sus computadoras para combatir a las grandes corporaciones financieras o a los gobiernos más poderosos del mundo, hasta los simples cibernavegantes o usuarios comunes. Estos Agresores virtuales no necesitan armas ni tener en muchos casos dinero para convertirse en una potencia agresora del ciberespacio, sólo sus amplios conocimientos en sistemas de información y de la Red Mundial de Internet, para poder violentarla.

Las actividades de los Hackers no son nuevas, son tan viejas como la misma Red de Información de Internet. La mayoría de ellos forman una comunidad muy cerrada y en ocasiones, sus actividades son relacionadas con otros movimientos sociales. Por ejemplo, podríamos decir que algunos de estos son activistas con los conocimientos de los Hackers, se dedican al espionaje de las potencias para saber cuales son sus actividades clandestinas que puedan dañar a la ecología, o bien ante la guerra de Estados Unidos de América en contra de Afganistán, estos activistas a favor de la paz utilizan la Red de Información de Internet a través de comunicación electrónica para hacer circular miles de cartas y manifiestos dirigidos a gobiernos, políticos y organizaciones de todo el mundo para difundir un mensaje humanista, en contra de la guerra y pidiendo por la paz.

Pero también hay cibernavegantes que no emplean sus conocimientos para hacer labores humanitarias y pacifistas, hay otros que emplean esos conocimientos para entrar en Internet y hacer de el un campo virtual de batalla. Los Hackers que usan la red para actividades ilícitas, de muchas maneras, podemos señalar que los delitos fueron trasportados virtualmente a la Red Mundial de la Información, que también funcionan para estos como los vínculos de tráfico de armas, blanqueo de dinero, narcotráfico, tráfico de órganos y personas, pornografía, todo tipo de crimen organizado, incluido el terrorismo, ya que sin ser un Hacker podemos encontrar en la Red de Información de Internet, manuales par crear bombas caseras, rifles caseros, propuestas de venta de artículos que prohíben las leyes de diversos países.

Así también, gobiernos, servicios de inteligencia y secretos, pequeñas y medianas empresas y grupos terroristas o racistas utilizan el Internet para difundir sus ideas, buenas o malas, conocer los secretos de sus enemigos u otros usuarios y causarles algún tipo de daño. Gracias a una tecnología tan cambiante todos estos usuarios han aumentado también su capacidad y velocidad para actuar en la Red de la Información de Internet con la utilización de tecnología de punta. Muchos de los servicios vitales, empresas privadas, oficinas de gobiernos ya están conectadas a la Red de Información de Internet y en caso dependen de ella, y esto las ha llevado a ser o que se han vuelto más vulnerables, en otras palabras, si un pequeño grupo de personas penetra las computadoras que controlan la red podrían cortar la electricidad e intervenir los principales servicios de una ciudad causando el caos. Así las comunicaciones, centro de la economía y la seguridad mundiales, empresas millonarias, y los gobiernos se han convertido en un objetivo militar, el ciberespacio es el

centro de operaciones donde se libran algunas de las batallas entre Hackers, militares y de inteligencia más importantes del mundo moderno, y no sólo hablamos de una guerra de agresión a estos sino también en la guerra de propaganda como en el bloqueo de los sistemas de información y defensa de algunos países para estos usuarios agresores.

Los cientos de atentados y los ataques electrónicos en la Red Mundial de la Información de Internet, demuestran que en la actualidad no se requiere de grandes aviones y bombas de alto poder para librar una guerra. A lo largo de esta investigación veremos como las principales amenazas a la seguridad son los virus, el hackeo, el pirateo, la negación de un servicio, la invasión a la intimidad de una persona, el espionaje, la intervención, la identidad falsa y los daños técnicos que se pueden realizar a través de este medio como los apagones. Por esta razón, no vamos a dejarle todo el crédito de estas actividades a los Hackers sino que de la misma forma el tener la capacidad de sabotaje, espionaje, robo de información, vigilancia de los mismos correos electrónicos es hoy uno de los objetivos militares de todo país que busque combatir a otros gobiernos o acabar con grupos terroristas. Las estrategias de sabotaje, espionaje y demás en el ciberespacio sólo requieren de conocimientos para atacar sistemas, escribir códigos de virus y espiar mediante mecanismos electrónicos tradicionales, robar información haciendo un traspaso de información. Es una forma eficaz, barata, efectiva y audaz, de atacar los objetivos militares y civiles.

Hay personajes que dicen que en momento que un usuario se encuentra conectado a la Red de Información de Internet, ya su información es pública, y que abogan por la libertad de información espían y sacan información secreta para ponerla a disposición del público, pero no es así, todos los ciudadanos tenemos el derecho a la intimidad, tener sus secretos, mientras no afecten a otras personas, no hay motivo por el cual se le tenga que violentar su información, o aun más robársela, obtener datos susceptibles a este y tal vez hasta extorsionarlo, o simplemente con que algún usuario entre a un equipo de computo ajeno y lo dañe, tal vez al lanzarle un virus que dañe su software o hardware o moviendo su información que este almacena.

Durante la investigación de este tema vamos a ver los distintos tipos de agresores, así como cual es la forma en la cual pueden dañar, cómo nace una cibersociedad la cual es creada con la tecnología actual, la legislación que hay en materia de delitos informáticos en relación a la violación a nuestro derecho de privacidad, así como los tipos de derechos que

hay comparando cada uno de ellos, tal vez esta investigación, llevará a pensar que nuestra sociedad actual esta cambiada por este tema y que la Red de la Información de Internet se ha vuelto la clave de la globalización, ya que no sólo a través de está se realizan las principales transacciones económicas del mundo, al mismo tiempo sirve para difundir ideas de modos de expresión de diversos usuarios, podemos tener conocimientos, a través de publicaciones las cuales son actualizadas constantemente, podemos conocer la historia de un país, un rey hasta indicaciones de cómo actuar en caso de ataques bacteriológicos o manuales para construir bombas. La Red de la Información de Internet, es una gran herramienta para la humanidad, hay que conocerla y aprender de ella.

Si bien es cierto que en la Red Mundial de Internet existe información, y todos tenemos el derecho a ella, pero también así tenemos un derecho, el cual es, el derecho a la confidencialidad o privacidad en nuestros documentos, archivos, números confidenciales y es mas a un, a no ser objeto de espionaje por este medio. Muchos de nosotros tenemos un servicio de Internet, pero no tenemos conocimiento de hacia donde dirigirnos para poder proteger nuestra información o denunciar un hecho que violento sus intereses.

La aportación original que se pretende plantear es exponer la urgencia que tiene México para canalizar y modificar las ya existentes para poder sancionar este tipo de conductas, así bien el desarrollo de las llamadas sociedades inteligentes que son las encargadas de vigilar los servidores de Internet, y la exigencia que se le debe realizar las compañías que suministran este servicio para llevar acabo vigilancias y registros en caso de que exista este tipo de violaciones y daños a el equipo de cómputo de un usuario.

El último capítulo de está investigación tomando ideas de muchos autores, trato de anexar a quien es competente el poder sancionar un ataque de cualquiera de los sujetos existentes en Internet, que pueda dañar tanto a los empresarios, gobierno federal o Estatal, así como a los usuarios comunes, que simplemente navegan en la amplia Red de la Información de Internet en busca de conocimientos, y es más por que no de ocio, todos tenemos derecho a nuestra privacidad, a guardar en nuestros equipos información confidencial, y nadie tiene el derecho de interferir en ello, siempre y cuando no dañe a terceros de ninguna forma.

Las infraestructuras electrónicas de comunicación como es la Red de Información de Internet ya actualmente son necesarias en todos los aspectos nos apoya en conocimiento, compras, diversión y mas aun contribuye al entendimiento internacional, al hacer un

alcance de muchas naciones, y tratando de eliminar barreras de distancia, pudiendo alcanzar conocimientos e información que no es en ocasiones fácil de entender. Es por esta razón y aún muchas más que la Red de la Información de Internet es muy importante para nuestra sociedad, hay que actualizar nuestras vidas, es simplemente inaceptable para todos cortar o destruir las líneas de comunicación tan importantes como el Internet u otro medio y en base a esta falta de aceptación hacer a una sociedad inconsciente de lo que pierde y así subir un ladrillo a una barda de concreto que aumenta la ignorancia.

Capítulo I

Marco Conceptual de la Informática

Capítulo I. Marco Conceptual de la Informática.

1.1. Concepto de Informática.

El término de Informática es una palabra que día a día es mas común en la vida de toda la sociedad, es decir tiene un gran desarrollo en la tecnología como en las actividades diarias del hombre, es en este tema que podemos destacar que la humanidad deber de empezar a desarrollarse a tal grado de conocer todo lo que la informática implica.

Luego entonces, la palabra informática la encontramos en Francia en los años setenta, que nos dice: "INFORMATIQUE, de information automatique."[1] De la definición anterior se puede entender que la definición de Informática, se refiere al almacenamiento de la información autentica, como el desarrollo de un nuevo modo para llevar a cabo el trabajo del hombre, como ya vimos las computadoras se desarrollaron para que la humanidad pueda mejorar su forma de trabajo en cuestiones que podían tardar años o bien eran actividades inexactas, podemos recordar el trabajo de Herman Hollerith, el cual gracias a la creación de las tarjetas perforadas, facilitó el censo de Estados Unidos en 1890, el cual tardo 2 años a diferencia del censo de 1880 el cual llevo siete años y medio en poderse terminar, esto demostró que de 1880 a 1890 la población creció de 50 a 63 millones de habitantes, esto es que aumento 13 millones, demostrando que el uso las máquinas daban mayor efectividad y rapidez, registrando la información real, ya que cuando los censos duraban muchos años al terminar era totalmente incierto el resultado.

Otro concepto que podemos citar es el de Téllez Valdés Julio, quien en un sentido general nos dice que *"la informática es un conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una mejor toma de decisiones desde el punto de vista de un sistema integrado"*[2].En este concepto de Telles Valdéz podemos expresar que la informática es el almacenamiento real de determinada información a una base de datos, esta información se obtiene, como hemos visto por medio de determinado lenguaje que ha ido evolucionando y de aquí podemos desprender el análisis de la palabra informática.

La informática es entonces una actividad que no se estanca ni en la información ni en su estudios, esto es que conforme a su uso se va enriqueciendo, para que las nuevas

---

[1] ACEDO QUEZADA, Octavio R. Cursos de Informática en la escuela de Derecho, en Revista Tribunal, Poder Judicial de Jalisco, 1997, número 4 Pág. 35.

[2] TÉLLEZ VALDÉS, Julio. Derecho Informático, Segunda edición. McGraw Hill, 1999, Pág. 6.

generaciones sigan con esta actividad alcanzando el desarrollo y la gran actividad de las telecomunicaciones actualmente, para que su uso no se límite a unos cuantos, sino que se desplace a un número mayor de usuarios. Este desarrollo de la informática nos permite actualmente presenciar evolución de esta, la informática es una de las actividades que llevara a partir de nuestra generación un gran arraigo y hasta el futuro. Cabe destacar y nombrar que la aparición del vapor junto con la Revolución Industrial llegó a la vida de millones de personas las cuales les cambió su vida, así como en la actualidad la aparición de los ordenadores de información, de los sistemas o equipos de computo, Internet y equipos sofisticados nos están cambiando la vida, y no solo eso, sino a futuro serán esenciales para el desarrollo de nuestra actividad cotidiana de cada uno de nosotros, lo cual será imprescindible el llevar una vida sin siquiera pensar en que el día de mañana habrá algún equipo sofisticado en base a una micro computadora que tendremos que aprender a utilizar.

Como dice Téllez Valdés que para el es la Informática: *"La Informática, junto con los micros, minis y macrocomputadoras, los bancos de datos, las unidades de tratamiento y almacenamiento, la telemática, etcétera, están transformando de manera indudable nuestro mundo."*[3] Este concepto de Téllez nos señala que las grandes y pequeñas computadoras son unidades de almacenamiento de datos, tanto personales como públicos como es el caso del Internet, que actualmente están cambiando nuestra sociedad y a través de estos medios podemos hacer actividades a grandes distancias.

Entonces gracias a estos conceptos podríamos decir que el mundo esta sufriendo y resintiendo cambios tanto económicos, políticos, sociales y aun más en el área del derecho, en el área de la tecnología que es la que esta cubriendo todos los puntos que se mencionan, la informática a través de la tecnología está tomando el control como de muchos están los ejemplos en bancos, teléfonos y muchos más, sobre todo por la gran ayuda que le presta a un hombre en su trabajo y desempeño.

---

[3]. Ibidem, p 4.

1.2. Concepto de Internet

Para poder conocer lo que es el Internet podemos señalar que gracias a la búsqueda de información, se han creado buscadores de información en Internet, los conocemos como las páginas a través de MSN, YAHOO y otros más, que se están convirtiendo en parte de nuestra vida cotidiana para poder obtener información de viajes, compras, Chat o foros de discusión, conocer en relación de noticias, poder conocer cuestiones de información científica y laborales, satisfacer curiosidad y muchas más actividades en el sistema de Internet según las necesidades de cada persona o usuario.

El concepto de Internet es algo sencillo de entender ya que este sistema es algo del cual todos nosotros hemos tenido contacto en determinado momento. Se puede definir Internet: *"es una red mundial de información compuesta por un enorme número de redes pequeñas interconectadas que vinculan decenas, centenas o miles de computadoras, permitiéndoles compartir información y recursos entre ellas."*[4]

En este punto no es algo muy difícil de entender, es simplemente un conjunto de computadoras interconectadas entre sí, esto es a nivel mundial, la red de Internet es un grupo de ordenadores conectados entre ellos.

Como podemos ver en otro concepto que señala algo similar: *"InterNet es un grupo de ordenadores de todo el mundo conectados entre sí. Hay ordenadores de todos los países." "InterNet es una red y una red es un conjunto de ordenadores conectados entre ellos."*[5] Ahora bien, en base a estos conceptos tan sencillos podemos hacer el señalamiento que el Internet es simplemente en la actualidad una parte de nuestra vida en la cual muchos de nosotros tomamos de ahí información y conocimientos para su consulta, es información de la cual día a día es actualizada y de la misma forma podemos conocer nuevas cosas del mundo.

1.3. Concepto de Cibernética.

> *"La Cibernética es la ciencia que se ocupa de los sistemas de control y de comunicación en las personas y en las máquinas, estudiando y aprovechando todos sus*

[4] http://webspcru.wperu.com/internet.html, Domingo 12 de octubre de 2003. 12:14 PM.
[5] http://www.cronis.com/kids/okids1a2.html, Domingo 12 de octubre de 2003. 13:30 PM.

aspectos y mecanismos comunes. El nacimiento de la cibernética se estableció en el año 1942. La unión de diferentes ciencias como la mecánica, electrónica, medicina, física, química y computación, han dado el surgimiento de una nueva doctrina llamada Biónica, La cual busca imitar y curar enfermedades y deficiencias físicas."[6]

Otro concepto similar de la palabra Cibernética nos dice: *"La Cibernética fue definida en 1949 por Norbert Wiener en su obra "Cibernética o control y comunicación en el animal y la máquina", como la ciencia que estudia los sistemas de control y especialmente de autocontrol tanto en los organismos como en las máquinas. El control, según Wiener, no es sino "el envío de mensajes que efectivamente cambian el sistema receptor", por tanto la cibernética investiga los problemas que plantea el envío, la transmisión, la recepción, la retención y traducción de mensajes. Estos problemas pueden estudiarse en organismos vivos con sistema nervioso cerebro-espinal o en estructuras físicas artificiales. El concepto de Cibernética involucra necesariamente entonces al de mensaje y al de información. La información consiste en un cierto número de datos..."*[7]

El nacimiento de la palabra Cibernética se da en el año de 1942, durante la celebración de un congreso de la inhibición cerebral en Nueva York, de la cual se fundieron ideas entre fisiólogos y técnicos en mecanismo de control.

"Cinco años más tarde, Norbert Wiener uno de los principales fundadores de esta ciencia, propuso el nombre de cibernética, derivado de una palabra griega que puede traducirse como piloto, timonel o regulador. Por tanto la palabra cibernética podría significar ciencia de los mandos. Estos mandos son estructuras con elementos especialmente electrónicos y en correlación con los mecanismos que regulan la psicología de los seres vivientes y los sistemas sociales humanos, y a la vez que permiten la organización de máquinas capaces de reaccionar y operar con más precisión y rapidez que los seres vivos, ofrecen posibilidades nuevas para penetrar más exactamente las leyes que regulan la vida general y especialmente la del hombre en sus aspectos psicológicos, económicos, sociales etc."[8]

También dentro del campo de la Cibernética se incluyen las grandes máquinas con inteligencia artificial, calculadoras toda clase de mecanismos o procesadores que pueden

---

[6] http://www.monografias.com/trabajos/cibernetica/cibernetica.shtml, Martes 14 de octubre de 2003. 12:30 PM.

[7] CARENA, Juan C. y FERRANTI, Liliana. Universidad Católica de La Plata –Unidad Académica Rosario Moreno 1056-200 Rosario. http://www.psicologia-online.com/ciopa2001/actividades/59/. Martes 14 de octubre de 2003, 15:30 PM.

[8] http://www.monografias.com/trabajos/cibernetica/cibernetica.shtml, Martes 14 de octubre de 2003. 12:00PM.

llevar el control de determinado equipos como por ejemplo, podríamos nombrar a un edifico inteligente, podemos señalar que la Cibernética es una ciencia que trata de ayudar a la humanidad a obtener grandes progresos y no se limita a lo mecánico, sino abarca también al campo de la electrónica.

Se mezcla la Robótica y la Cibernética para poderse aplicar en la informática al diseño y empleo de aparatos mecánicos, con inteligencia e información para poder desempeñar determinada tarea, trabajos que requieren una manipulación rápida y exacta que un ser humano no puede llevar a cabo con esta delicadeza que puede llevar una máquina especialmente diseñada para ello, hay que señalar que durante el desarrollo de la humanidad durante estos últimos años existe un gran desarrollo en la Inteligencia Artificial, que requiere aplicaciones de la cibernética aplicada a la informática para la creación de computadoras con gran capacidad de guardar información y con la capacidad de ser programada para mejorar la vida del hombre y su trabajo.

1.4. Concepto de Servidor.

En base a la investigación son escasos los conceptos de servidor pero podemos empezar este rubro haciendo una explicación de este en base a lo analizado, esencialmente un Servidor es un proveedor de Internet, un servidor es aquel que siempre se encuentra conectado a Internet, y que forma parte integral de este, es decir se requiere una computadora personal, y quien suministre el servicio de Internet.

Aquí entra la calidad de usuario y proveedor, ya que el usuario es el cual requiere que el primero le permita conectar su equipo de computo a su servidor de Internet los cuales conocemos como son MSN, YAHOO.COM, TODITO.COM, AOL.COM y otros los cuales no son más que una conexión a una base de datos e infinidad de información, el usuario ordinario no puede manejar esta información, sólo puede acceder a ella y conocerla pero no puede modificar nada de lo que ahí se encuentre, es decir toda lo que podemos encontrar en la Red de la Información de Internet, es Información de la cual nosotros no podemos realizar modificaciones. Son objeto de consulta sólo pueden ser modificadas o bien dar la autorización de su modificación los que la crearon entrando al servidor e ingresando determinadas claves de acceso a esa, o bien a menos que seamos Hackers.

En otras palabras y de una manera más sencilla el Servidor no es más que el proveedor o la manera por medio de la cual un usuario dueño de un equipo de cómputo puede acceder por medio de esta a un mundo de información en la red de Internet.

> *"Acceso simultáneo a la base de datos: InterBase habilita a un ilimitado número de aplicaciones cliente para acceder simultáneamente a la misma base de datos. Con la aparición de las bases de datos relacionales, entró en escena un nuevo concepto: EL SERVIDOR DE BASES DE DATOS. Ahora ya no es el propio programa el que realiza las operaciones, sino el servidor. El programa cliente simplemente "pide" datos al servidor y el servidor realiza la operación. Implementar concurrencia, transacciones, operaciones atómicas..."*[9]

1.5. ¿Qué es un Cibernavegante en la creación de una Cibersociedad?

Para poder comprender lo que son los Cibernavegante es necesario decir que no es más que un usuario de Internet, son aquellas personas las cuales entran a la red de la información en Internet para así formar parte de ella. En el Ciberespacio, una palabra tan utilizada por estos navegantes, al conectarse los usuarios a la red de Información, se convierten en Cibernavegantes en un Ciberespacio amplio de información, podríamos decir que estas dos palabras de Cibernavegante y Ciberespacio nos lleva a crear una Cibersociedad.

La integración de las Tecnologías de la Información en nuestra sociedad está provocando cambios profundos en la estructura económica y social de la misma y está teniendo unos efectos inmediatos en los usuarios de Internet. Cómo son valorar los efectos de la tecnología de la información en la sociedad a través de la Red de la Información, así como también cuál es realmente el impacto de las de está a la sociedad actual. En torno a este tema podríamos calificar a esta sociedad como Cibersociedad o bien Sociedad del Conocimiento su valoración e identificación real dependerá de números, diferentes que los identifican unos de otros en la Red de la Información podemos encontrar algunos conceptos de la Cibersociedad en la Red.

Al entrar un usuario a la red de información se convierte en un navegante, en un Cibernavegante en la red de información que es el Ciberespacio.

---

[9] http://www.servisoft.es/htm/base_datos.htm, Jueves 16 de octubre de 2003. 12:30 PM.

Podemos apreciar lo que es la creación de la Cibersociedad, para los usuarios de Internet, en un concepto bastante explicito en el cual hacen una detallada explicación de esta, y también nos dicen que:

> *"CiberSociedad es el concepto que hemos escogido para referirnos a lo que otros llaman Internet, Nuevas Tecnologías de la Información y la Comunicación (NTIC), Ciberespacio, etc. Existe un gran número de palabras y conceptos para referirse a "todo esto" y nuestra elección no es, en ningún sentido, casual. Se trata de reconocer que el componente más importante de "todo esto" es la sociedad que lo usa. La perspectiva de nuestro Observatorio para la CiberSociedad (OCS) proviene de las ciencias sociales y humanas, de modo que no resulta extraño que la primera de nuestras "cruzadas" sea contra el "tecnocentrismo" que sufren la mayoría de aproximaciones divulgativas al fenómeno de Internet. Hablar de Cibersociedad, para nosotros, implica hablar, en primer lugar, de la sociedad, de la gente interconectada, en un contexto tecnológico, comunicativo, laboral, económico, etc. que se ha visto considerablemente alterado por la aparición y popularización de los diversos instrumentos y ámbitos a los que llamamos, conjuntamente, 'Internet'."*[10]

En pocas palabras un Cibernavegante es aquel Usuario de Internet que se conecta a través de un servido y así va a tomar un lugar en el Ciberespacio, este Usuario es parte de un Ciberespacio que forma parte de una nueva Cibersociedad.

1.6. Conexión a Internet.

Muchos de los que conocen o usan el sistema de Internet tiene el conocimiento de que para poder acceder al servicio, es conectarse a el vía telefónica o bien por otro medio, es que la relación funciona como a través de un cliente y un servidor o proveedor, a través de una computadora, aquí podríamos calificar este tipo de relación como, a aquel que es el servidor es también un proveedor de información; mientras que el cliente, es el receptor de la información, los cuales van a funcionar a través de una línea telefónica, un equipo celular, computadora de mano, y aún algunos nuevos servicios como banda ancha, o bien vía satelital, estos dos últimos son pioneros en nuestro país, ya por lo general estos servicios

[10] FERNÁNDEZ MUERZA, Alex. Observatorio para la Cibersociedad, http://www.elprincipe.com/teleformacion/notas/index55.shtml, Lunes 13 de octubre de 2003. 12:00 PM.

son utilizados en empresas grandes y aun así, no es preferido, ya que en la mayoría de los lugares el acceso a Internet por medio de líneas telefónicas.

Una explicación más detallada de lo que es la conexión a La Red de la Información de Internet señala:

> *"La computadora cliente accede a Internet a través de una línea de comunicación de datos -por ejemplo una línea telefónica- y un ISP, Internet Service Provider, empresas que proveen el servicio de acceso a Internet. Para evitar confusiones, cada computadora tiene asignado un número único que la identifica -el IP-, este número es asignado por el ISP. Una vez que la computadora cliente se conecta al servidor que contiene la información requerida, éste se la envía en forma de paquetes que se enumeran y marcan con la dirección de la computadora destino. Luego se distribuyen por la Red para su entrega. Del otro lado, la computadora destino recolecta los paquetes y los reensambla, dejando los datos como estaban originalmente para ser vistos por un programa especial llamado navegador o browser."*[11]

También existen otros medios para la conexión a Internet, como son los medio de banda ancha, que es un sistema de comunicación a la red por medio de un cable más ancho que el tradicional de teléfono, por ello es que es llamada banda ancha, la única empresa que tiene este servicio para México es a través de Cablevisión podemos encontrar un poco de lo que es este sistema; lo cual sintetizamos señalando que es un cable módem general, el cual es un cable ancho, similar al cable de antena, pero en este caso sirve para transmitir el sistema de Internet, el cual permite conectar la computadora en el hogar o negocio a una red de datos cable, aquí como señalamos y recordando que este sería el servidor o proveedor. Esté permite el acceso a alta velocidad a la Internet, este cable módem es el llamado dual o coaxial de uso común para la televisión, el cual simplemente se conecta a la red sin utilizar la línea telefónica.

1.6.1. Intranet.

Esa una derivación del sistema de Internet, esto es que este sistema es esencialmente ocupado por las empresas e instituciones a nivel interno, es un sistema por medio del cual se puede compartir toda clase de información entre ellos, esencialmente es un servidor

[11] http://websperu.wperu.com/internet.html, Domingo 12 de octubre de 2003. 12:14 PM.

interno, el cual deja libre la información para los usuarios de la empresa, y cuenta con un correo electrónico con las mismas características que un correo externo, es decir, es compatible con todos los equipos, fabricantes, redes, y medios de transmisión.

"Con estas premisas, una idea muy interesante es utilizar las tecnologías de Internet dentro de una organización. En ello se basan las llamadas Intranet, es decir, se aprovechan de las herramientas de Internet para su utilización interna dentro de las redes corporativas de la empresa."[12]

1.6.2 Extranet.

"La Extranet consiste en permitir que personas ajenas a la empresa, como nuestros clientes o proveedores puedan acceder a parte de la Intranet de la organización. Es decir, técnicamente se trata de que... permita también el acceso a usuarios externos, lo que complica los aspectos relativos a la seguridad."[13]

Aquí podemos resaltar que este sistema no tiene todos el acceso que podría tenerse en Internet, este tipo de acceso es exclusivamente a determinados puntos, esta información solo puede ser a productos, precios o bien informes internos que son de carácter público como es el caso de instituciones gubernamentales. De la misma forma el sistema de Extranet, es para algunas empresas un sistema de boletín al cual se pueden suscribir los interesados, cuando una persona necesita determinada información de alguna institución u organismos, simplemente se conecta a esta solicitando el sistema de boletín informativo y automáticamente se le informa día a día de los movimientos de la institución o bien de la información que requiera.

1.6.3. Internetting.

El sistema de Internet se baso en la existencia de varias redes independientes, como son Hotmail, Yahoo y otras así como la red pionera de ARPANET la cual ya hemos visto fue la red pionera en la comunicación de información, el Internet es un sistema que no funciona por un sistema previamente diseñado en basado a un modelo especifico, como pudiera ser una red de araña, si no que se puede basar en cualquier tecnología de red individual, podía

[12] http://www.ciberconta.unizar.es/LECCION/INTRANET/INICIO.HTML, Viernes 17 de octubre de 2003. 15:30 PM.
[13] http://www.ati.es/DOCS/internet/histint/histint1.html#conceptos, Viernes 17 de octubre de 2003. 12:00 PM.

ser seleccionada libremente por un proveedor e interactuar con las otras redes de niveles llamados trabajo de redes, esto es que las redes se conectaban a niveles de circuitos, esto es que se conectan simultáneamente entre si, para formar por decir algo un especie de red de araña, claro sin ser esté su diseño.

> *"En una red de arquitectura abierta, las redes individuales pueden ser diseñadas y desarrolladas separadamente y cada una puede tener su propia y única interfaz, que puede ofrecer a los usuarios y/u otros proveedores, incluyendo otros proveedores de Internet. Cada red puede ser diseñada de acuerdo con su entorno específico y los requerimientos de los usuarios de aquella red. No existen generalmente restricciones en los tipos de red que pueden ser incorporadas ni tampoco en su ámbito geográfico, aunque ciertas consideraciones pragmáticas determinan qué posibilidades tienen sentido. La idea de arquitectura de red abierta fue introducida primeramente por Kahn un poco antes de su llegada a la DARPA en 1972. Este trabajo fue originalmente parte de su programa de paquetería por radio, pero más tarde se convirtió por derecho propio en un programa separado. Entonces, el programa fue llamado Internetting. La clave para realizar el trabajo del sistema de paquetería por radio fue un protocolo extremo a extremo seguro que pudiera mantener la comunicación efectiva frente a los cortes e interferencias de radio y que pudiera manejar las pérdidas intermitentes como las causadas por el paso a través de un túnel o el bloqueo a nivel local. Kahn pensó primero en desarrollar un protocolo local sólo para la red de paquetería por radio porque ello le hubiera evitado tratar con la multitud de sistemas operativos distintos y continuar usando NCP."*[14]

1.6.4. Internet aplicación y funcionamiento.

El Internet es una herramienta muy potente en la actualidad, la cual nació a fines de los setentas y hasta nuestros días, pero al inicio de el Internet a servido en su aplicación tanto para la investigación y comunicación exclusivamente en los campos Académicos y Militares, de los cuales solo podía ofrecer un solo servicio, solo ejecutar programas de una computadora remota, con el tiempo se añadieron mas funcionamientos como el poder copiar archivos de una computadora a otra a distancia, enviar mensajes por medio del correo electrónico.

---

[14] Idem.

Por lo que respecta a la parte civil de la Internet y que es la que la mayoría de nosotros conocemos, su aparición se debe a que el número de ordenadores subió en los ochentas, las aplicaciones del Internet, su aplicación esencial es el poder obtener acceso a información sobre cualquier tema que se pueda imaginar, o bien obtener una conversación con otra persona por lo mas lejano que esta este, siendo el único obstáculo el idioma, a esta actividad se le conoce como conferencia a distancia o bien lo que se conoce popularmente como el chatear con otra persona, o bien se puede obtener otro tipo de comunicación como son las video conferencias, esto es poder mandar la imagen a distancia por lo más lejos que esta sea vía Internet a otro usuario o un grupo de estos por medio del Internet a través del medio que se conoce como Net Meeting, lo cual podríamos decir que es el conocerte a través o por medio de la red, sin más inconveniente que la distancia que pudiera separar a los conferencistas.

De la misma forma el Internet nos proporciona: *"juegos, lectura de noticias, participación en discusiones, investigación, software gratuito compras, música e inclusive la posibilidad de aprender a distancia. Los negocios llevan acabo el comercio electrónico con sus proveedores y clientes a través de Internet y ésta permitida que la gente telenconmute o trabaje a distancia. Los ejemplos que se podrían citar de cómo está siendo utilizada Internet y de cómo está cambiando la forma de estudiar, trabajar, entretenernos y comunicarnos, son innumerables."*[15]

Ahora bien por lo que respecta a su funcionamiento del Internet, es que este esta formado por redes que tiene su propia directriz, esto es que no tiene una forma determinada para poder ser ella misma, no quiere decir que exista un desorden en ella ya que está formada de tal manera que requiere una mínima organización para que pueda subsistir, y por sí misma establece una serie de normas para los usuarios.

Solo podemos señalar como concepto que aparece en la Red Mundial de Internet que: *"En Internet no existe una empresa o institución que se encargue de forma global de la operación y explotación de la red, ese es un tema del que se ocupa el administrador de cada subred."*[16]

[15] http://webseperu.wperu.com/internet.html, Domingo 12 de octubre de 2003. 12:14 PM.
[16] http://www.nodo50.org/manuales/internet/1.htm, Domingo 12 de octubre de 2003. 15:30 PM.

1.7. Virus Informático.

Durante el inicio de la historia el hombre a sido blanco de los virus que causan las enfermedades, durante décadas lucharon contra estos creando medicamentos, métodos para poder evitarlos y protegerse de ellos, evolucionando de tal manera que se han creado medicamentos que pueden ayudar a la salud del hombre, para así hacerlo mas inmune a tales ataques. Este tema trata esencialmente de lo que es un virus pero no un virus común que puede dañar a una persona, trata sobre un virus especial que también puede dañar a una persona, y no sólo eso, igual que los virus que dañan a una sociedad creando una plaga, el virus que veremos es también un virus capaz de crear una plaga, pero sin peligro de dañar la salud de las personas, sino con la expectativa de dañar la economía de una nación e incluso de las potencias mundiales, ya que este virus puede desplazarse en cuestión de segundos de un continente a otro.

A lo que nos referimos es que este tipo de virus son denominados VIRUS INFORMÁTICOS, a diferencia de los virus que dañan la salud de las personas, los virus informáticos hacen daños económicos en las sociedades, causando estragos en esta, causando perdidas de información que pueden ser esenciales simplemente por el hecho de causar el daño, que en muchos de los casos es irreparable.

Para poder definir este tema es necesario el conocer el significado de lo que es un virus, y empezaremos por lo que es un virus que afecta la salud de las personas para poder diferenciar un Virus causante de enfermedad humana, animar o vegetal de un Virus Informático, el primero lo podemos definir como:

> *"Virus: Principio de las enfermedades contagiosas: Microbios invisibles al microscopio ordinario que tiene una dimensión inferior a 0,2 micras, que pasan a través de los filtros de porcelana y son causa de muchas enfermedades en el hombres (rabia, viruela, poliomielitis, sarampión, escarlatina, gripe), en los animales y en las plantas."*[17] Aquí se hace mención a un daño en la salud de un ser orgánico.

El Virus Informático también lo define el Diccionario Larousse como: *"Virus Informático, instrucción o conjunto de instrucciones parásitas introducidas en un programa y que pueden borrar la información que contiene"*.[18]

---

[17] GARCÍA PELAYO Y CROSS, Ramón. Pequeño Larousse Ilustrado, Edición Larousse, S. A. DE C. V. MARCELLA, 53, MÉXICO, 1992, Pág. 1067.
[18] Idem.

Pero no son las únicas definiciones que podemos encontrar ya que el lugar donde se encuentra infinidad de definiciones es en la misma Red de la Información, la Internet; en donde vamos a ver todo tipo de información en relación a los virus y su desarrollo:

> *"virus (virus) Programa cuyo objetivo es causar daños en un sistema informático y que a tal fin se oculta o disfraza para no ser detectado. Estos programas son de muy diversos tipos y pueden causar problemas de diversa gravedad en los sistemas a los que infectan. Hoy día se propagan fundamentalmente mediante el correo electrónico. Ver también: "antivirus", "e-mail ", "malware ", "program", "Trojan Horse ", "worm "."*[19]

Otro significado indica: *"Un virus es un programa que puede ingresar en un sistema a través de cualquiera de los métodos de acceso de información externa, se instala, se reproduce y causa daño. La gravedad de los virus es variable, puede ser simplemente una molestia en la pantalla, como el caso del "ping-pong" y también existen aquellos que pueden llegar a eliminar el contenido de una base de datos."*[20]

Como podemos ver el significado de un Virus Informático es similar para los autores y podemos desprender que el Virus informático, puede causar un daño extremo en nuestras computadoras, o bien una simple molestia esta puede ser desde que nuestro equipo de computo se pasme congelando la actividad y no nos deje trabajar en el o bien no guarde nuestra información, hasta la pérdida de la información que queremos almacenar, esto es como lo vimos al inicio de este tema que puede ser un virus tanto inofensivo como maligno, aquí podemos señalar que son virus que en la actualidad y gracias a la evolución de la tecnología es algo raro de señalar pero este virus afecta a las maquinas o sea no son inmunes a daños casados por una enfermedad cibernética, causada por la evolución de las máquinas.

1.8. Concepto de Delito.

Nuestro Derecho Penal, contempla el concepto de delito tanto en el fuero común como en el fuero federal, y ambos coinciden en señalar que nuestras leyes penales se encargan de tratar de salvaguardar a la todos aquellos que se encuentran bajo la protección de estas,

---

[19] FERNÁNDEZ CALVO, Rafael. Glosario básico ingles-español para usuarios de Internet, versión HTML4.0 (julio 2001) de la cuarta edición (mayo2001), http://www.alax.net/Library/diccionario.html#V. miércoles 01 de octubre de 2003, 12:00 PM.

[20] VIEGA RODRÍGUEZ, María José. Delitos Informáticos, http://derecho.org/comunidad/mjviega/deli_inf.htm. miércoles 01 de octubre de 2003, 14:00PM.

hacen un intento por proteger la vida, integridad, derechos y propiedades, este último esencialmente se centra en la economía, aquí nuestra ley lo que trata de hacer es garantizar una pena de carácter pecuniario que pueda cubrir el daño hecho por una persona a otra en sus bienes o posesiones, en el Código Penal para el Distrito Federal y en el Código Penal Federal, nos dan el mismo significado de Delito como lo veremos en lo siguiente que nos señala:

"TITULO SEGUNDO

EL DELITO

CAPITULO I

FORMA DE COMISIÓN

Artículo 15. (Principio de acto). El delito solo puede ser realizado por acción o por omisión.

Artículo 17. (Delito instantáneo, continuo y continuado). El delito, atendiendo al momento de consumación, puede ser:

I. Instantáneo, cuando la consumación se agota en el mismo momento en que se han realizado todos sus elementos de la descripción legal;

II. Permanente o continuo: cuando se viola el mismo precepto legal, y la consumación se prolonga en el tiempo, y

III. Continuado: cuando con unidad de propósito delictivo, pluralidad de conductas e identidad de sujeto pasivo, se concretan los elementos de un mismo tipo penal."[21]

Así como de la misma forma el Código Penal Federal nos dice:

TITULO PRIMERO

RESPONSABILIDAD PENAL

CAPITULO I

REGLAS GENERALES SOBRE DELITOS Y RESPONSABILIDAD

Artículo 7. Delito es el acto u omisión que sancionan las leyes penales.

En los delitos de resultado material también será atribuible el resultado típico producido al que omita impedirlo, si éste tenía el deber jurídico de evitarlo. En estos casos se considerará

[21] Nuevo Código penal del Distrito Federal. Editorial Sista S. A. de C. V. México D. F. 2003.

que el resultado es consecuencia de una conducta omisiva, cuando se determine que el que omite impedirlo tenía el deber de actuar para ello, derivado de una ley, de un contrato de su propio actuar precedente

El delito es:

I. Instantáneo, cuando la consumación se agota en el mismo momento en que se han realizado todos sus elementos constitutivos;

II. Permanente o continuo, cuando la consumación se prolonga en el tiempo, y

III. Continuado, cuando con unidad de propósito delictivo, pluralidad de conductas y unidad de sujeto pasivo, se viola el mismo precepto legal[22]

En este orden de ideas que nos da nuestra legislación, podemos comprender que el ser humano es el único con la capacidad de someterse a los preceptos jurídicos, ya que todos lo seres humamos tenemos la capacidad intelectual de comprender entre los actos bueno y malos que pueden dañar a nuestros iguales, y poder llegar a crear un desorden en la convivencia social.

En los casos que atañen a los daños que se realizan a los equipos de cómputo, no crean un desorden de convivencia social, pero si crean un desorden en cuestiones de daño a la posesión de terceras, cuartas y más personas.

Nuestras leyes tiene el fin de crear la justicia, que se conoce como el equilibrio que hay entre los actos creados por los hombres, actos que pueden ser encaminados al daño a segundas y terceras, siendo estos regulan por los actos jurídicos creados por los legisladores.

1.9. Concepto de Delito Informático.

No es muy adecuado hablar de un delito informático, esto es por que, como sabemos, que como tal, es decir no existe. En el ámbito de lo que actualmente esta naciendo como lo que llamamos "Derecho Informático". Pero podemos destacar que la Informática y el Internet es una herramienta creada por el hombre y para los hombres, y por esta razón hay que señalar, que el empleo que de esto se desprende, es su responsabilidad, así también como en México en muchos países a existido mucho debate sobre lo que son Delitos Informáticos,

[22] Código Penal Federal, Compendio de leyes, reglamentos y otras disposiciones conexas sobre la materia 2003. grupo ISEF. México D. F. 2003.

podemos nombrar diversos ilícitos que crea el hombre ocultos tras la Red de l información, la piratería de las cuales es una práctica muy común, que consiste en lo que es hacer copias de determinado artículo y venderlo a más bajos costos o también conocido como falsificación así como sucede en la vida cotidiana, sucede en la red de la Información de Internet, como es la falsificación de algunos software que se duplica y ponen a la venta para hacer un lucro económico sin tener los derechos de este, ahora bien, vamos a nombrar también algo muy nuevo que se presenta por Internet, como el Fraude electrónico, sucede cuando hay vendedores que usan el medio de Internet para hacer ventas fantasmas, el comprador nunca recibe el artículo que deseaba comprar, Publicaciones Ilícitas, sucede cuando un usuario publica en la Internet fotos o anuncios ilegales como pueden ser fotos dirigidas a pedofilos, especulaciones y rumores a personas publicas, como sucede en nuestra vida común al revisar una revista en la cual se hacen publican artículos sin tener pruebas de lo que se da conocer al público, manipulación en el mercado de valores, el cual se presenta cuando usuarios conocen de informática y entran a la Red de Información para manipular dolosamente la información de esta mercado para obtener un lucro y sin dejar a un lado lo que es importante para este teman de investigación que es el robo de información, espionaje, manipulación de nuestra información en las propias computadoras lo comúnmente llamado hackeo, que es como en un juego de ajedrez poner en hacke, solo que en este caso, el hacke no es sino que una intervención de la información a los equipos de computo a través de Internet, esta actividad es común por los conocidos Hackers quienes son los usuarios que tienen conocimientos amplios en informática e Internet para poder violentar los equipos de computo.

Todos estos delitos informáticos que se pueden considerar un aspecto negativo del desarrollo de la informática y todo lo que esto emplea, como es el caso de la materia del derecho el ámbito de la conducta delictiva de los usuarios. Como todos nosotros hemos visto las computadoras han dado a los usuarios con finalidades negativas nuevos modos de hacer o causar un daño a personas que también son usuarios, y como hemos visto esto da modos nuevos para cometer nuevas faltas tradicionales pero de una manera ya mas sofisticada.

Para poder conocer lo que es Delito Informático la Dra. Maria José Viega Rodríguez, en su publicación en Internet nos da diversos conceptos de nuestro tema:

La Universidad Nacional Autónoma de México ha realizado un estudio en los cuales define a los delitos informáticos como: *"todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático".*[23]

Jijena Leiva lo define como: *"... toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma".*[24]

La Organización para la Cooperación Económica y el Desarrollo (OECD) da una definición que es considerada como "abarcante" y lo define como: "cualquier conducta, no ética, o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos".[25]

Todos estos conceptos nos dan la las nuevas posibilidades que la informática nos dan para la comisión de un delito o falta, esto es como hemos mencionado que las computadoras y el desarrollo de la tecnología han dado una nueva herramienta en la realización de determinadas acciones dolosas. Hay muchos tipos de delitos clasificados como delitos informáticos, de los cuales podemos señalar también;

1. Delitos contra la propiedad intelectual
2. Delitos contra la propiedad industrial
3. Delitos en contra la intimidad
4. Delitos contra el mercado
5. Delitos por daño o falsedad
6. Delitos por estafa
7. Delitos por injurias
8. Delitos contra la libertad: amenazas
9. Delitos por provocación sexual y prostitución

Por otra parte en la Red de la Información de Internet, en los que son las páginas Web nos hace un esquema sobre los tipos de delitos informáticos reconocidos por Las Naciones Unidas, para la cual le es importante este tema ya que afecta a todas las naciones del mundo las cuales están entrando en el mundo de la tecnología moderna.

---

[23] VIEGA RODRÍGUEZ, María José. Delitos Informáticos, http://derecho.org/comunidad/mjviega/deli_inf.htm. miércoles 01 de octubre de 2003, 14:00PM.
[24] Idem.
[25] Idem.

La información sobre tales delitos nos la proporciona dividiendo el texto en dos columnas: una para los delitos y otra para sus características. Esta estructura nos permite una rápida búsqueda para el delito informático en concreto que busquemos, y a la vez nos permite diferenciar unos de otros (piénsese en delitos aparentemente iguales).

Esta página se estructura como sigue:

- Fraudes cometidos mediante manipulación de computadoras.
  - Manipulación de los datos de entrada.
  - La manipulación de programas.
  - Manipulación de los datos de salida.
  - Fraude efectuado por manipulación informática.
- Falsificaciones informáticas.
  - Como objeto
  - Como instrumentos.
- Daños o modificaciones de programas o datos computarizados.
  - Sabotaje informático
    - Las técnicas que permiten cometer sabotajes informáticos son:
      - Virus
      - Gusanos
      - Bomba lógica o cronológica
    - Acceso no autorizado a servicios y sistemas informáticos
    - Piratas informáticos o hackers
    - Reproducción no autorizada de programas informáticos de protección legal.[26]

1.10. Conceptos generales empleados por los usuarios de Internet.

Para poder comprender bien este trabajo hay que poner en claro que los usuarios de la Red de la Información de Internet, hay que conocer por lo menos los significados más frecuentes de quienes la usan, así como algunos conceptos muy interesantes que se

[26] PÉREZ LOZANO, José Manuel. Universidad de Granada España, Delitos Informáticos, http://comunidad.derecho.org/plozano/webs_sobre_delitos_inform%E1ticos.htm, Domingo 26 de octubre de 2003, 12:00 PM.

desprenden del conocimiento del uso del Internet del cual son tomados de la misma red de información, estos conceptos son los mas esenciales como son:

Arroba @. Arroba Símbolo que se utiliza para separar el nombre del usuario del dominio en las direcciones de correo electrónico, por ejemplo: josue@podernet.com.mx ver: "e-mail address".

401 Unauthorized. (401 No autorizado). Es mensaje que nos indica que la página que queremos ver no se encuentra disponible y que no estamos autorizados a consultarla. 401 forma parte de una serie de códigos que en el año de 1992 el creador de la WEB Tim Berners-Lee adoptó de los que ya formaban parte del FTP (File Transfer Protocol). Ver: "404 Not found", "page", "WWW.

404 Not found. (404 No encontrado). Este mensaje es el más común cuando navegamos por Internet, nos aparece cuando una página no existe o ha sido movida de lugar, en resumen una página no encontrada. 404 forma parte de una serie de códigos que en el año de 1992 el creador de la WEB Tim Berners-Lee adoptó de los que ya formaban parte del FTP (File Transfer Protocol). Ver: "401 Unauthorized", "FTP", "HTML", "HTTP", "page", "WWW".

ADSL. Asymmetrical Digital Subscriber Line ADSL (Línea de Subscripción Asimétrica Digital). Se refiere a una tecnología para mejorar el ancho de banda de los hilos del cableado telefónico convencional que transporta hasta 16 Mbps (megabits por segundo) gracias a una serie de métodos de compresión.

Active Server Page. ASP (Página de Servidor Activo). Las páginas ASP, son un tipo de HTML que además de contener los códigos y etiquetas tradicionales, cuenta con programas (o scripts) que se ejecutan en un servidor Microsoft Internet Information Server antes de que se desplieguen en la pantalla del usuario. Por lo general este tipo de programas realizan consultas a bases de datos, siendo los resultados de éstas los que el ususario final obtiene. La extensión de estos archivos es ".asp." Ver: "page", "JSP", "server", "HTML", "script".

ActiveX (ActiveX). Dentro de las aportaciones tecnológicas a Internet desarrolladas por Microsoft se encuentra el ActiveX que puede ser ejecutada sobre cualquier plataforma y por lo general a través de navegadores como Explorer o Netscape. Agrega dinamismo a las páginas y en ocasiones aporta al diseño de la misma. Ver: "applet", "Java".

Address (dirección). La manera en que navegamos por la red es a través de direcciones, ya sea para mandar un correo electrónico (e-mail address) o visitar una página (internet address), siempre necesitamos una dirección.Dicha dirección está formada por una serie de caracteres ya sea letras y números que nos llevan de manera única a la dirección determinada. Ver: "IP address", "email address", "site", "internet address".

Advanced Research Projects Agency. ARPA. (Agencia de Proyectos de Investigación Avanzada). En la actualidad es el nombre del organismo militar norteamericano que antes se llamaba DARPA. Ver: "DARPA".

Advanced Research Projects Agency Network.ARPANET (Red de la Agencia de Proyectos de Investigación Avanzada). Una de las primeras redes de computadoras interconectadas a través de líneas telefónicas. Este proyecto fue financiado por DARPA y sin duda constituye uno de los proyectos piloto que sirvió de base para el desarrollo de Internet. 7. APD (Data Protection Agency) - Agencia de Protección de Datos Fue en el año de 1993 cuando en España se crea con el fin de proteger la intimidad de los usuarios de Internet del ataque a su intimidad a través de medios informáticos. Esto se ampara en el artículo 18.4 de la Constitución Española. Ver también: "privacy".

Agent (agente). Dentro de lo que es el modelo del cliente-servidor, se refiere a la parte del sistema que realiza la preparación e intercambio de información por cuenta de una aplicación del cliente o del servidor.

Alias (sobrenombre, apodo). Se ha vuelto muy popular en los Chat, en los registros de páginas, etc. etc. la utilización de un "alias", el cual por lo general es de pocos caracteres, fácil de recordar y que en cierta, manera protege la intimidad de las personas.

Anonymous FTP (FTP anónimo). Este concepto se refiere a la utilización de un nombre de usuario anónimo (anonymous) dentro de un FTP en Internet para acceder a la información deseada sin necesidad de proporcionar un nombre (login) y contraseña (password). De esta manera se superan los mecanismos de seguridad teniendo acceso a los archivos disponibles para todo público que se encuentran en un servidor en cualquier parte del mundo. Ver: "archive site", "FTP".

Anonymous mail (correo anónimo). Se refiere a mandar correos electrónicos de manera anónima, en donde la dirección del remitente no aparece. Lo anterior se realiza a través de un protocolo implantado en el servidor. Esta práctica además de ser ilegal en muchos países, resulta poco ética al igual que en el correo convencional. Ver: "email".

Apache (Apache). Servidor de Internet que corre bajo la plataforma Linux, el cual fue desarrollado en 1995 y que en la actualidad acapara gran parte del mercado de servidores HTTP. Ver: "Free Software", "Linux"

Application (aplicación). Hace referencia a una acción que se realiza a través de un programa de manera directa con el usuario. Navegadores, chats, correo electrónico, etc. son algunos ejemplos de aplicaciones en el medio de Internet.

Application Program Interface API (Interfaz para programas de aplicación). Una serie de reglamentos y acuerdos que nos definen la manera en cómo llamar determinado servicio desde cierto programa.

Archie (archie). Aplicación de Internet ya en desuso cuya función era la de recopilar, listar y distribuir la información dentro de Internet de manera automátizada. Ver: "WAIS", "Gopher", "archive site".

Archive site (lugar de archivo, sitio de archivo). Es una computadora conectada a Internet que permite la obtención de archivos para los usuarios. El "anonymous FTP archive site", permite la obtención de dicho material mediante el protocolo FTP. Los servidores WWW pueden también emplearse como lugares de archivo. Ver: "archie","anonymous FTP", "WAIS" , "Gopher", "WWW", "site".

Artificial Intelligence. AI (Inteligencia Artificial). Interesante rama de la informática que se encarga del desarrollo de programas que tienen como base el razonamiento análogo del ser humano y aprovecharlos con fines tecnológicos.

Asymmetrical Digital Subscriber Line ADSL (Línea de Subscripción Asimétrica Digital). Se refiere a una tecnología para mejorar el ancho de banda de los hilos del cableado telefónico convencional que transporta hasta 16 Mbps (megabits por segundo) gracias a una serie de métodos de compresión.

Asynchronous Transfer Mode ATM (Modo de Transferencia Asíncrona). Dentro del medio informático hace referencia a la conmutación de paquetes (cells -- celdas o células) de un tamaño fijo con alta carga, rápida velocidad (entre 1,544 Mbps. y 1,2 Gbps) y una asignación dinámica de ancho de banda. También se conoce como "paquete veloz" (fast packet).

Attachment (documento anexo). Se denomina así al archivo que se manda junto con un correo electrónico. Dicho archivo puede ser de difeentes tipos tales como: texto

(Word, Excel, etc.) hasta imágenes (Gif, Jpg, etc.), sonido, etc. "MIME", "file", "e-mail message".

Authentication (Autentificación). Dentro de las medidas de seguridad que pueden llegar a implementarse en Internet se tiene esta que es una verificación de determinado usuario o proceso para tener acceso a cierto sistema, o realizar una operación en específico. Es aplicable también para verificar la identidad de origen de un mensaje.

Banner (anuncio, promocional virtual). Dentro del universo de Internet, la manera más popular de presentar la publicidad es a través de un banner, los hay de todos tamaños, su objetivo primordial es el de captar la atención del usuario y llevarlo a que haga "click" en ellos para llevarlos a los sitios que promueven.

Baud (baudio). En cuanto a la transferencia de información dentro de Internet, un baudio es el número de veces que se modifica el "estado" del medio que transmite en un segundo. El tiempo de descarga de la información se ve afectado directamente por esto la tasa de bits de datos transferidos en ocasiones puede ser superior a la correspondiente tasa de baudios. Ver: "bps".

Beeper (busca). Popular medio de comunicación en la actualidad que funcionan a través de vía satélite (amplia cobertura) o microondas (de manera local), para anunciar al usuario la llegada de un nuevo mensaje lo pueden hacer por medio de sonido ("beeps") o vibración. Los mensajes se pueden enviar vía telefónica o Internet.

Bounce (rebote). Esto sucede cuando se nos retacha o devuelve un correo electrónico ocasionado ya sea por un error en la dirección, una falla en el servidor, etc.

Browser (navegador, visor, visualizador). La manera como viajamos a través de Internet es por medio de un navegador. Se componen de aplicaciones de hipertexto que facilitan la comunicación con los diversos servidores en Internet, los más populares son Internet Explorer de Microsoft y Netscape de Netscape Communications. Nos permiten el acceso a servidores WWW, FTP, etc.

Bug (error, insecto, bicho). Se remonta este concepto informático al año 1945 cuando la ingeniera Grace Murray, valuarte en el desarrollo de la programación moderna notó como un insecto (bug) había hechado a perder uno de los circuitos de una computadora en la que trabajaba.

Bulletin Board System BBS (Tabla de Anuncios Electrónicos). Se trata de un servicio casi descontinuado en donde a través de una computadora y software se

proporcionaban servicios de mensajería y transferencia de archivos para operadores del BBS. actualmente han sido sustituidos casi en su totalidad por WWW. Ver: "WWW".

Buzón de correo electrónico. Se refiere al área que un servidor de correo electrónico reserva para que el usuario pueda almacenar sus mensajes de correo electrónico.

Bit (bit, bitio). Se trata de la unidad mínima de información que se maneja en una computadora. Se deriva de la contracción de la expresión binary digit (dígito binario). Ver: "byte"

Byte (byte, octeto). Dentro de las unidades de medición de memoria en las computadoras un byte representa la suma de ocho bits que forman un carácter. Ver: "octet", "bit".

Cache (caché, memoria de visitas). Es una copia que el navegador mantiene en nuestra computadora de las páginas visitadas recientemente, de esta manera si el usuario requiere volver a entrar a estos sitios ya lo hará a través de su disco duro y no desde Internet. La ventaja de este tipo de memoria es que nos disminuye el tiempo de carga de las páginas, la desventaja es que si la página sufre una actualización, nosotros no lo podremos ver porque tendremos la versión anterior.

Cc: (copia). Se trata de una de las líneas que compone la cabecera del correo electrónico y el objetivo es el de enviar de manera simultánea una copia del mensaje al número deseado de usuarios, cuyas direcciones de correo aparecen a diferencia de lo que sucede con los incluidos en la línea "Bcc". "Cc" es un acrónimo de la conocida frase inglesa "Carbon copy" (copia de papel carbón).

Censorship (censura). Algo muy difícil de conseguir es la sensura en un medio tan global y vertiginoso de comunicación como es el Internet. En este caso se trata de restricciones que algunos gobiernos o empresas privadas implementan para que cierto tipo de información no llegue a los usuarios, esto puede ser porque lo consideren no apto, no conveniente e inclusive peligroso. Ver: "Communications Decency Act".

Chat (conversación, charla, chateo, platicar). Los tan populares Chats en Internet representan la comunicación entre dos o más usuarios. Existen diversas plataformas y programas que se utilizan para Chats, los hay en modo Java, HTML, con imágenes, etc. etc. Los más vanguardistas permiten ya la transferencia de audio y video en tiempo real. La adicción a estos sitios puede llegar a convertirse en todo un vicio. Ver: "CU-SeeMe", "Internet phone", "talk", "chat room", "Internet Relay Chat".

Chat room (cuarto de charla, sala de charla). Se refiere a una especie de canal que se encuentra en algún lugar de la red, en donde se clasifican por temas específicos, diversos usuarios interesados en un tema en común ingresan al mismo para platicar. Ver: "chat".

Cookie (cuqui, espía, delator, fisgón, galletita, pastelito). Se trata de un conjunto de programas, en ocasiones encriptados en el mismo navegador que se almacenan en el disco duro de la computadora del usuario cuando éste entra a determinadas páginas en Internet. Numerosas protestas se han originado respecto al tema, ya que en muchas ocasiones las compañías utilizan esto para conocer las preferencias de los usuarios y de esta manera enfilar una campaña publicitaria. Ver: "website", "browser", "web server".

Copyright (derecho de copia). Los derechos que tiene un autor ya sea de un sistema, programa, hardware, etc. sobre todas y cada una de las obras que cree, así mismo establece las condiciones y el uso que se hará con respecto a la utilización y comercialización de las mismas. Este derecho es irrenunciable y las restricciones acerca de su uso quedan estrictamente bajo las condiciones que el autor decida. Para mostrar de manera este derecho se utiliza el símbolo: ©. Ver: "copyleft", "BSA", "software piracy".

Cracker (intruso, saboteador). Se define como un individuo cuyas malas intenciones lo llevan a tratar de entrar a una red o sistema burlando su seguridad. Son personas muy capaces y que cuentan con una serie de herramientas para lograr su cometido. Ver: "phracker", "hacker".

Cybernaut (cibernauta). Usuario que navega por la red.

Cybernetics (Cibernética). Proviene del vocablo griego "cibernetes", que se traduce como timonel o piloto, que se refiere a la ciencia o estudio de los mecanismos de control o regulación de los sistemas mecánicos y humanos, en esta definición también se incluye a las computadoras.

Cyberspace (Ciberespacio). Fue utilizado por vez primera en la novela "Neuromancer" de William Gibson en donde se aplicaba para describir un universo de computadoras y una civilización creada en torno a estas máquinas.

Data (datos). Plural de la palabra latina datum (dato). Puede caerse en el error al emplearse en inglés y pensar que se refiere a un solo dato.

Dialup (conexión por línea conmutada). Se llama así a la conexión de Internet casera, no temporal que depende de una línea telefónica normal. Para accesar a Internet es

necesario marcar un número telefónico, así como agregar un nombre de usuario y contraseña.

Digerati (entendidos). Dentro de la cultura de Internet se entiende como aquellas personas que se especializan en temas de la denominada Sociedad de la Información. Su raiz proviene del término latino ligerati (letrados).

Digital signature (firma digital). Se trata de un protocolo en Internet a través del cual se verifica la autentificación de un usuario y nos confirma que es quien dice ser.

Directory (directorio). Se dice de un espacio jerárquico que funciona como estructura en forma de árbol que contiene la información que se almacena en una computadora, que por lo general se organiza en archivos. Los directorios se identificana a través de un nombre, por ejemplo: "Archivos de programa".

Domain (dominio). Se trata de la dirección electrónica de una página de Internet, el cual se conforma de caracteres que lo identifican de manera única. Por ejemplo tenemos que la extensión de dominio que identifica a las páginas de Internet mexicanas es el ".mx", a las alemanas ".de", etc.

Download (bajar, descargar). Se denomina en Internet al proceso de bajar información desde un servidor que se encuentra en cualquier parte del mundo a nuestra computadora. Ver: "upload".

Electronic mail (correo electrónico). Sin duda alguna una de las más populares aplicaciones de Internet que ha cambiado la forma de comunicación de miles de personas en todas partes del mundo, de esta forma un usuario puede intercambiar información con otros desde puntos remotos. Se le llama así también a los mensajes que se manda a través de este medio. Ver: "electronic mail message".

Electronic mail address (dirección de correo electrónico). Es el conjunto de letras, números y signos que juntos dan por resultado al dirección de correo electrónico de un usuario. Técnicamente se compone de tres partes: el nombre del usuario, la arroba y el nombre del servidor, por ejemplo: heidi@podernet.com.mx. Ver: "e-mail", "domain".

Electronic Privacy Information Center EPIC (Centro de Información sobre la Intimidad Electrónica). Esta organización se formó en los Estados Unidos, es de caracter no gubernamental y su meta principal es la promoción de las libertades ya sea individuales o colectivas en la Sociedad de la Información.

Electronic publishing (publicación electrónica). Se trata de un sistema o metodología para la distribución de publicidad a través de medios digitales, ya sea Internet, CD-ROM, etc.

Extranet (Extranet, Extrarred). Es una arquitectura de comunicación entre dos empresas o compañías cuyos sistemas de comunicación se basan en Internet.

E-zine (revista electrónica). A últimas fechas pregonan en el ciberespacio las denominadas publicaciones electrónicas que tienen la gran ventaja de que no requieren ser impresas, evitando costos de papel y tintas entre otros.

Hacker (pirata). Persona de elevados conocimientos en el ramo informático que tiene la capacidad de violar los sistemas de seguridad de una computadora o una red, lo cual le provoca placer, este término no debe de llevarse al extremo de alguien malo con fines de destruir sistemas, esto encaja mejor en la definición de "cracker". Ver: "phracker", "cracker".

File (archivo, fichero). Es la base de la estructura de organización de la información en una computadora, de esta manera se puede manipular por el sistema operativo de la misma. Un archivo se compone de tres partes fundamentales: el nombre del archivo, el punto (.) y la extensión, de esta manera tenemos "ejemplo.html" (en este caso se trata de un archivo HTML cuyo nombre es ejemplo).

File transfer (transferencia de archivos) Es la acción que consiste en sacar una copia de un archivo de una computadora a otra a través de una red.

File Transfer Protocol FTP (Protocolo de Transferencia de archivos). Uno de los protocolos más utilizados en Internet lo es sin duda el FTP, el cual nos permite bajar información de los servidores que se encuentran en Internet, para lo cual debemos de teclear un nombre de usuario y una contraseña.

Filter (filtro). Se realiza para eliminar a todas aquellas direcciones de correo que no queremos que nos manden más, esto se genera de manera automatizada al introducir en el sistema determinadas palabras clave o nombres que queremos evitar tanto en los mensajes de entrada o de salida. Es muy útil para evitarnos esas molestas listas de publicidad o de sitios indebidos.

Firewall (barrera contra fuegos). Se denomina así al sistema de seguridad que se coloca entre la red local e Internet, de esta manera la empresa o compañía regulará completamente toda la comunicación hacia Internet estableciendo sus políticas de

seguridad. En ocasiones este sistema incorpora autentificación de usuarios entre otras cosas.

Free Software (Software Libre). Se trata de programas en donde cualquier usuario puede hacer uso de ellos, además si así lo requiere puede realizar modificaciones al código fuente, modificarlo según sus necesidades, mejorarlo, etc. Se debe hacer la aclaración de que un software libre no necesariamente es gratuito, esta confusión se ha generado porque en inglés el término "free" tiene el significado tanto de libre como gratuito.

Free Software Foundation FSF (Fundación para el Software Libre). Organización con sede en los Estados Unidos que tiene como objetivo la promoción del desarrollo y distribución del software libre en cualquier área de la informática.

Freenet (red libre). Un loable esfuerzo por fomentar la comunicación humana es este, en donde se promueve el uso de redes libres, cuyo financiamiento es a través de voluntarios. Entre muchos otros servicios se cuenta con correo electrónico, comunicación interactiva, videoconferencias, bibliotecas virtuales, etc. Una de las principales redes libres es la National Public Telecomputing Network (NPTN) en los Estados Unidos.

From: (de, desde). Se trata de una de las líneas que componen el encabezado de un correo electrónico y en donde va el nombre del emisor del mensaje. Por motivos de cortesía y buena educación en Internet es recomendable incluir el nombre y los apellidos, en caso de tratarse de una persona física, de ser una persona jurídica será necesario incluir la empresa a la que representa. Dichos datos son incluidos por el usuario en su editor de correo electrónico.

Global Information Infrastructure GII (Infraestructura Global de Información). Es un ambicioso proyecto a futuro, en donde se denomina así a la gran autopista de información que cubrirá por completo el planeta.

Globalization (globalización, mundialización). Se trata de un fenómeno que ha cobrado mucha fuerza a últimos días, fomentado ampliamente por el efecto Internet, en donde se traspasan fronteras y las distancias se acortan entre un país y otro en segundos, se da en todos los ámbitos, tanto social, cultural, económico, etc. Como todo en exceso es dañino, existen ya problemas generados a causa de la globalización y algunos países toman ya medidas para evitar un desajuste como el de la denominada "Tasa Tobin", que gravaría los flujos financieros internacionales.

Hacking (pirateo). Ver: "hacker".

Hardware (fierros, hardware, maquinaria). Se trata de todos los componentes físicos de una computadora, entre los cuales se pueden mencionar el disco duro, procesador, monitor, etc. que en conjunto con el software (programas) hacen que funcione nuestra máquina.

Header (cabecera). Se traduce como cabecera, que es el lugar dentro de los correos electrónicos en donde se coloca el remitente, la fecha, hora, etc. Otra definición de header se refiere a la parte de inicio en un paquete que viene antes de los datos propiamente dichos que contiene información acerca del remitente, control de fallos, etc. Ver:

Hoax (chisme exagerado). Muchas ocasiones se cunde el pánico por supuestos virus que se encuentran en Internet, estos chismes y rumores no tienen ningún fundamento pero son igual de dañinos que un problema real.

Hypertext (hipertexto). Mucho antes que el WWW fue creado el Hypertexto (texto que nos permite hacer ligas o referencias entre documentos) por el físico estadounidense Vannevar Bush en el año de 1945. Dentro del universo de Internet se aplica a todas aquellas páginas que se forman con el código HTML y que nos enlazan a otras páginas, las cuales son accesadas a través de un navegador.

Information (información). Se trata de la suma de varios datos que tiene un significado completamente distinto al de cada uno de ellos visto de manera individual. Por ejemplo j, o, s, u y e son datos, Josué es una información. Es un recurso invaluable dentro del desarrollo y expansión de las tecnologías.

Information Society (Sociedad de la Información). Se denomina así a la sociedad en que el poder de las computadoras y la tecnología en general repercute de manera directa en la mente, sentimientos y sueños del hombre.

Integrated Services Digital Network. ISDN (Red Digital de Servicios Integrados RDSI). La gran ventaja de este tipo de tecnología es que permite que los datos, conexiones de voz, etc. viajen a través de un solo cable. Actualmente este servicio es ofrecido por las principales compañías telefónicas a nivel mundial y goza de gran aceptación.

Internet (Internet, La Red). Se denomina así a la red de telecomunicaciones que surgió en los Estados Unidos en 1969 y que en sus orígenes era de caracter meramente militar, para el día de hoy convertirse en uno de los principales medios de comunicación que de manera global afecta la sociedad en diversos aspectos como son el social, cultural,

económico, etc. Se puede clasificar en tres niveles: el primero lo conforman las redes troncales, el segundo las redes de nivel intermedio y el tercero lo constituyen las redes aisladas. El internet es además una red multiprotocolo capaz de soportar cualquier tecnología.

Internet address (dirección internet). Se refiere a la dirección IP que hace referencia de manera inequívoca cierto punto de conexión en una red de Internet.

IP address (dirección IP). Se entiende como una dirección de Internet que tiene 32 bits y definida por el Protocolo Internet en STD 5, RFC 791. Por lo general se representa por medio de una cifra decimal separada por puntos: por ejemplo: 200.36.1.21.

Java (Java) Se trata de una de las principales aportaciones tecnológicas a Internet por parte de Sun, la cual consiste en pequeñas rutinas o programas que pueden ser exportables y ejecutados a Internet, capaces de operar sobre casi cualquier plataforma a través de un navegador. Una de las principales aportaciones de Java es que agrega dinamismo y diseño a las páginas de Internet, en contraparte quizá la desventaja sea de que es muy tardado de bajar (en ocasiones) y alenta los recursos de nuestra máquina.

Java Server Page JSP (Página de Servidor Java). Se refiere a un tipo especial de páginas HTML, en las cuales se insertan pequeños programas que corren sobre Internet (comunmente denominados scripts), se procesan en línea para finalmente desplegar un resultado final al usuario en forma de HTML. Por lo general dichos programas hacen consultas a bases de datos y dependiendo del resultado que se despliegue será la información que se muestre a cada usuario de manera individual. Los archivos de este tipo llevan la extensión ".jsp"

Java Script (JavaScript). Otra importante aplicación desarrollada por Netscape es esta, se trata de programas muy parecidos a los de Java, la diferencia estriba en que los Javascripts se encuentran incorporados dentro del HTML.

Junk mail (correo basura). Se trata del uso indiscriminado del correo electrónico para el envío de propaganda o publicidad no deseada en Internet, lo cual es ampliamente rechazado por los usuarios. (estos pueden ser los famosos "Spam".

Kbps (kilobits por segundo). Es la unidad de medida de la capacidad de transmisión en una línea de telecomunicación. Un kilobit esta formado por 1.024 bits.

Key (clave). Se trata de una serie de signos previamente convenidos que sirven como clave o fórmula para transmitir mensaje secretos o privados.

Keyword (clave de búsqueda, palabra clave). Indispensables cuando se busca una información dentro de algún buscador o cuando queremos registrar una página en uno de ellos.

Mbps (megabits por segundo). Se refiere a una medida en cuanto a la capacidad de transmisión de información por una línea de telecomunicación. Un megabit se forma con 1.048.576 bits.

Modem (módem). Se trata de un aparato que se encarga de convertir las señales digitales en analógicas y viceversa que a su vez permite que dos computadoras se comunique a través de una línea telefónica normal o de cable.

Mouse (mouse, ratón). El multiconocido mouse o ratón es el dispositivo electrónico que nos permite dar instrucciones a nuestra computadora a través de un cursor que aparece en la pantalla y haciendo click para que se lleve a cabo una acción determinada.

MPEG-1 Audio Layer-3 MP3 (Estrato de Audio 3 de MPEG-1). Se trata de un formato de archivo de sonido de amplia compresión, el cual es ampliamente utilizado en Internet y escuchado en nuestra computadora a través de diversos programas como Winamp. A últimas fechas se ha propagado en forma desmesurada su uso, por lo que las compañías disqueras han tomado medidas severas contra quienes promueven su uso, argumentando sobretodo la violación a los derechos de autor.

Napster (Napster). Maravillosa idea de intercambiar archivos MP3 de música a través de Internet por medio de un programa se le ocurrió a Shawn Fanning en Estados Unidos a finales de los 90s. Cuenta con la posibilidad de búsqueda, chats y miles de canciones dentro de su stock lo que hace de Napster sin duda el programa más popular en Internet con millones de usuarios en todo el mundo. Todo no podía ser color de rosa y de inmediato las compañías disqueras se convirtieron en las principales opositoras de Napster, al cual acusan como un facilitador del pirateo de canciones y por consiguiente de la violación de los derechos de autor.

Off line (fuera de línea, desconectado, off line). Se refiere al estado en que nuestra computadora no se encuentra conectada a Internet o a una red en general en ese preciso momento.

Open Systems Interconnection OSI (Interconexión de Sistemas Abiertos). Se trata de un modelo de referencia que fue diseñado por el ISO con la finalidad de que se

conviertan en estándares a nivel mundial con respecto a la arquitectura de redes y ordenadores.

On line (en línea, conectado, on line) Es el estado en que nuestra computadora se encuentra en línea, o sea, conectada a Internet.

Password (contraseña, palabra de paso). Conjunto de números, letras y caracteres especiales que dan acceso a un usuario a un determinado recurso del sistema o de Internet.

Pay-per-view (pago por pase, pago por visión). Esto se refiere a un servicio de televisión en el cual se permite ver al usuario un determinado programa. Por ejemplo una pelea de box, películas, etc., cuya señal es emitida de manera codificada, y liberada por medio del pago de una tarifa.

Peer-to-Peer P2P (entre colegas, entre iguales, entre pares). Se trata de un tipo de comunicación que se da entre dos usuarios de Internet de manera recíproca. El multifamoso Napster es un ejemplo de esta aplicación.

Portal (portal). Se ha dado en últimas fechas la fiebre por los portales de Internet que hasta el momento son la novedad, se autodenominan sitios de internet en donde los usuarios de una manera fácil y rápida tienen acceso a una serie de servicios de manera global como son: noticias, chats, juegos, compras en línea, etc. sin tener que buscar esa información en lugares distintos.

RDSI Ver: **"Integrated Services Digital Network".**

Videoconference (videoconferencia). Se refiere a una plática entre personas que se encuentran en distintas partes del mundo utilizando audio y video a través de Internet conectados en un punto común. Ver: "CU-SeeMe".

Virtual (virtual). Es lo que no existe o no es real aparentemente.

Web, web (malla, telarafia, web). Se emplea este término para definir a un servidor WWW, así como para definir el universo de Internet en su totalidad. Ver: "WWW", "website".[27]

[27] http://www.podernet.com/2000/glosario/indice.html#arpanet, Domingo 26 de octubre de 2003, 15:00 PM.

Capítulo II
Evolución del uso de la Informática, Internet y sus Usuarios.

Capítulo II. Evolución del uso de la Informática, Internet y sus Usuarios.

2.1. Telecomunicaciones en México.

En México, las telecomunicaciones han sido un teman del cual a ido avanzando con gran lentitud, con más de 100 millones de habitantes, hasta nuestros días cuenta con el 11% de la densidad de telefonía, y de toda Latinoamérica, hablar de la telefonía básica en México, es de lo más caro en cuanto a costo para los usuarios, hablar de comunicación en México es hablar de una especie de monopolio.

Teléfonos de México S. A; *"Telmex, con unos 10 millones de líneas, es el gigante en el mercado de las telecomunicaciones mexicano. Cuenta con una cuota de mercado del 95% en telefonía local y un 75% de telefonía de larga distancia. En Internet las cosas no son muy diferentes: alrededor del 70% de los internautas mexicanos navegan con él. También posee el 49% de Cablevisión, la mayor empresa de cable de México. El 51% restante corresponde a Televisa. De hecho los intereses de Telmex no acaban en México; esta compañía con aspiraciones de multinacional participa en la estadounidense Prodigy con un 19%, también posee un 1% de la empresa de EEUU dedicada a la fibra óptica Williams Communications Group y está presente en la telefonía móvil y/o fija de Puerto Rico, Guatemala, Ecuador y Brasil."*[28]

Las Comunicaciones en México fueron mejorando con el tiempo ya que se emplearon sistemas satelitales: *"México cuenta en la actualidad con tres satélites en órbita. Uno doméstico que es el Morelos y dos Regionales Solidaridad I y II. Con la banda Ku abarca E.U. y México y con la banda C, a E. U. y toda Latinoamérica, a la que vende servicios de comunicaciones."*[29]

Los cuales apoyaron el desarrollo de la telefonía, pero no sólo Telmex, se estanca en esto, como se dijo gracias a el uso de los satélites, también se incorporó a los negocios de la telefonía celular o también llamada Móvil en México, de la cual Telmex, a través de Telcel, su división dedicada a la telefonía móvil;

"dispone de 5,3 millones de clientes, un 65% del total. En este punto conviene recordar que a finales de este verano Telmex anunció su escisión del negocio de los móviles para huir de una acusación de monopolio por parte de Cofetel, el organismo

---

[28] http://www.baquia.com/com/20001113/art00014.html, Martes 21 de octubre de 2003. 12:00 PM.

[29] Cobertura regional de los satélites para servicios de televisión y video. Fuente GAO, Telecommuinacatiosn issues in international satellite communications, October, 1996, p. 40 (artículo aparecido en el periódico Reforma en el Suplemento especial de Telecommunicaciones, noviembre de 1996 p. 19.

regulador mexicano. El negocio de telefonía móvil de la operadora, líder con unos 10 millones de usuarios, pasó a llamarse América Móvil y a operar de manera independiente. América Móvil aglutina a Telcel, Telgua y Telgua Wireline (telefonía móvil y fija de Guatemala), la brasileña ATL y Compusa, minorista de artículos de informática estadounidense. Pese a la separación, y a que la nueva empresa tiene un equipo gestor diferente, tiene los mismos amos que su progenitora."[30]

El mercado de las Telecomunicaciones se puede decir que continua siendo aún de Telmex, pues bien tiene un 60% del dominio de las comunicaciones en México, de ahí empezaron a tratar de abarcar una parte del mercado, Unefon a través de Televisión Azteca, y esta a su vez cuenta con uno de los portales de Internet en México como es Todito.com. También otras telefonías entraron a México, a tratar de deshacer el monopolio que existía en México, por lo menos en telefonía de largas distancias como Alestra, Avantel y la compañía mundial AT&T.

Pero no sólo fue en cuestiones de telefonía de larga distancia Telmex ha tenido competencia también en telefonía móvil o llamada telefonía celular, señalando que Telcel, ha sido el monopolio más grande en cuestiones de comunicaciones de telefonía celular en México, y no sólo a sido la más grande, sino que aun lo sigue. Con la apertura comercial a México, entraron nuevas compañías celulares que han hecho la competencia a Telmex teniendo competitividad de estas en telefonía móvil, es así que en la actualidad Telmex tiene que llevar una competencia con otras como; con Usacell, Pegaso, Movi Star y otras más sin mucha relevancia y poca calidad esto se debe a que son equipos de telefonía móvil que funcionan al 100% por ondas de radio, y no por medio de sistema satelital como Telcel e Usacell, por esta razón es que son más baratos en cuestión de tiempo aire, pero son de menor calidad en cuestiones de las comunicaciones.

2.2. Evolución de las Computadoras.

Nuestro mundo esta viviendo cambios muy drásticos en cuanto a la sociedad actual, es decir una gran evolucionando en la tecnología de las comunicaciones, como es el desarrollo de las computadoras que día a día, nos están acercando a los lugares más apartadas del mundo, esta es una situación de la cual hace años atrás, no se pensaba por parte de la gente

[30] http://www.baquia.com/com/20001113/art00014.html, Martes 21 de octubre de 2003. 12:00 PM.

común la cual no se preocupaba por los cambios en la cibernética y la informática. Se podría decir que en muchos grupos sociales, de nuestro mundo actual, es preocupante la marcha directa a un sistema computacional de una manera acelerada, ya que se podría considerar, que nos estamos encarrilando a una sociedad electrónica, controlada por las computadoras.

Las computadoras en nuestra sociedad generan ventajas y desventajas las cuales se pueden ver en la capacidad que estas tiene para ayudar o entorpecer las labores de los usuarios, esto es que las computadoras tienen cualidades esenciales como es la velocidad, precisión en sus funciones, así como la gran capacidad actual para el almacenamiento de datos, de aquí se desprende una gran gama de posibilidades de desahogar en cuestiones de trabajo a los usuarios de estos equipos. El sistema computacional acelerado de la sociedad nos podría llevar a creer que esto nos llevara a una sociedad impersonal en la cual todos podríamos considerarnos como un número, lo podemos ver muy marcado en la forma de comunicación actual vía Internet como el Chat, net meeting, Messenger, en los cuales los usuarios son simples números, o en otro caso un seudo nombre corto.

A las computadoras las podremos considerar como una herramienta que actualmente y en el futuro nos ofrecerá muchas características que nos podrán ahorrar tiempo dinero y esfuerzo, nos ayudarán en nuestras labores académicas, en actividades peligrosas o repetitivas, esto nos llevar a entender que necesitamos actualizarnos en lo personal en el manejo y uso de las computadoras para no quedarnos rezagados ya que en su evolución han superado su capacidad de funcionamiento y desempeño, los primeros equipos de apoyo al hombre para mejora y facilitar sus actividades se pueden describir las siguientes en un proceso de evolución hasta nuestros días, los cuales pasaron desde la cuenta simple hasta lo más sofisticado como lo señala Tellez Valdés, el cual señala una serie de mecanismos usados por el hombre para llegar a la sofisticada computadora como lo veremos a continuación:

Ábaco. Es un objeto que todos tenemos conocimiento, por lo menos lo hemos visto en algún momento, *"Fueron los egipcios quienes 500 años AC inventaron el primer dispositivo para calcular, basado en bolitas atravesadas por alambres. Posteriormente, a principios del segundo siglo DC, los chinos perfeccionaron este dispositivo, al cual le agregaron un soporte tipo bandeja, poniéndole por nombre Saun-pan. El ábaco permite sumar, restar, multiplicar y*

dividir. La palabra ábaco proviene del griego ABAX que significa una tabla o carpeta cubierta de polvo. Este dispositivo en la forma moderna en que la conocemos, realmente apareció en el siglo 13 DC y sufrió varios cambios y evoluciones en su técnica de calcular. Actualmente está compuesto por 10 columnas con 2 bolitas en la parte superior 5 en la parte inferior".[31]

El ábaco fue el primero de los equipos rudimentarios utilizados por el hombre para poder realizar sus cuantas en aquellos numerales que superaban los diez dígitos, y el cual a sobrevivido hasta nuestros días, es un equipo rudimentario para poder realizar sumas, restas, divisiones y multiplicaciones, el ábaco hasta nuestros días lo podemos encontrar, pero como se ha señalado anteriormente aun este a sido desplazado por las calculadoras. Años atrás en la educación primaria, eran requeridos los ábacos para la practica de los estudiantes que empezaban en el proceso de una educación y aprendizaje, pero en el momento que empiezan a conocer los números prefieren usar algo más actual como una calculadora por más sencilla que esta sea.

Tabla de Logaritmos. Esta tabla fue creada en 1614 por John Naiper. Hasta antes de la creación de equipos más sofisticados para mejorar y facilitar el trabajo de la humanidad, ya que la vez que el tiempo seguía transcurriendo se iban complicando más las situaciones de trabajo y haciendo más difícil las sumas, divisiones, restas y multiplicaciones, se creo esta tabla la cual facilitaba un poco estas tareas, solo que tenía grandes problemas en su creación, ya que para la elaboración de esta tabla se tenían que crear sus antilogaritmos e imprimirlos, esto significaba mucho trabajo para poder realizar una tabla, es decir no era tan fácil su elaboración, se tenía que crear la tabla con la participación de matemáticos.

Reglas de cálculo. Poco tiempo después de la Tabla de logaritmos, se creo un nuevo invento que aun más exacto y aun más manejable para las personas, la cual fue la regla de cálculo, la cual tenía un simple funcionamiento de dos reglas paralelas las cuales tenían una relación entre si, esto utilizando la escala logarítmica, estas operaciones eran sumamente exactas, pero como hemos señalado anteriormente estos equipos fueron remplazados por las calculadoras.

Máquina Pascal. *"Esta fue una creación de Blaise Pascal, fue un francés interesado en las matemáticas desde los 12 años, en 1642 construyó una máquina*

[31] http://www-etsi2.ugr.es/alumnos/mlii/abaco.htm. miércoles 02 de octubre del 2003, 19:00 PM.

mecánica para realizar alucines, esta máquina contaba de una serie de engranes en los cuales cada uno contaba con un dígito del cero al nueve llamada Pascalina, su función era que cuando se completaba una vuelta daba un resultado de determinadas cantidades, esta máquina sumadora era destinada a ayudar a su padre, alto funcionario de las finanzas nacionales, esta fue la primera y rudimentaria calculadora."[32]

Tarjeta Perforada. Esta constaba de un telar de tejido, el cual fue inventado por el francés Joseph-Marie Jackard en 1804, el cual es usado aun en la actualidad, era controlado por medio de tarjetas perforadas, su modo de operar consiste en perforar estratégicamente las tarjetas y se acomodaban de tal manera que llevaran una determinada secuencia para indicar un diseño de tejido en particular. Esta idea fue la precursora, para realizar otras ideas y así usar las tarjetas perforadas en otros usos, este diseño convirtió a Joseph Marie Jackard en el padre de las tarjetas perforadas.

Máquina de Babbge. Su nombre se debe a su creador Charles Babbage matemático e inventor. Esta máquina nació en base a el Diseño de las Tarjetas Perforadas, a principio del siglo XIX pensó en varias teorías para las cuales las basaba en aquellos ordenadores, y pensando en los actuales, desgraciadamente vivía en tiempos en los cuales no les importaba la tecnología y mucho menos la materialización de estos. En el año 1822 diseño una máquina diferencial, para el cálculo de polinomios, esta tabla fue utilizada con gran éxito en la navegación y en el la artillería, gracias a esto permitió a Babbage que el gobierno le proporcionara un financiamiento para mejorar esta máquina, pero solo hasta diez años después que la mejoro, pensó en una máquina que pudiera resolver cualquier problema matemático;

"Como los modernos computadores la máquina de Babbage tenía un mecanismo de entrada y salida por tarjetas perforadas una memoria una unidad de control y una unidad aritmético-lógica. Preveía tarjetas separadas para programa y datos. Una de sus características más importantes era que la máquina podía alterar su secuencia de operaciones en base al resultado de cálculos anteriores algo fundamental en los ordenadores modernos. la máquina sin embargo nunca llegó a construirse. Babbage no pudo conseguir un contrato de investigación y pasó el resto de su vida inventando

[32] Idem.

piezas y diseñando esquemas para conseguir los fondos para construir la máquina. Murió sin conseguirlo."[33]

Herman Hollerith. A pesar de que muchos otros inventores trataron de copiar y realizar modelos de calculadoras u otros equipos autónomos siguiendo el modelo del Babbage, estos fueron olvidados por el tiempo no fueron considerados de gran relevancia como para ser considerados en los anales del tiempo. Pero uno de los inventos que sobresalió posteriormente en el año de 1880 fue el de Herman Hollerith, quien a los 19 años fue contratado por el Censo Norteamericano, el cual se comenzó a organizar en 1879, y este censo tardó en realizarse 7 años y medio en poderse realizar ya que este era de manera manual y la información tardaba en poderse recopilar, fue entonces que Herman Hollerith tuvo la idea de desarrollar un sistema de cómputo automático, esto pensando en que en futuras tareas similares pudiera realizarse con mayor velocidad. *"El sistema inventado por Hollerith utilizaba tarjetas perforadas en las que mediante agujeros se representaba el sexo la edad raza etc. En la máquina las tarjetas pasaban por un juego de contactos que cerraban un circuito eléctrico activándose un contador y un mecanismo de selección de tarjetas. Estas se leían a ritmo de 50 a 80 por minuto."*[34] Gracias a este invento se realizo un nuevo censo en 1890 el cual duro dos años, ante el gran éxito que tuvo su máquina, Herman dejó la oficina de censos en 1896 para fundar su propia compañía la cual se llamaba; Tabulating Machina Company. Continuo el desarrollo de sus investigaciones y desarrollo de su invento y en 1900 logro desarrollar una maquina que tenía la capacidad de clasificar 300 tarjetas por minuto, una perforadora de tarjetas y una máquina de cómputo semiautomática. En el año de 1924 Herman Hollerith, fusionó su compañía con otras dos, y esta fusión trajo consigo la creación de Internacional Bussines Machines; esta no era más que la hoy mundialmente conocida compañía de IBM en la actualidad de aquí se desprende una serie de generaciones en computo.

---

[33] http://www.atlas-iap.es/~pepcardo/index.shtml?http://www.atlas-iap.es/~pepcardo/historia.htm, miércoles 02 de octubre de 2003, 13:30 PM.
[34] Idem.

2.2.1. Evolución de las Computadoras Primera Generación.

A partir de la primera aparición de los equipos desarrollados por el hombre se desprende la evolución de la tecnología, la Primera Generación de Computadoras se comienza a desarrollar entre los años 1951 al 1958. Estos equipos se desarrollaron a base de una tecnología de bulbos o tubos al vacío, estos equipos eran exageradamente grandes y generaban demasiado calor obviamente el funcionamiento que tenía era en términos de un nivel bajo en lo que respecta al lenguaje de las computadoras este se conoce como el lenguaje de las máquinas. Los operadores ingresaban los datos y programas en códigos especiales por medio de las tarjetas perforadas, el almacenamiento de los datos se lograba gracias a un tambor interno que giraba sobre un dispositivo de lectura y escritura de tal manera que generaba marcas magnéticas, de igual manera para el manejo de estos equipos se requería tener un amplio conocimiento en el hardware y el software, los cuales no son más que el primero la parte física de la computadora todo lo visible y lo tangible, y lo segundo no la parte que no vemos, ósea el software, es la función o la manera en la que se desarrolla y lleva a cabo los comandos la máquina, o sea es la clasificación del Sistema Operativo y del Lenguaje de Programación en otras palabras es el uso general de su aplicación.

La primera generación se destaca por la creación de una Compañía privada a manos de Eckert y Mauchly quienes construyeron y dieron el desarrollo de las computadoras que formaron el desarrollo de las computadoras de la primera generación las cuales se pueden son;

- **1947 ENIAC.** Primera computadora digital electrónica de la historia. No fue modelo de producción, sino una maquina experimental. Tampoco era programable en el sentido actual. Se trataba de un enorme aparato que ocupa todo un sótano en la universidad. Constaban de 18 000 bulbos, consumía varios KW de potencia eléctrica y pesaba algunas toneladas. Era capaz de efectuar cinco mil sumas por segundo. Fue hecha por un equipo de ingenieros y científicos encabezados por los doctores John W. Mauchly y J. Prester Eckert en la Universidad de Pennsylvania, en Estados Unidos.
- **1949 EDVAC.** Primera computadora programable. También fue un prototipo de laboratorio, pero ya incluía en sí diseño las ideas centrales que conforman a

las computadoras actuales. Incorporaba las ideas del doctor John von Neumann.

- **1951 UNIVAC I.** Primera computadora comercial. Los doctores Mauchly y Eckert fundaron la compañía Universal Computer (Univac), y su primer producto fue esta máquina. El primer cliente fue la oficina del censo de Estados Unidos.
- **1953 IBM 701.** Para introducir los datos, estos equipos empleaban el concepto de tarjetas perforadas, que había, sido inventada en los años de la revolución industrial (finales del siglo XVIII) por el francés Jacquard y perfeccionado por el estadounidense Hermand Hollerith en 1890. La IBM 701 fue la primera de una larga serie de computadoras de esta compañía, que luego se convertiría en el número uno por su volumen de ventas.
- **1954 – IBM.** Continúo con otros modelos, *"que incorporaban un mecanismo de 1960 almacenamiento masivo llamado tambor magnético, que con los años evolucionaría y se convertiría en disco magnético."*[35]

2.2.2. Evolución de las Computadoras Segunda Generación.

Fue durante un período de 5 años en los cuales se realizo la invención del transistor el cual pudo hacer posible la creación de una nueva generación de computadoras, esta generación duro relativamente poco tiempo ya que debido al gran desarrollo que han tenido de aquí y de la primera generación se desprendieron nuevos avances estructurales, gracias a los bulbos y tubos al vació y al desarrollo de los transistores, estos últimos lograron desplazar a los dos primeros, esto logro la revolución de estas máquinas procesadoras las cuales fueron conocidas como las Segunda Generación, estas computadoras a diferencia de las ya antes visto eran más estéticas, esto es que eran computadoras más pequeñas, más rápidas, tenían un consumo menor de energía, por ello también generaban menos calor que sus antecesoras, necesitando así menor ventilación.

Estas computadoras contaban con una nueva forma de comunicación más avanzada que aquel lenguaje de máquina, también utilizaban redes de núcleo magnético, a diferencia que las anteriores que utilizaban tambores giratorios para el almacenamiento de

[35] http://www.pchardware.org/historia/primera.php, Martes 01 de octubre de 2003, 12:30 PM.

información. Los núcleos magnéticos con los que contaban estas computadoras eran anillos de material magnético en lazados entre sí, esto permitía el almacenamiento de datos y lo que hoy conocemos como comandos o lenguaje de la computadora de alto nivel o bien de programación, de la misma forma se desarrollaron los programas, de hecho ya existía en el mercado algunos tipos de computadoras hechas durante la primera generación, pero obviamente eran computadoras con tecnología pasada, esta generación de computadoras ya no requería que el entendimiento pleno del hardware y software de la computadora como en la primera generación, cabe destacar que estas computadoras tenían una sola función para el apoyo del hombre ya sea estaban diseñadas para poder desempeñar aplicaciones matemáticas o de negocios pero no para las dos.

Fue durante el desarrollo de esta generación de computadoras en la cual se empezó a desarrollar el tráfico aéreo, y en otras aplicaciones de uso industrial, esto fue que la industria comenzó a interesarse por el uso de las computadoras en el manejo de las nominas, inventarios, registros y en la contabilidad.

> *"La marina de E.U. utilizó las computadoras de la Segunda Generación para crear el primer simulador de vuelo (Whirlwind I). HoneyWell se colocó como el primer competidor durante la segunda generación de computadoras. Burroughs, Univac, NCR, CDC, HoneyWell, los más grandes competidores de IBM durante los 60s se conocieron como el grupo BUNCH (siglas)."*[36]

2.2.3. Evolución de las Computadoras Tercera Generación.

Esta generación de computadoras se desarrollo durante los años de 1964 y 1971, tuvo un período de evolución de 7 años, en esta generación surgieron los circuitos integrados multifunciónales, la aparición de estos equipos se dio gracias a estos circuitos, que eran unas pastillas de silicio en las cuales se colocaban miles de componentes electrónicos en la formación de una tarjeta en una integración en miniatura. Aquí no esta de más recalcar que las computadoras de esta generación se hicieron a un más pequeñas, se siguió mejorando en cuestiones de generación de calor, así bien el consumo de energía eléctrica era aun un poco menor que las anteriores claro esta eran a un más eficientes.

---

[36] http://www.monografias.com/trabajos/computacion/computacion.shtml, miércoles 24 de septiembre de 2003, 10:30 AM.

Gracias a la creación de los circuitos integrados los cuales desplazaron a los transistores, se desarrollaron a un más los equipos a diferencia de las computadoras de segunda generación, las de la tercera ya eran más flexibles en los programas y estas si podían hacer más estables, así como estabilizar los modelos. Esta generación de computadoras se destaca por la creación de la máquina que marco su inicio la cual fue la IBM de la serie 360, esta fue la primera computadora de uso comercial que utilizo circuitos integrados, a diferencia de las generaciones anteriores esta máquina se podía realizar trabajos tanto de análisis numéricos como administración en el área empresarial como el procesamiento de archivos, esta IBM360 se empezó a utilizar tanto en ingeniería, comercialización y mercadotecnia, ya no era una computadora que solo podía ser adquirida por las grandes empresas millonarias sino podía estar al alcance de las sociedades industriales de la época.

Estas computadoras tenían cualidades que para la época eran extraordinarias, podían correr los programas anteriores a ella y a su vez también corres más de un programa de manera simultanea, es decir la computadora era ya multiprogramada, por ejemplo podía realizar la nómina y a su vez se podía estar realizando pedidos. Las computadoras de la tercera generación tienen ventajas importantes, están hechas a base de silicio en la cual se agrupan determinados transistores miniaturizados conocidos como circuitos integrados; así como también su programación que es lenguajes de alto nivel, en base a un sistema operativo que ya tenía prediseñados los comandos y acciones de la computadora esto es un método de comunicación con el programador que resulta más fácil de emplear que el lenguaje de las dos anteriores generaciones.

2.2.4. Evolución de las Computadoras Cuarta Generación.

La cuarta generación es el nacimiento de la microcomputadora la cual se empezó a desarrollar en los Estados Unidos de América en el comienzo del año de 1970, fue apartar de la creación y comercialización de los microprocesadores Intel 8008.8080.

En esta etapa de de la evolución y desarrollo de las computadoras se puede encontrar 2 mejoras en la tecnología y a partir de estas se marca el inicio de la cuarta generación, estas mejoras son: El reemplazo de las Memorias con Núcleo Magnético, por un Chip de silicio, y también la colocación de muchos más componentes en un Chip; esto

es producto de una miniaturización en todo lo relacionado a los circuitos lo que actualmente podemos encontrar como una microtecnología.

Esta miniaturización y comercialización de todos los componentes en las máquinas de la cuarta generación, provocó que durante el año de 1970 surgiera otra tendencia aparte de la IBM, y esta era la de los Sistemas APPLE, pudo hacer posible la creación de las conocidas como PC en 1981 que no es más que una Computadora Personal, esto provocó una explosión de comercio masivo, en razón a que las máquinas de IBM basadas en microcomponentes Intel 8008.8080, tenían características atractivas para los nuevos usuarios, era más fácil de usar. Podemos señalar que las máquinas de esta generación no tengan un punto de comparación en tamaño y tecnología con las computadoras de la primera generación que ocupaban un cuarto completo, a una PC que sólo ocupa el espacio de unos centímetros cuadrados.

Existe una serie de familias de computadoras personales que fueron evolucionando a partir del año de 1970:

- 1971 Microprocesador Intel 8008. Circuito de alta integración que luego daría inicio a las microcomputadoras.
- 1975 Aparece la microcomputadora Apple. Aparece el microprocesador Zilog Z80. Inicia el auge de la microcomputación.
- 1981 IBM lanza la computadora personal, luego conocida como PC-XT.
- 1984 IBM ofrece la computadora personal PC-AT, basada en el microprocesador Intel 80286.
- 1988 IBM presenta la serie de computadoras personales PS/2, algunas de las cuales emplean el microprocesador 80386. Surge una gran cantidad de computadoras con ese y otros procesadores similares.
- 1991 Microprocesador de muy alto rendimiento: Intel 80486, Motorola 68040, Sparc, tecnología RISC, etc. Microprocesador Power PC (Performace Optimization With Enhanced RISC PC) resultado de alianza de Apple, IBM y Motorola.
- 1993 Intel lanza al mercado el procesador 80586 conocido como Pentium.

"En la actualidad los circuitos integrados son capaces de contener secciones completas de la computadora, o a veces la computadora en su totalidad (excluyendo los medios de almacenamiento y comunicación). En las computadoras actuales el criterio de

las ayudas para la comunicación sigue siendo básicamente el mismo que en la tercera generación. Claro que ha habido mejoras importantes. Pero no podríamos considerar que justifica un cambio de denominación a una nueva generación."[37]

2.2.5. Clasificación de las Computadoras.

Actualmente las computadoras están en un proceso de cambios que toda computadora tiene determinados programas, esto es que en muchas de las ocasiones los usuarios las tienen para usos específicos, ya sea como procesador de texto, para llevar a cabo nóminas, como controladores en los llamados edificios inteligentes, esto nos lleva a que actualmente las computadoras tiene determinadas funciones dependiendo de las necesidades del usuario de esta, cabe destacar que en la actualidad existen varias clasificaciones de estas computarizadas y van desde lo más sofisticado hasta lo personal las cuales se enumeran de la siguiente forma:

- **Supercomputadoras.** Estamos hablando de las máquinas más potentes y más rápidas que pueden existir en un momento determinado, estas maquinas como su nombre lo dice están diseñadas para llevar tareas muy pesadas, como son, un enorme cantidad de información en cuestión de segundos y las cuales por lo importante y delicado de sus funciones de sus funciones están destinadas a llevar a cabo una tarea específica, por estas razones son las más caras del mercado, son utilizadas en la gran mayoría por los gobiernos, ya que las tareas que por lo general realizan las súper computadoras son: Búsqueda y estudio de la energía y armas nucleares. 1. Búsqueda de yacimientos petrolíferos con grandes bases de datos sísmicos. 2. Búsqueda de yacimientos petrolíferos con grandes bases de datos sísmicos. 3. El estudio y predicción de tornados. 4. El estudio y predicción del clima de cualquier parte del mundo. 5. La elaboración de maquetas y proyectos de la creación de aviones, simuladores de vuelo, etc. Por ello sus precios superan los 30 millones de dólares, cuentan con sistemas especiales de control de temperatura ya que pueden tener estar arriba de 100 grados centígrados, debido a este precio son muy pocas Supercomputadoras las que se construyen para los gobiernos.

[37] http://www.pchardware.org/historia/cuarta.php. miércoles 24 de septiembre de 2003, 13:00 PM.

- **Macrocomputadoras.** Son también conocidas como Mainframes. Los son grandes, rápidos y caros sistemas que son capaces de controlar cientos de usuarios simultáneamente, así como cientos de dispositivos de entrada y salida. Las microcomputadoras por estas razones tienen un costo en la actualidad de 350,000 dólares hasta varios millones de dólares. De alguna forma las microcomputadoras son mucho más poderosas que las supercomputadoras ya que estas pueden soportan más programas simultáneamente a diferencia de la supercomputadora. Pero esta ultima pueden ejecutar un sólo programa más rápido que una macrocomputadora, esto que la microcomputadora puede ser de mayor capacidad en programas y uso pero puede llegar a ser lenta por lo mismo. En el pasado, las macrocomputadoras ocupaban cuartos completos o hasta pisos enteros de algún edificio, en la actualidad, las microcomputadoras son una hilera de archiveros en algún cuarto con piso falso, para ocultar los cientos de cables que conforman la su sistema, estas máquinas también tiene el problema de la temperatura ya que tiene que estar controlada.
- **Minicomputadoras.** Surgen en el año de 1960 es una versión de la macrocomputadora, pero a diferencia de esta ya no necesita un sistema tan grande de cableado son orientadas a tareas especificas, esto ayudo a reducir sus costos, y su poder de procesamiento esta a la par de una microcomputadora, soporta de 10 hasta 200 usuarios, en la actualidad se utiliza para el almacenamiento de base de datos y automatizar industrias.
- **Microcomputadoras.** Son las conocidas como PC o computadoras personales, como hemos visto tiene su origen en la creación de los microprocesadores. Estas PC son computadoras para uso personal, son computadoras relativamente baratas, las podemos encontrar en todos los lugares de trabajo, escuelas y en las casa. *"Esta PC es originalmente de la IBM PC pero otras empresas tomaron el modelo con componentes compatibles al grado de solo ser llamadas PC y compatibles en la actualidad existen muchos diseños de esta. Como también aquí se desarrollo la conocida LAPTOP son aquellas*

computadoras diseñadas prta ser trasportadas y no pesan más que de 2 a 5 kilogramos, esto diseñado para facilitar las labores del hombre."[38]

2.3. La Informática.

Toda esta información la podemos traducir en que la informática para poder llevarse a cabo, se requiere de una computadora de la cual, esta complementada por un lenguaje que gradualmente ha ido evolucionando para dar una gran eficacia a la informática misma, la cual también gracias a este lenguaje de programación que día a día es universal, y menos difícil. La informática nos da la posibilidad de almacenar nuestra información en la memoria de la computadora, así también podemos acceder a está y recuperarla en un momento determinado, de la cual podemos ampliar y estudiar posteriormente. Esto es que la informática se compone de lenguajes artificial, es un lenguaje creado por los hombres para las computadoras, las cuales pueden utilizarse para definir una secuencia de instrucciones, y de está manera llevar acabo el procesamiento de datos por estas máquinas, y se dice generalmente, que este es un sistema de código que lee la computadora es sistemático, gracias a este lenguaje la computadora pude facilitarle al hombre el trabajo, dándole a la computadora determinada información o problema, y así esta poder almacenar o bien poder dar un resultado 100% en cuestión de segundos.

En basé a todo lo anterior podemos señalar que la informática tiene especialmente determinadas características esencialmente, las cuales son el estudio de las computadoras y de su principios básicos de la utilización de estas, como son su programación del software en base a un lenguaje de programación avanzado hasta nuestros días, así como de la información que se almacena en ella, también el estudio del hardware, esto es estructura de la computadora, y algo muy importante es que la informática es un instrumento de estudio para llevar a la sociedad moderna a campos más avanzados en cuestiones computacionales en el mundo de la cibernética.

---

[38] http://www.monografias.com/trabajos/computacion/computacion.shtml. miércoles 24 de septiembre de 2003, 10:30 AM.

2.4. Origen del Internet.

El origen del Internet lo vamos a encontrar en los anales de la historia, hace más de veinticinco años, este fue un proyecto militar en el cual se desarrollo durante la guerra fría entre los Estados Unidos de Norteamérica y la Unión Soviética, esto fue a fines de los años sesentas, durante el año de 1969 el Departamento de Defensa de este país, pudo percatarse que durante este período los sistemas de comunicación era muy vulnerable, ya que se detectaba que la Unión Soviética podía realizar interferencias a las comunicaciones del país y realizar espionaje en este, durante este período, los equipos militares se dieron a la tarea de poder desarrollar un sistema, en el cual pudiera costar trabajo y de ser mejor el no poder descifrar las comunicaciones que se tenían internamente entre dirigentes y militares a pesar de el daño del espionaje se encontraba en los sistemas telefónicos el Internet o llamada Red Mundial se baso en el sistema de Red Telefónica también, es decir, que se pensaba en la tecnología de llamar y ser llamado, este sistema inicio con el proyecto de ALPANET, este sistema comenzó de la simple manera, en la cual se conectaban a una red local de comunicación, este sistema al inicio como trataba de algo exclusivo del gobierno, no tenía gran importancia a nivel económico y mucho menos social; ya que solo lo usaban los científicos encargados en análisis computacional y militar, esta tecnología también era denominada Comunicación de Circuito, este era un sistema único y en un número limitado de usuarios, esto es que como se conectaba vía telefónica y funcionaba a base de códigos en el dado caso de un ataque militar podría ser desconectado al derribar las líneas telefónicas y dejando aislada determinada área del país, por esta razón se empezó a realizar determinadas investigaciones;

Para poder solucionar este problema se pensó en:

"Como alternativa, el citado Departamento de Defensa, a través de su Agencia de Proyectos de Investigación Avanzados (Advanced Research Projects Agency, ARPA) decidió estimular las redes de ordenadores mediante becas y ayudas a departamentos de informática de numerosas universidades y algunas empresas privadas. Esta investigación condujo a una red experimental de cuatro nodos, que arrancó en Diciembre de 1969, se denominó ARPAnet. La idea central de esta red era conseguir que la información llegara a su destino aunque parte de la red estuviera destruida. ARPA desarrolló una nueva tecnología denominada conmutación de paquetes, cuya principal característica reside en fragmentar la información, dividirla en porciones de

una determinada longitud a las que se llama paquetes. Cada paquete lleva asociada una cabecera con datos referentes al destino, origen, códigos de comprobación, etc. Así, el paquete contiene información suficiente como para que se le vaya encaminando hacia su destino en los distintos nodos que atraviese. El camino a seguir, sin embargo, no está preestablecido, de forma que si una parte de la red cae o es destruida, el flujo de paquetes será automáticamente encaminado por nodos alternativos. Los códigos de comprobación permiten conocer la pérdida o corrupción de paquetes, estableciéndose un mecanismo que permite la recuperación".[39]

Gracias a esta tecnología se ofrecieron grandes ventajas que han llegado hasta nuestros días, como es la: a) Fiabilidad, esto es que toda la información que se haya recibido independientemente de la calidad de las líneas telefónicas y si en determinado caso se hayan caído las redes la información recibida era exacta. b) Distribución más fácil de los datos, en este caso la información que se repartía, también se distribuía para poder ser recibida de la mima forma en otros equipos que ocupaban el mismo sistema de comunicación. c) Posibilidad de técnicas de comprensión, esto es que la forma que se recibía la información era codificada de tal manera que se asegure la confiabilidad de los datos que se reciben.

En el año de 1972 se pudo crear un sistema de correo electrónico, este sistema fue algo muy importante ya que la mayoría de los usuarios del sistema se esclavizaban a las dependencias, y este sistema de correo electrónico llevó a los usuarios de estas dependencias a liberar a los de horas de trabajo ya que ahora lo podían hacer y recibir información fuera de los horarios o bien podía ser mandada fuera de horarios y poder tenerla a la orden al siguiente día almacenada en su computadora, esto trajo consigo un aumento de tráfico de usuarios.

"Para que los ordenadores puedan comunicarse entre sí es necesario que todos ellos envíen y reciban la información de la misma manera. La descripción de los pasos a seguir se denomina "protocolo". En 1974, se presentó el protocolo "Transmission Control Protocol / Internet Protocol" (TCP/IP). Este protocolo proporcionaba un sistema independiente de intercambio de datos entre ordenadores y redes locales de distinto origen, eso sí, conservando las ventajas relativas a la técnica de conmutación de paquetes. A principios de los ochenta el Departamento de Defensa de Estados Unidos decidió usar el protocolo TCP/IP para la red ARPAnet,

[39] http://www.nodo50.org/manuales/internet/1.htm. Domingo21 de septiembre de2003, 10:30AM.

desdoblándola en Arpanet y Milnet, siendo esta segunda de uso exclusivamente militar, conectada a Arpanet bajo un tráfico extremadamente controlado. Igualmente en Europa se creó la red Minet, como extensión de Milnet. Dado que una gran cantidad de las organismos tenían sus propias redes de área local (RAL) conectadas a los nodos de la red se fue evolucionando hacia una red llamada ARPA Internet formada por miles de equipos. El nombre sufrió algunos cambios más, como: Federal Research Internet, TCP/IP Internet y finalmente, INTERNET."[40]

Gracias a toda esta investigación y trabajo de especialistas informáticos, el uso del Internet creció considerablemente y se desarrollo durante los ochentas, esto es que claro en las Universidades, Centros de Investigación y claro esta en domicilios de altos funcionarios o investigadores. Posteriormente este sistema se fue ampliando e incorporando a empresas privadas, organismos públicos, a partir de los ochentas se dio un fuerte impulso de uso del Internet en todo el mundo, el cual dejo de ser un proyecto a nivel estatal y de uso restringido para los militares y gubernamental, dando un salto para convertirse en el mayor red de ordenador de información de todo el mundo. *"formado por más de cincuenta mil redes, cuatro millones de sistemas y más de setenta millones de usuarios."*[41]

"Teniendo en cuenta que se estima un crecimiento del censo de usuarios de Internet de aproximadamente un diez por ciento mensual, se deduce que para el año dos mil se superarían los trescientos millones de usuarios conectados a la 'Red de redes'. Internet no es simplemente una red de ordenadores, es decir, unos cuantos ordenadores conectados entre sí. Se trata de una asociación de miles de redes conectadas entre sí. Todo ello da lugar a la "RED DE REDES", en la que un ordenador de una red puede intercambiar información con otro situado en una red remota."[42]

Todo este gran crecimiento de la llamada red mundial, se debe a la gran cantidad de información real que se puede encontrar en está, así también como se han mantenido los servicios originales de transferencia de ficheros o llamados archivos, correo electrónico, podemos decir que la llamada red mundial no es más que, una conexión entre los países en donde hay documentos textuales, así como imágenes, que nos pueden ayudar a resolver problemas de información, y no sólo eso sino que a pesar de poder encontrar diferentes autores, en relación a la información que buscamos.

---

[40] Idem.
[41] Idem.
[42] Idem.

2.4.1 Cómo Funciona Internet.

Internet se basa en un concepto de relación comercial de un cliente y un servidor o también lo podemos calificar como un cliente y un servidor. Podríamos describir esta relación como un conjunto de computadoras, una que hace de servidor o proveedor de información, mientras que hay otros que van a actuar como los receptores de esta información del ya mencionado servidor al que es el cliente, por lo regular esta información llega a nuestros quipos como son televisores equipados para recibir esta información, o también a los dispositivos inalámbricos como los teléfonos celulares, computadoras de mano o las conocidas computadoras de escritorio las llamadas conocidas computadoras personales (Personal Computer, PC).

Los que van a ser los equipos receptores van a acceder a Internet por medio de lo que es una línea telefónica y a través de ISP que en ingles significa Internet Service Provider, que no es otra cosa que un Proveedor de Servicio de Internet. Para poder evitar los errores esto funciona a través de lo que es un número único de identificación, el cual va ser proporcionado por el Proveedor de Servicio de Internet, esto es, como un número de registro que tiene el servidor para poder localizarlo como cliente y así dejarlo entrar a la Red de Información o Internet.

> *"Una vez que la computadora cliente se conecta al servidor que contiene la información requerida, éste se la envía en forma de paquetes que se enumeran y marcan con la dirección de la computadora destino. Luego se distribuyen por la Red para su entrega. Del otro lado, la computadora destino recolecta los paquetes y los reensambla, dejando los datos como estaban originalmente para ser vistos por un programa especial llamado navegador."*[43]

Internet se basa en lo que es un conjunto de protocolos que son denominados Protocolos de Control de Transmisión, esto provoca que el flujo de los paquetes ya mencionados lleguen con seguridad e intactos y sin errores, también el número de identificación que proporciona el servidor sirve para que el usuario o receptor pueda conectarse en una zona distinta y poder mover datos de un lugar a otro, esto es que todo el proceso de conexión, recepción y manejo de información lo hacen los equipos de computo en conjunto con las líneas de comunicación de manera automática, sin que los usuarios

[43] http://websperu.wperu.com/internet.html, Domingo 12 de octubre de 2003. 12:14 PM.

puedan darse cuenta de ello, aquí podemos señalar que por esta razón, es lo mismo que el servidor que esta mandando la información a los equipos se encuentre al otro lado del mundo o bien en la misma casa, no importa la distancia ya que la información de Internet es una sola red, única e intacta.

2.4.2. Tipos de Conexión.

Para que un equipo de cómputo se conecte a la Red de la Informaciones necesario que se tengan determinados elementos, en principio en nuestro equipo debemos tener instalado un módem o una tarjeta de comunicación interna así como una tarjeta de Red para una conexión a Internet. Cuando se realiza la conexión normalmente se requiere introducir en primer lugar la contraseña y nombre de usuario que nos otorga el servidor, estos datos al entrar a la red los envía al servidor para que este compruebe que son correctos y nos permita navegar en la Red, esto es con motivo de control a la conexión de la Red de Información por medio de el sistema de telefonía.

El acceso a la Internet recae en dos categorías:

- **Acceso Dedicado.** En este medio computadora está directamente conectada Internet, es el caso de algunos servidores de Internet como son Cablevisión en México que proporciona un sistema de conexión directa a el servidor de manera permanente por medio de un cable módem sin la necesidad de estar conectado a una línea de comunicaciones como telefónica, así como también puede ser de manera satelital.
- **Acceso por Marcador Telefónico.** En este medio la computadora se conecta a Internet de manera temporal, generalmente por medio de una línea telefónica y un módem de la computadora.

Las compañías que ofrecen el servicio de acceso a Internet por cualquiera de estas modalidades son conocidas como Proveedores de Servicios de Internet o Internet Service Providers (ISP).

2.4.3. Alternativas de Conexión por medio de un MODEM.

Las líneas telefónicas fueron diseñadas para trasportar la voz humana en forma de señal analógica, no así datos electrónicos enviados por computadora.

> *"Los Módems fueron inventados para convertir la señal digital generada por computadora a señales analógicas. Otro módem, al externo de la línea, realiza la función inversa, es decir convierte la señal analógica en señal digital. Es así que la palabra MODEM proviene del acrónimo MOdulación/DEModulación. Actualmente la velocidad máxima a la que se puede transmitir a través de un módem analógico es de 56 Kbps, esto es, 56 mil bits por segundo."*[44]

2.4.4. Alternativas de Conexión por medio de un RDSI o ISDN.

En lugar de lidiar con conversaciones de digital a analógico y viceversa, la Red Digital de Servicios Integrados (RDSI, por su siglas en inglés), maneja señales digitales a través del proceso de transmisión.

> *"Las líneas de transmisión RDSI son ordinariamente líneas telefónicas de dos hilos que llevan señales digitales en tres canales separados. La compañía de teléfonos utiliza un canal para propósitos de control; los canales remanentes pueden ser utilizados por el usuario para transmitir voz, datos o ambos. RDSI tiene un máximo de velocidad de 128 Kbps."*[45]

2.4.5. Alternativas de Conexión por medio de un ADSL.

Al igual que RDSI, Asymmetrical Digital Subscriber Line (ADSL) permite la transmisión de datos digitales sobre líneas telefónicas ordinarias. *"Es llamada Asimétrica porque realiza la transmisión en una dirección (desde la red) más rápido que a la inversa (a la red). ADSL lleva señales a la red a velocidades tope de 640 Kbps, y puede recibir datos desde ella a velocidades de hasta dos millones de bits por segundo (Mbps)."*[46]

---

[44] http://websperu.wperu.com/internet/2.html, Domingo 12 de octubre de 2003. 12:14 PM.
[45] Idem.
[46] Idem.

2.4.6. Alternativas de Conexión por medio de un CABLE MODEM.

El cable módem permite la transmisión de datos sobre redes de antena de televisión de la comunidad (CATV), esto es, la red de cables utilizada para la distribución de televisión por cable. Al igual que un módem análogo estándar, cable módem convierte señales digitales a análogas y viceversa. "*Pero el cable módem es mucho más complicado que un módem análogo estándar. Incorpora un sintonizador que separa los datos digitales del resto de información que viaja a través de la señal de televisión por cable. Cable módem transmite datos desde la red (downstream) a una a una velocidad de 3 Mbps y a la red (upsstream) a 500Kbps a 2.5 Mbps. Los cables módems son dispositivos externos que se instalan al lado de la computadora.*"[47]

2.5. Nacimiento de la Cibersociedad.

Como podemos observar Cibersociedad es un concepto que en nuestro mundo moderno se esta empezando a utilizar para referirse a los que otros llaman Internet, a lo que nos lleva a las nuevas tecnologías de la informática y la evolución de la comunicación, podremos navegar en Internet buscar significados de lo que es esto pero, por el significado correcto lo vamos a encontrar en la sociedad contemporánea, que es quien lo usa y esta aprendiendo a vivir con ello. Esto es que para poder hablar de la Cibersociedad hay que observar a las sociedades humanas, ya que como la palabra lo dice hablar de la Cibersociedad es hablar de de la gente interconectada, en hablar de la sociedad de la información en una conexión de tecnología comunicativa, lo cual contiene información sobre la misma tecnología, comunicaciones, cuestiones laborales, económicos, etc.

Todos estos conceptos de la civilización actual también han ido evolucionando en la aparición y la popularización del uso de los diversos instrumentos y hábitos a los que llamamos Internet. Día a día escuchamos y vemos por el radio por la televisión o bien en los periódicos, de algo nuevo de un avancé a nivel medico o bien tecnológico, nadie puede negar que vivimos tiempos de grandes cambios de una nueva revolución tecnológica, por esta revolución, a muchos de nosotros no nos causa impresión por la misma aclimatación que tenemos a ello. Donde podamos voltear la mirada podremos muchos artículos que

[47] Idem.

siguen sin un cambio pero también junto a ellos una infinidad de nuevos artículos que han mutado vigorosamente para mejorar la calidad de vida de la humanidad, y esto es una dinámica de fuerza en los cambios y de continuidad la cual describe nuestra actualidad. Todos estos cambios de la tecnología, en la información y la regulación que esto implica podemos desprender que todos estos cambios afectan nuestra vida cotidiana, de nuestra forma de relación y socialización, aun más de nuestra identificación ante una colectividad e incluso de una agrupación específica. Es aquí en estos puntos en concreto donde señalamos la intención de poner en relación nuestras formas contemporáneas de agrupación con los nuevos modos de comunicación y relación que han popularizado las Nuevas Tecnologías de la Información en el Internet con la Cibersociedad o Sociedad de la Información.

Una visión más crítica y ácida sobre la sociedad de la información es aportada por Schiller, quien nos dice que para el todo lo anterior consiste en:

> *"La producción, proceso y transmisión de una cantidad muy elevada de datos relativos a todo tipo de cuestiones individuales y nacionales, sociales y comerciales, económicas y militares, en la que la mayor parte de los datos se elaboran con el fin de satisfacer las necesidades específicas de las grandes empresas, las burocracias oficiales nacionales y los estamentos militares del estado industrial avanzado".*[48]

El gran cambio en la tecnología y en la sociedad se han visto más marcadas y sobre todo su producción en las Sociedades Modernas, las cuales se están organizando en torno a la tecnología, a la información, al conocimiento lo cual le va a garantizar en esta el control social y de la dirección de las innovaciones y más a un garantiza los cambios en nuestro mundo. El socialista Daniel Bell señala que es para el paso de la humanidad a la Cibersociedad o a la Sociedad del Conocimiento.

> *"tiene un sustrato intelectual de software: la información es el recurso o materia prima; el conocimiento es el recurso estratégico; la abstracción es el método superando la simple inducción del método científico; la codificación del conocimiento es el gran valor; la formación científica es la mejor base de capacitación profesional; la tecnología intelectual es la que hace posible la actividad "quinaria" de servicios de software (salud, investigación, ocio, educación, política, etc.)".*[49]

Todo este impacto social lo podemos entender gracias a la gran aceptación que hay del hombre hacia la tecnología y a su desarrollo, de no ser por este, no habría alcanzado el

---

[48] H. SCHILLER, El poder informático, Madrid, Gustavo Gili, 1983, Pág. 46.

[49] BELL, Daniel, El advenimiento de la sociedad post-industrial, Madrid, Alianza, 1976, Pág. 146.

crecimiento que tiene en la actualidad, Todas estas son tecnologías de la información que han ido añadiéndose unas a otras y que tienen en común, entre otras características, que se desarrollan en una dimensión no física de la realidad, es decir algo virtual, algo que se puede ver percibir por alguno de los sentidos no todos ya que no podemos tocarlo No debemos confundir, como se ha advertido en muchísimas ocasiones, el lugar donde están las máquinas (el telégrafo, el teléfono, la emisora de televisión o los ordenadores) con el lugar donde tiene se encuentra la interacción comunicativa, que es la que da el golpe a un nivel social y de creación de significados colectivos. En relación a este punto podemos citar dos cuadros a los que se hace referencia que hace Joan Mayans I Planells en cual hace un estudio de los grados de aceptación de los medios de comunicación.

Uno es por su grado de popularidad y la cantidad de personas que pueden hacer uno de ellos:

	Popular	**Uno a uno**	**Uno a muchos**	**Muchos a Muchos**
Telégrafos	Poco	Sí	No	No
Radio	Si	No	Sí	No
Teléfono	Sí	Sí	No	No
Televisión	Sí	No	Sí	No
Internet	Sí	Sí	Sí	Sí

Resulta útil, además, combinar la progresiva evolución que nos muestra gráficamente la tabla anterior, con esta otra que se presenta a continuación, donde se quiere reflejar el tipo de contenido o función que caracteriza a cada una de las mencionadas tecnologías de la información:

	Interactivo	**Información Personal**	**Información General**	**Entretenimiento**
Telégrafo	Poco	Sí	No	No
Radio	No	No	Sí	Sí
Teléfono	Sí	Sí	No	No
Televisión	No	No	Sí	Sí
Internet	Sí	Sí	Sí	Sí

"Sería muy difícil medir el impacto cotidiano, social y cultural, de estas tecnologías. Sin embargo, resulta muy fácil e ilustrativo tomar los datos de estas dos tablas, sumarlos y compararlos. Si a cada "sí" le damos el mismo valor, generaríamos un gráfico absolutamente inútil a nivel analítico o descriptivo, pero quizá ilustrativo de la aceleración que suponen las nuevas con respecto a las no-tan-nuevas tecnologías de la información que estamos comparando aquí."[50]

Las tablas anteriores hacen una comparación en la sociedad de los impactos que tienen determinados medios de comunicación, esto es que el Internet tiene una línea ascendente y a media que avancen los días y años será a un más marcado, por ejemplo, cabe señalar que actualmente las oficinas de Correos están teniendo menos problemas de trabajo a disminuido en estos aspectos y esto se debe a que en estos días, se esta empleando más el sistema de Correo Electrónico el cual puede mandar casi todo lo que se requiera en cuestiones de archivos e información personal. Es decir puede tener generalidades, es altamente interactivo y con una pluralidad de difusión muy grande en la sociedad, hay que tratar de conocer y sobre todo entender el impacto en nuestra sociedad del la Cibersociedad, ya que estos son los que hacen y coordinan lo que existe en el Ciberespacio.

La creación de una Cibersociedad es algo inevitable, algo que va evolucionar día a día y requiere que todos podamos entenderla y conocerla no rezagarnos en su conocimiento y desarrollo, es más que un conjunto de máquinas y cables, también tiene relacionados como hemos mencionado cuestiones de carácter económicos, políticos, jurídicos, históricos y socioculturales, en conclusión es de carácter social.

2.5.1. Característica y Naturaleza de la Cibersociedad.

La naturaleza de la Cibersociedad, la vamos a encontrar esencialmente en las características de cada uno de nosotros como usuarios, esto es que la Cibersociedad esta creada con las características de cada persona, es como la creación de una ciudad en la cual esta hecha dependiendo de las necesidades y deseos de quienes la construyen. Como ya vimos en los setentas nació el concepto de la Cibersociedad, obviamente la mezcla entre tecnología e información se creía que iban a causar problemas de inadaptabilidad, y no estamos hablando solo de orden tecnológico, ni en carácter de información sino también en el orden

[50] MAYA I PLANELLS, Joan. Comunicaciones Electivas, Nota sobre la virtualización de lo comunitario en el tiempo de desterritorialización, http://cibersociedad.rediris.es/mayans/mayans_12.php, Lunes 13 de octubre de 2003. 12:30 PM.

social y psicológico. Como características podemos encontrar lo similar a una Sociedad Real, la que todos vivimos esto es que también en la Civilización Virtual o Cibersociedad, vamos a encontrar estructuras institucionales, legislaciones, ofertas y demanda, demandas de trabajo, solicitud de trabajo, así también como una sociedad contemporánea vamos a encontrar emergencias de nuevos conflictos como también algo que no se puede escapar de toda civilización que es desigualdades sociales, marginación y mucho más.

Con el transcurso del tiempo el progreso de la tecnología y con todo lo anterior aumento y junto con esto la introducción masiva de la información en las empresas, en la administración pública , hospitales, fábricas, y junto a estos el desarrollo de los edificios llamados inteligentes, todo esto se debe a que gracias al desarrollo de la tecnología y la demanda de participar en la Red de la Información se a creado esta Cibersociedad que se a convertido en un fenómeno en masa, y como una sociedad se crea en base al respeto y libertad de los demás este servicio de Internet tiene como objetivo el ponerse al servicio de la comunidad.

No solo podemos hablar de lo interno de una sociedad sino que también la tecnología han conseguido introducirse en el comercio y así también en el comercio exterior, no podemos decir que la Cibersociedad es para bien o para mal, tal vez eso lo veremos en muchos años más ya que podemos imaginar una civilización controlada por algo virtual, que se interconecta en todo el mundo, podrá servir como un ingrediente fundamental del equilibrio entre la autoridad y los ciudadanos, entre los representantes de Estado y la libertad de la Sociedad esto es que la informática nos ayudará a obtener la democracia gracias a su gran base de datos que en ella se puede alojar.

Como se ha comentado con anterioridad, la sociedad de la información ha producido una auténtica revolución que va a transformar radicalmente la sociedad. La causa fundamental es una herramienta inventada apenas hace cincuenta años:

> *"el ordenador". "La revolución acaba de comenzar, pero ya se puede decir que está empezando a rebasar nuestras fronteras ordinarias. Por esta causa es preciso examinar cómo podemos enfrentarnos a esta revolución con garantía de éxito, y asegurarnos que sus beneficios serán amplios, benignos y superarán a los inconvenientes. Este trabajo de investigación ha considerado la situación actual y ha tratado de encontrar la forma de sacar beneficios de esta nueva revolución y el modo*

de aminorar sus riesgos y vulnerabilidad, así como reducir sus impactos y efectos negativos."[51]

La Cibersociedad es un tema relacionado con la tecnología actual pero también algo muy importante del cual nunca lo vamos a poder desprender, ya que pertenece a la cultura y a la sociedad de la cual será un punto que tendremos que superar y a controlar, podemos referirnos a la Red de la Información como un terreno nuevo en donde la humanidad esta empezando a conocer sus terrenos, a conocer el papel que va a desempeñar en la información y el conocimiento, en el comportamiento humano y el impacto en una sociedad. Es una Revolución de Información, la cual esta empezando, además se esta incrementando a todas partes del mundo favoreciendo a este y alimentando la Red de la Información, social, comunicación, favorece a consultas de conocimiento en general, coordinar y operar en conjunto con otros algún equipo a grandes distancia, poder estar conectado durante un largo período de tiempo, poder llevar relaciones de personas a distancia, obtener la información de cosas, manuales, artículos, actividades personales no podrían imaginar y cada día toda esta información se actualiza y se alimenta

2.5.2. La Cibersociedad y sus Ciudadanos.

La humanidad esta entrando en un momento en el cual se está desenvolviendo en la sociedad de la información, más bien conocida como la Cibersociedad. Los interrogantes que plantea esta Cibersociedad son consecuencia inmediata de la revolución de la información y eso nos lleva a tratar de entender a futuro numerosas preguntas que la humanidad se hará con forme avance la tecnología y cada vez más personas se unan a este territorio virtual. Las cuestiones que expertos se harán con el tiempo serán entre otras, ¿Cómo va a ser la nueva sociedad de la información o Cibersociedad?, ¿Cómo vivirán y cómo trabajarán los individuos en una Cibersociedad?, estas preguntas se harán por los avances de esta materia y por el tratar de llevar el control de estos nuevos terrenos a los cuales la humanidad esta conociendo y alimentar de información, en la cual tiene sus propias reglas y estructura. La Cibersociedad se caracterizará por la infinidad de

[51] JOYANES AGUILAR, Luis. Cibermaneras. Revista Vivat Académica, Abril 2000.
http://www2.uah.es/vivatacademia/anteriores/catorce/cibermaneras.htm#NOTA%2059, Lunes 13 de octubre de 2003. 13:00 PM.

posibilidades que la informática y las autopistas de información aportarán a la vida de los ciudadanos. Algunos aspectos que ofrecerá la nueva socialización serán:

- **El hogar electrónico.** La casa inteligente a la que tanto han recurrido la literatura y el cine de ciencia ficción será una realidad a principios del siglo XXI.
- **La Telecompra.** Cada día es mayor la invasión de las empresas de ventas de productos a través de la televisión. En el futuro, se podrá elegir y seleccionar a voluntad muchos de los productos que deseemos, entre ellos ropa, electrodomésticos, etc.
- **El comercio electrónico.** En el tercer milenio la mayoría de las operaciones comerciales se realizarán a través de redes de ordenadores mediante el intercambio electrónico de datos, a través de la Red Internet y de las redes corporativas Intranet.
- **Telebanco.** Ya es una realidad en España. El Banco directo de Argentaria y el Open Bank del Banco de Santander, son los primeros modelos de lo que se anuncia será la nueva banca del futuro.
- **El ciberdinero o dinero virtual.** Los telebancos se convertirán en bancos virtuales, y el dinero virtual será una de las formas de pago que en breve plazo, junto con el monedero electrónico constituirán el eje central de las operaciones comerciales del 2000.
- **La enseñanza multimedia y la teleenseñanza.** La enseñanza tradicional se apoyará en los sistemas multimedia para incrementar su eficacia. La enseñanza a distancia se convertirá en uno de los pilares de la nueva cultura, ya que los últimos avances podrán llegar hasta las aldeas y pueblos más pequeños y lejanos.
- **El ocio y el turismo.** Estas facetas de la vida ordinaria serán seguramente las que sufran más impacto, y ayudarán al bienestar social.

El impacto que tendrá en la humanidad será en la vida laboral, las empresas, los trabajadores y las relaciones entre ellos cambiarán radicalmente. Las estructuras laborales adoptarán cada vez más, una forma esencialmente de cuatro partes muy importantes ya que cada parte tendrá una función en esto, en el cual todos estarán interrelacionados, esto es, que;

"una de las partes se dirigirá de manera directa a la producción se hará con personal propio, escaso, el mínimo de personal o hecho por uno mismo, otra parte con empresas subcontratadas; la tercera con personal independiente conocidos como freelances, que son personas que trabajan por su cuenta realizando trabajos por tanto. Y final mente el ocio será una de las facetas de la vida que más sufrirá. Existirán dos tipos de personas: unas con exceso de trabajo y otras con exceso de ocio; esto implicará que la futura sociedad del ocio sólo llegará a media sociedad y eso planteará una serie de connotaciones políticas, laborales y sociales que será preciso acotar para que los riesgos sean los meno posibles y que causen el menor impacto negativo en la sociedad."[52]

2.6. Los Perfiles de los Usuarios de la Cibersociedad.

Como sucede en todas las comunidades del mundo vamos a encontrar gente que se encarga de dañar la estabilidad de esta, gente que se encarga de cometer los delitos los cuales son sancionados por la sociedad la cual crea reglas de buenas costumbres para así poder llevar acabo una convivencia social entre los habitantes, vamos a poner un claro ejemplo de ello es la colonización un territorio nuevo, ahí se trasladaron personas con buenas costumbres, con ánimo de de progresar y sacar adelante esa colonia.

Como en todas las colonizaciones existe un pero: junto a estos colonos de buenas costumbres y ánimo de progresar se trasladan también personas con el ánimo de causar daño y poder sacar provecho de otros, sin remunerarle o vivir de ellos por medio del delito, es decir a raíz de la introducción de la informática en los hogares y los avances tecnológicos que esto aporta ha surgido una generación de nuevos personajes que podríamos decir más o menos peligrosos que difunden el miedo en la Red de la Información.

Podemos adentrarnos ahora en lo que es la colonización de nuestra Cibersociedad la cual trae consigo a usuarios que como ya hemos denominados son los Cibercuidadanos, los cuales realizan es esta diversas actividades, económicas, culturales, laborales y sociales entre otras, pero así como la tecnología de una Cibersociedad, también en esta hay por desgracia gente o Ciberciudadanos que están poblando esta nueva colonia de tecnología e información con el ánimo de obtener beneficios por medio de una actividad ilícita.

[52] Idem.

Desde el inicio del Internet hay personas que han estado en ella, la han regulado, controlado y dado empuje para su actual crecimiento, pero también con este impulso se desarrollaron, personas que descubrieron como poder indagar en el sistema de información, pudieron desarrollar medios ya sea físicos o no para poder introducirse en los equipos de usuarios que solo buscan, trabajar a través de la Red de Información, obtener información de esta o simplemente ocio.

A esta actividad en la actualidad la podemos denominar Espionaje el cual vamos a trasladarlo a nuestra Cibersociedad en el cual se ha denominado por los usuarios de esta como los tradicionales Hackers, es aquí en donde entramos en lo importante de la materia, es decir es en donde vamos a poder ver que los usuarios de el Internet no tienen una privacidad absoluta, están a la merced de de otros usuarios los cuales violentan esta privacidad, estos personajes no causan un daño material a nuestros equipos sino que simplemente como o hemos visto son los espías de la Cibersociedad.

Los Hackers son personajes cuentan con el conocimiento necesario así como también para poder realizar su espionaje en sistemas ajenos se rodean de tecnología por medio de la cual pueden lograr y obtener lo así desean. Podemos hacer una valoración entre lo que hace un espía en la sociedad, el cual se acercara a sus víctimas u objetivos de espionaje y hará que esta persona confíe en el para poder obtener la información que se busca. Y los Hackers tiene varios medios para poder obtener la información que necesitan, uno de estos métodos era al principio de el nacimiento del Internet en el cual el Hacker contactaba a un usuario al asar y lo convencen para que le de el numero de su módem, sabe arreglárselas para que los usuarios confíen y crean en el, pero en nuestros días la tecnología a ayudado a estos personajes a poder obtener lo que desean sin contactar directamente a el usuario, gracias a esta tecnología los Hackers emplean equipos con determinadas funciones, por medio de los cuales este busca los equipos y entra al sistema de computo del usuario, así puede ver lo que tenemos almacenado en nuestros equipos de computo, aun más puede ver lo que hacemos, revisar nuestros archivos confidenciales, extraer esta información y después puede venderla o bien simplemente para uso personal, en la actualidad existen de estos pocos, son personas que tratan de obtener un beneficio de la información que pueden robar de un usuario.

El la Cibersociedad actual también vamos a encontrar Hacker que no les interesa lo anterior, la mayoría de los actuales Hacker son gente joven con ganas de divertirse y

molestar a los demás, los cuales simplemente al estar navegando por Internet, entran a los sistemas informáticos y lo hurgan, pueden robar de él lo que les interese, información, fotos, por simple curiosidad o por molestar, mueven los archivos o bien pueden llegar a destruir un trabajo de varios días o manipulan el equipo de computo para que se apagué sin más ni más interrumpiendo las labores de los usuarios, después de realizar su actividad los usuarios nunca se percataron o lo hicieron al ver que sus archivos están en desorden o bien alterados, o simplemente le llega un correo electrónico, un mensaje por algún tipo de mensajero instantáneo algún mensaje ofensivo o de burla haciendo alusión a los archivos hurgados, y es aquí en donde nos percatamos de que nos están espiando.

Dentro de nuestro tema principal de la privacidad de los navegantes podemos decir que los Hackers son aquellos individuos los cuales tienen el conocimiento y los medios para poder violentar nuestra privacidad de información o documentos personales, exclusivos de los usuarios, lo único bueno que podemos decir de este individuo es que junto con ellos hay Hackers que aparte de revisar la información de los equipos de computo pueden en ocasiones ser los quienes señalan a los usuarios que tienen determinado problema en sus equipos esto es que no solo hay Hackers que roban la información, sino que también hay quien señala los daños de la computadora, no todos son espías, pero aun así al hacer una revisión no autorizada por los usuarios esta violentando la privacidad de este.

2.6.1. Sujetos Activos y Sujetos Pasivos en una Agresión vía Internet.

Sujeto Activo. Vamos a señalar que las personas encargadas de cometer los Daños y Delitos Informáticos, no son delincuentes común y corrientes o dicho de otra manera, los Sujetos Activos son los Delincuentes Informáticos, estas personas poseen características que no presenta la mayoría de los delincuentes, esto se debe a que los Sujetos Activos son aquellos que cuentan con excelentes habilidades para el manejo de los sistemas Informáticos, y a consecuencia de esto y por su posible situación laboral se encuentra en lugares estratégicos donde tiene a su alcance el manejo de información a través de la Red de Comunicación de Internet, o bien son jóvenes que por simple ocio y su habilidad en el uso de los medios de Información sin que tengan la necesidad de encontrarse en un trabajo,

se encuentran todo el día conectados a esta Red y cuentan con los medios económicos para poder adquirir medios tecnológicos para facilitarle esta labor de daño o comisión del delito.

Podemos señalar que hablar de los Delitos Informáticos es hablar de personas o delincuentes no comunes, ya que como hemos dicho los Sujetos Activos cuentan con Características Especiales como son:

a) Cuentan con importantes conocimientos en los Sistemas de Información y en cuanto al conocimiento de navegación de Internet.

b) Para poder cometer el daño o el delito estas personas se encuentran situadas en lugares estratégicos en su trabajo cuentan con una conexión de manera interrumpida a la Red de la Información. Devenido a esta ubicación pueden manejar información de carácter sensible. Y a esto se le denomina "Delitos Ocupacionales" ya que son cometidos por la ocupación que se tiene en el acceso al sistema que puede ser financiero.

c) Otro puede ser aquel joven que cuenta con las mismas características especiales de conocimientos en equipo Informático, el cual entra por curiosidad a la Red de la Información con el motivo de violar el sistema de seguridad como un desafío personal, este joven puede contra con recursos necesarios para adquirir tecnología o bien simplemente adquiere programas para poder realizar este daño.

d) *"Estos delitos se han calificado "Delitos de Cuello Blanco", por que la persona que comete el delito es de cierto status socioeconómico."*[53]

Lo anterior nos puede señalar que los que cometen los Delitos Informáticos son personas muy diversas, no solo se pueden centrar a las personas que entra a la Red de Información, como son personas que trabajan en instituciones financieras y desvían fondos para si, también personas que entran para realizar un simple daño por ocio, o bien para realizar copias no autorizadas de determinados programas.

En toda la información relacionada con esto hay controversia en cuestión alas personas que cometen este tipo de delitos, señalan diferencias marcadas entre estos, muchos dicen que son personas con grandes actitudes intelectuales, en cuestiones de informática, son personas listas, dedicadas, motivadas y con la disposición de aceptar un reto de carácter

[53] VIEGA RODRÍGUEZ, María José. Delitos Informáticos, http://derecho.org/comunidad/mjviega/deli_inf.htm. miércoles 01 de octubre de 2003, 14:00PM.

tecnológico, estas características, podemos encontrarlas en personas dedicadas al sistema informático pero no es tanto así, esta es una diferencia que vamos a señalar más adelante en cuento veamos a los diferentes perfiles de estas personas y veremos que para ser un Sujeto Activo de los Delitos Informáticos no es necesario tener estas características sino simplemente es el tener el conocimiento necesario en cuestión de informática y manejo de la Red.

Sujeto Pasivo. En primer término podemos decir que el Sujeto Pasivo es la víctima o la persona en la que recae la conducta que realiza el Sujeto Activo. Y poniendo más claro en el caso del Sujeto Pasivo de los Delitos Informáticos la víctima puede ser ya sea un individuo común que navega en la Red de la Información, una Institución de cualquier tipo, financiera, crediticia, gobierno u otras, pero obviamente para que puedan ser Sujetos Pasivos deben de ser usuarios de sistemas de información y contar con una conexión y trabajar en ella como actual mente la mayoría lo hace.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los "delitos informáticos", ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos. Dado lo anterior;

> *"ha sido imposible conocer la verdadera magnitud de los "delitos informáticos", ya que la mayor parte de los delitos no son descubierto o no son denunciados a las autoridades responsables" y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y dar tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra"*[54]

La "cifra negra" es muy alta. No es fácil descubrirlo ni sancionarlo, en razón del poder económico de quienes lo cometen y también es importante destacar que los daños económicos son altísimos. "*Se habla de pérdidas anuales por delitos informáticos y otros tecno-crímenes, que van desde los U$S 100 millones (Cámara de Comercio de los Estados*

---

[54] Supremo Tribunal de Justicia del Estado de Sinaloa, Derechos Reservados 1998. http://www.stj-sin.gob.mx/Delitos_Informaticos2.htm#CAPÍTULO%20I, miércoles 01 de octubre de 2003, 12:00PM.

Unidos) hasta la suma de U$S 5.000 millones, de acuerdo a un estudio de 1990 hecho por una firma auditora."[55]

2.6.2. Perfil de los Sujetos Deseosos de Conocimiento los Hacker.

Un perfil exacto de lo que podemos llamar Hacker no existe en si, pero gracias a la basta información que hay en relación a ellos podemos acercarnos aun análisis, y hacer un acercamiento al perfil de este. Un Hacker es una persona compulsiva y con una gran obsesión por acumular u obtener información, pueden ser las personas que suelen abrir todos los aparatos eléctricos que hay en sus casas, también en cuestiones de informática, son aquellos que suelen revisar su computadora en cuestiones de ordenador y modificarla a ver que es lo que pasa.

Una Persona con tendencia a ser un excelente Hacker prueba y modifica las cosas que pudieran llegara sus manos y se pasa largas horas pensando en ello analizándolo, tratando de sacar un por que, que pasaría si le faltara algún componente.

Existen dos tipos de Hacker los Hackers en sí y los Hardware Hakers. En primero de ellos es aquel que solo obtiene el conocimiento para practicar con los ordenadores, para introducirse en los sistemas de otros usuarios, y el segundo van a tener más interés por el sistema electrónico, pero por lo regular la mayoría de los Hacker tiene ambos conocimientos ya que son muy útiles tener ambos conocimientos.

Físicamente un Hacker no es el típico personaje de lentes, pelo engomado y graso, o bien el típico chico tímido cubierto de granitos en la cara, son personajes que no van a ser los tópicos que tiene cara de delincuentes, pocos amigos y que portan camisas negras o chamarras del mismo color adornadas con dibujos alusivos a la calavera o a cosas delictivas, en relación a esto los Hackers son aquellos personajes comunes y corrientes que vas a ver en cualquier tienda de auto servicio, que gusta de consumir productos como pizza, coca cola, son personas que nunca delataran que son Hackers, podemos tener a nuestro mejor amigo y sin que el nos diga es un Hacker.

El Hacker es aquel quien se interesa por la tecnología, sin importar si complexión, alguien que posee ansia de tener conocimientos sobre algo que tiene en sus manos, es una

---

[55] VIEGA RODRÍGUEZ, María José. Delitos Informáticos, http://derecho.org/comunidad/mjviega/deli_inf.htm. miércoles 01 de octubre de 2003, 14:00PM.

persona curiosa por naturaleza, al margen de su vestimenta. El Hacker, es alguien normal, con sus miedos y sus dudas, pero que posee una fuerte voluntad de pasarse horas delante del ordenador probando cosas. Le encanta descubrir como funcionan los programas o por lo menos para que sirve cada cosa a la que tiene acceso.

Cuando un Hacker llega a poseer el conocimiento necesario, es capaz de desproteger un programa o bien copiar una tarjeta electrónica, gracias a los conocimientos que adquiere en base a lo que a observado y estudiado. Aquí vemos algo esencial de un Hacker, ya que un bueno y verdadero Hacker apunta todo lo aprendido y no lo difunde con una sonrisa a sus amigos o conocidos simplemente aplica sus conocimientos en secreto, ya que esa es la manera de trabajar de estos individuos. Como hemos visto al Hacker le interesa e entusiasma todo lo que rodea la tecnología, la telefonía celular, los ordenadores, las tarjetas de crédito electrónicas o los satélites estos sujetos normalmente los vamos a ver hasta en las calles con pesados libros de electrónica, informática, así como libros de técnicas nuevas en cuestión de técnicas informáticas, es una persona común y corriente, con grandes conocimientos acomunados en base de curiosidad y fuerza de voluntad, los cuales que al obtener estos conocimientos y llevados por los malos caminos pueden llevar a este a constituirse en aquellos personajes que realmente llegan a ser los agresores de la Red Mundial de la Información.

2.7. Calificación de los Agresores de la Cibersociedad.

Como hemos visto hay una gran diferencia entre un Hacker únicamente entra al equipo informático de otro usuario, para ver su información y si le interesa algo poder hacer una copia y almacenarla para si, es obtener más conocimiento en base a otros.

Hay que hacer una aclaración de las personas que son agresores en la Cibersociedad y el papel que tienen cada uno de ellos para no tener una confusión, como podría ser en el caso de que la sociedad ya que la gente actual desconoce quienes son los personajes dentro de este sistema de Internet de los daños y como se producen. Ya hemos visto lo que es un Hacker pero hay otro tipo de personas que causan otros daños no solo espionaje o robo de información sin daño alguno.

En la actualidad son cada día más comunes los jóvenes que se autodenominan, Hackers sin serlo, esto es que en ocasiones lo único que hacen, es soltar virus en la red y

probar programas de Hacking sin llegar a tener el conocimiento pleno. Esto es lo que confunde a las personas en cuestión de ubicarlos. Este tipo de individuos si son algo violentos y dañan lo material, son personas que disfrutan dañando a los demás usuarios, cuando sueltan sus Virus o Gusanos en la Red de la Información.

Vamos a hacer una distinción de cada uno de los individuos que dañan a los usuarios en la Cibersociedad para conocerlos y no tener una confusión de cada una de las actividades, como es en Derecho existen diversos tipos de delincuentes con características diferentes en la Cibersociedad, de la misma manera encontramos diferentes tipos de agresores dedicados a dañar los equipos de otros usuarios, estos agresores informáticos los vamos a encontrar clasificados en diversos sitios de Internet, en la mayoría sólo tiene contemplados a los famosos Hacker, haciendo una serie investigación para encontrar las figuras de los agresores informáticos ; http://derecho.org/comunidad/mjviega/deli_inf.htm, http://www.delitosinformaticos.com/noticias/archivo/arc6-2001.shtml.

2.7.1. Los Crackers.

Estos individuos son Hackers con intencionas más allá de la experimentación en casa, más allá del espionaje, como su nombre lo indica cambian de Hackers Crackers, a reventar a tronar.

Un Cracker se dedica única y exclusivamente a Tronar o Reventar como lo dice el nombre los sistemas informáticos, o bien los sistemas electrónicos. Este tipo de sujetos obtienen una satisfacción absoluta cuando logran tronar un sistema y esto se convierte una obsesión compulsiva, nunca se satisfacen de hacerlo y tratan de demostrarle al mundo entero que tiene el control y que saben más que cualquier otro. Entre ellos existe una competencia para demostrar quien es el mejor, pero claro esta que todos y cada uno de estos sujetos tiene conocimientos necesarios y diferentes para quebrar cualquier sistema aun protegido.

Existen dos clases lo que nunca revelaran su acción, y los que si lo hacen y publican por la red sus programas capaces de reventar los programas de otros. Esta es la razón por la que se les denomina Ckackers, por que su objetivo es tronar los Sistemas de Información y seguridad aun violando la filosofía de los propios Hackers que no dañan a los usuarios solo

espían y hacen una copia robando la información, que es todo lo contrario que hace un Cracker.

2.7.2. Los Gurus.

Estos son personas que tienen gran conocimiento en la Informática, se puede decir que son los maestros y son hasta cierto punto los que enseñan a los Hackers la gran mayoría son personas jóvenes, los cuales como ya dijimos tiene amplios conocimientos y experiencia en los Sistemas Informáticos y electrónicos, son los que están de alguna forma para resolverle las dudas a los aprendices de Hacker en cualquier tema.

Son personajes que no dicen lo que realizan pero cuando encuentran a una persona que tiene interés y le demuestra que tiene conocimientos e interés en los temas de Informática, pueden descubrirse con ellos y ofrecerle sus conocimientos en el tema, lo identifican como el mejor de su serie. El Guru no es un sujeto activo en cuestión de usuario, pero absorbe demasiados conocimientos y nunca deja de estudiar y practicar los temas en relación a ello, aumentando conocimientos propios pero este solo enseñara las técnicas básicas, nunca todo lo que sabe.

2.7.3. Los Lamers.

Estos si son sujetos realmente peligrosos, no tienen conocimientos reales es decir no saben nada, y son los clásicos que creen que tiene el mundo de la Informática en sus manos, esto es que si, llegara a caer en sus manos un programa generador de Virus, simplemente los sueltan en la Red y con expresiones estúpidas hacen a larde de lo que son capaces de hacer.

Los Lamers son aquellos que se meten a la red y rastrean en la basura Cibernetica, bajan todos los programas que pueden y los prueban. Es el típico tipo que se pasa la vida molestando a los demás, enviando Bombas Lógicas o Virus por la Red, y lo peor de todo esto que son tipos que creen saber lo que hacen cuando no tienen ni la idea de cómo resolverlo.

En la actualidad cualquier individuo es capaz de manejar un programa determinado con poco o casi nada de enseñanza de la informática, ya que es información que por lógica se da clic en el lugar determinado el programa se ejecutara automáticamente, y en esencia

es lo que hace un Lamer, ejecuta programas que otros hicieron, sin saber siquiera lo que realmente hace. En realidad estos tipos son peligrosos por su falta de conocimiento y soberbia de creerse los conocedores cuando en realidad no cuentan con los conocimientos para hacer alarde de algo que hacen cuando ni siquiera ellos lo crearon o saben como se crea.

2.7.4. Los Copyhackers.

Estos son los que podremos conocer como los Falsificadores, obtiene lo que les interesa y sin ningún escrúpulo lo venden a quien creen que le interesa y comercializa los sistemas. Son personas que buscan una vida fácil, compulsivas y más que personas que buscan conocimiento solo desean conocer lo necesario. Suelen leer lo que les interesa en la red, revistas de carácter técnico en cuestiones de informática y cuando encuentra a alguien que les interesa o que les pude dar el conocimiento lo contactan para sacarles las ideas, o bien robarlas por Internet, para después copiarlas y llevarlas a la venta con el bucanero.

2.7.5. Los Bucaneros.

Estos en realidad son comerciantes, son los que comúnmente llamamos Piratas. Los Bucaneros son los que venden los productos Craqueados como tarjetas de control de acceso de canales de pago. Son personajes que no existen en la Red de la Información, solo se dedican a explotar este tipo de tarjetas que los Hardware Crackers crean.

Los Bucaneros suelen ser personas que no tiene ningún conocimiento en relación a la Informática o a la electrónica, pero si saben de negocios, estos sujetos compran al CopyHacker y revenden esta Información o producto bajo un nombre comercial, son personas con afecto a ganar dinero rápido y de forma sucia.

2.7.6. El Newbie.

Este tipo de individuos se va a encontrar como Novato. Es alguien que empieza a partir de la Red de la Información basada en el Hacking. Al principio es un joven que entra en la Internet es un novato, no sabe y no hace nada aprende de manera lenta. Muchas de las

ocasiones entra en un sistema fácil y la mayoría de las ocasiones fracasa en los intentos, por que no recuerda como hacerlo y tiene que entrar en las Paginas Web de los Hackers para estudiar nuevamente los parámetros de hacking. Es un tipo que no representa peligro alguno para los usuarios. Ya que no causa daño en el mundo de Cibersociedad es un cero a la Izquierda, ya que pocos son los que llegan a ser Hackers.

2.7.7. El Wannaber.

Son los Individuos que quieren llegar a ser verdaderos Hackers pero en realidad su mente no le da para más, son los que no consiguen aprender nada pero se esfuerzan al máximo, a diferencia del Newbie no llegan a conseguir mucho o nada en todos los casos. Sin embargo, son sujetos que poseen paciencia y actitud positiva para seguir intentado, los que también tienen es llegan a ser personas depresivas.

2.7.8. Piratas Informáticos.

No hay mucho de información de estos solo que en la mayoría de los casos la gente los confunde con los Hackers, cuando en realidad son personas que exclusivamente se dedican a copiar algún tipo de información o programas y los programas de grabación realizan todo el trabajo, ya cuando se realizo la copia lo que hacen es venderlo. Si habláramos de los derechos de Copyright, se consideran como los más peligrosos ya que estafan y crean copias ilegales haciéndose de dinero fácil.

2.7.9. Los Phreakers.

Estos sujetos cuentan con conocimientos en telefonía los cuales son insuperables, conocen perfectamente el funcionamiento y actividad de los sistemas telefónicos incluso más que los mismos técnicos de la Compañía de Teléfonos. Crean cajas de colores con funciones determinadas como por ejemplo, crean la llamada caja azul que es simplemente un sistema para desactivar el contador de la central telefónica y poder realizar llamadas gratuitas.

En la actualidad y gracias a la evolución de los sistemas telefónicos se dedican esencialmente a la creación de tarjetas prepagadas o sea se dedican a la clonación de tarjetas telefónicas

Estos personajes no tienen mucho que ver en la red, la mayor parte las veces son sujetos que suben su información a ella o bien la bajan para tener nuevas formas para mejorar sus actividades.

2.8. Ataques a la Información.

El objetivo es describir cuales son los métodos más comunes que se utilizan hoy para perpetrar ataques a la seguridad informática confidencialidad, integridad y disponibilidad de la información de una organización o empresa, y que armas podemos implementar para la defensa, ya que saber cómo nos pueden atacar y desde donde, es tan importante como saber con que soluciones contamos para prevenir, detectar y reparar un siniestro de este tipo. Sin olvidar que éstas últimas siempre son una combinación de herramientas que tienen que ver con tecnología y recursos humanos.

Los ataques pueden servir a varios objetivos incluyendo fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar un sistema. Esto puede ser realizado por empleados internos que abusan de sus permisos de acceso, o por atacantes externos que acceden remotamente o interceptan el tráfico de red.

A esta altura del desarrollo de la sociedad de la información y de las tecnologías computacionales, los piratas informáticos ya no son novedad. Los hay prácticamente desde que surgieron las redes digitales, hace ya unos buenos años. Sin duda a medida que el acceso a las redes de comunicación se fue generalizando, también se fue multiplicando el número de quienes ingresan ilegalmente a ellas, con distintos fines.

Genios informáticos, por lo general jóvenes que apenas pasan los veinte años, se lanzan desafíos para quebrar tal o cual programa de seguridad, captar las claves de acceso a computadoras remotas y utilizar sus cuentas para viajar por el ciberespacio, ingresar a redes de datos, sistemas de reservas aéreas, bancos, o cualquier otro lugar más o menos peligroso.

Como los administradores de todos los sistemas, disponen de herramientas para controlar que; *"todo vaya bien", "si los procesos son los normales o si hay movimientos sospechosos, por ejemplo que un usuario esté recurriendo a vías de acceso para las cuales*

no está autorizado o que alguien intente ingresar repetidas veces con claves erróneas que esté probando. Todos los movimientos del sistema son registrados en archivos, que los operadores revisan diariamente."[56]

2.8.1. Métodos y Herramientas de Ataque.

En los primeros años, los ataques involucraban poca sofisticación técnica. Los empleados disconformes o personas externas con acceso a sistemas dentro de la empresa utilizaban sus permisos para alterar archivos o registros. Las personas que atacan desde afuera de la ubicación física de la organización, ingresaban a la red simplemente averiguando una password o conocido como clave de acceso válida.

A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar lugares en la Red de la Información así como también para poder realizar configuración y operación de los sistemas en los cuales no se encuentran autorizados. Esto permite a los nuevos atacantes tomar control de sistemas completos, produciendo verdaderos desastres que en muchos casos lleva a la desaparición o bien al daño interno en sus sistemas o bases de datos de aquellas organizaciones o empresas con altísimo grado de dependencia tecnológica como podríamos nombrar entre algunos a bancos, servicios automatizados, etc.

Estos nuevos métodos de ataque han sido automatizados, por lo que en muchos casos sólo se necesita conocimiento técnico básico para realizarlos. El aprendiz de intruso o Hacker tiene acceso ahora a numerosos programas de numerosos "Hacker", en donde estos publican sus conocimientos, así como sus códigos de conducta, donde además encuentra todas las instrucciones para ejecutar ataques con las herramientas disponibles.

> *"Los métodos de ataque están divididos en categorías generales que pueden estar relacionadas entre sí, ya que el uso de un método en una categoría permite el uso de otros métodos en otras. Por ejemplo: después de crackear una password, un intruso realiza un "login" que quiere decir que se registra el en el sistema de otro como usuario legítimo para navegar entre los archivos y explotar vulnerabilidades del sistema. Eventualmente también, el atacante puede adquirir derechos a lugares que le*

[56] http://www.monografias.com/trabajos/hackers/hackers.shtml, miércoles 12 de marzo de 2003, 12:00 PM.

permitan dejar un virus u otras bombas lógicas para paralizar todo un sistema antes de huir."[57]

2.8.2. Eavesdrompping y Packet Sniffing.

Muchas redes son vulnerables al eavesdropping, o dicho de otra manera la pasiva intercepción sin modificación del tráfico de red. En Internet esto es realizado por packet sniffers, que no son más que programas que monitorean los paquetes de red que están direccionados a la computadora donde están instalados. El sniffer puede ser colocado tanto en una estación de trabajo conectada a red, como a un equipo router o a un gateway o también dicho equipos móviles de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías. Existen kits o paquetes disponibles para facilitar su instalación.

Este método es muy utilizado para capturar Nombres de Identificación y claves de acceso de usuarios, que generalmente viajan y durante este viaje se conectan a la Red de la Información por medio de estos sistemas de acceso remoto.

"También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mailes entrantes y salientes. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos, como podría ser la información que se transmiten entre si."[58]

2.8.3. Snooping y Downloading.

Los ataques de esta categoría tienen el mismo objetivo que el sniffing, obtener la información sin modificarla. Sin embargo los métodos son diferentes. Además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en la mayoría de los casos un downloading o bien bajar la información, que no es más que pasar esa información a su propia computadora.

"El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos más resonantes de este tipo de ataques fueron :el robo de un archivo con más de 1700

---

[57] Idem.
[58] Idem.

números de tarjetas de crédito desde una compañía de música mundialmente famosa, y la difusión ilegal de reportes oficiales reservados de las Naciones Unidas, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra."[59]

2.8.4. Tampering ó Data Diddling

Esta categoría se refiere a la modificación desautorizada de los datos, o al software instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada. O aún si no hubo intenciones de ello, el administrador posiblemente necesite dar de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada. Como siempre, esto puede ser realizado por insiders, personas que tienen acceso directo u outsiders personas que entran por otra parte del sistema sin acceso directo, generalmente con el propósito de fraude o dejar fuera de servicio de un competidor.

Son innumerables los casos de este tipo como empleados o externos bancarios que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que se les anule la deuda por impuestos en el sistema municipal.

Múltiples Web Sites o sitios de Internet han sido víctimas del cambio por imágenes terroristas o humorísticas, o el reemplazo de versiones de software para download por otros con el mismo nombre pero que incorporan código malicioso o bien virus troyanos.

La utilización de programas troyanos esta dentro de esta categoría, y refiere a falsas versiones de un software con el objetivo de averiguar información, borrar archivos y hasta tomar control remoto de una computadora a través de Internet.[60]

---

[59] Idem.
[60] Idem.

2.8.5. Spoofing.

Esta técnica es utilizada para actuar en nombre de otros usuarios. Una forma común de spoofing, es conseguir el nombre y clave de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él, como puede ser el envío de falsos e-mail.

El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y en otro. Este proceso, llamado Looping, tiene la finalidad de evaporar la identificación y la ubicación del atacante. El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país. Otra consecuencia del looping es que una compañía o gobierno pueden suponer que están siendo atacados por un competidor o una agencia de gobierno extranjera, cuando en realidad están seguramente siendo atacado por un insider quien no es más que un sujeto que trabaja desde adentro de la compañía o por un estudiante a miles de Km. de distancia, pero que ha tomado la identidad de otros.

El looping hace su investigación casi imposible, ya que el investigador debe contar con la colaboración de cada administrador de cada red utilizada en la ruta, que pueden ser de distintas jurisdicciones.

Los protocolos de red también son vulnerables al spoofing. Con el nombre de usuario y clave de acceso, el atacante genera paquetes de Internet con una dirección de red falsa en el campo "From" de un e-mail, pera que sea aceptada por el destinatario del paquete.

El envío de falsos e-mail es otra forma de spoofing permitida por las redes. Aquí el atacante envía a nombre de otra persona e-mail con otros objetivos.

> *"Tal fue el caso de una universidad en USA que en 1998 debió reprogramar una fecha completa de exámenes ya que alguien en nombre de la secretaría había cancelado la fecha verdadera y enviado el mensaje a toda la nómina de 163 estudiantes. Muchos ataques de este tipo comienzan con ingeniería social, y la falta de cultura por parte de los usuarios para facilitar a extraños sus identificaciones dentro del sistema. Esta primera información es usualmente conseguida a través de una simple llamada telefónica."*[61]

[61] Idem.

2.8.6. Jamming o Flooding

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más puede utilizarla.

Muchos proveedores de Internet han sufrido bajas temporales del servicio por este tipo de ataque. Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección Identificación Personal del emisor, el mensaje contiene falsas direcciones de Identificación Personal o sea que este ataque involucra también spoofing. El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.

> *"Muchos usuarios de Internet han sido dados de baja por el "ping de la muerte", una versión-trampa del comando ping. Mientras que el ping normal simplemente verifica si un sistema esta enlazado a la red, el ping de la muerte causa el reboot o el apagado instantáneo del equipo.*
>
> *Otra acción común es la de enviar millares de e-mail sin sentido a todos los usuarios posibles en forma continua, saturando los distintos servidores de destino."*[62]

2.9. Otro tipo de Delitos Informáticos Conocidos.

Esta siguiente clasificación de delitos Informáticos a pesar de que no es tema central de este trabajo, no pretende ser una clasificación con un criterio metodológico propio, sino simplemente una enumeración que he realizado de los delitos informáticos que se conocen, para que podamos tener un amplio criterio de las diferentes modalidades delictivas que podemos encontrar en la Red de la Información.

1. Delitos contra la propiedad intelectual.
2. Delitos contra la propiedad industrial.
3. Delitos contra el mercado.
4. Delitos por daño o falsedad.
5. Delitos por estafa.

---

[62] Idem.

6. Delitos por injurias.
7. Delitos contra la libertad: amenazas.
8. Delitos por provocación sexual y prostitución. Y por supuesto el que nos importa:
9. Delitos contra la intimidad.

2.9.1 Manipulación de los Datos de Entrada. Insiders.

Estamos ante un fraude informático, conocido también como sustracción de datos y estamos ante el delito informático más común ya que es fácil de cometer y difícil de descubrir. *"Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos."*[63]

2.9.2. La manipulación de Programas.

Otro caso muy difícil de descubrir y a menudo pasa inadvertida debido a que el sujeto activo en este caso debe tener conocimientos técnicos concretos de informática. Consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas.

> *"Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora en forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal. El nombre se debe al episodio de la Ilíada de Homero, Ulises urdió una estratagema en virtud de la cual le regala a los troyanos un gran caballo de madera, que en el interior ocultaba soldados, haciendo creer que el ejército griego abandonaba el sitio de la ciudad. El caballo entró en el recinto amurallado de Troya y aprovechando la noche y la confianza de los habitantes, los guerreros ocultos hicieron entrar a las tropas griegas que aguardaban en las puertas de la ciudad."*[64]

---

[63] VIEGA RODRÍGUEZ, María José. Delitos Informáticos, http://derecho.org/comunidad/mjviega/deli_inf.htm. miércoles 01 de octubre de 2003, 14:00PM.

[64] Idem.

2.9.3. Manipulación de los Datos de Salida. Outsiders.

El caso de manipulación más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.

> *"Tradicionalmente esos fraudes se hacían a partir de tarjetas bancarias robadas, sin embargo, hoy en día se usan equipos y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito."*[65]

2.9.4. Fraude Efectuado por Manipulación Informática. Técnica del Salami.

Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salami" en la que cantidades de dinero muy pequeñas, como es que; *"se van sacando repetidamente de una cuenta y se transfieren a otra. Esta modalidad de fraude informático se realiza sin grandes dificultades y es muy difícil de detectar. Uno de los casos más ingeniosos en el "redondeo hacia abajo", que consiste en una instrucción que se le da al sistema informático para que transfiera a una determinada cuenta los centavos que se descuenten por el redondeo."*[66]

2.10. Daños o Modificaciones de Programas o Datos de los Sistemas de Computo.

El tema esencial de este trabajo de investigación, es en relación a el Daño o la Modificación del cual puede ser víctima un usuario de Internet, que podrían ser delitos en contra de la Intimidad, como hemos podido apreciar anteriormente, algunos Virus Informáticos pueden causar este tipo de actividad en el Sistema de Computo, antes de poder ver lo que es en si el tema central de esta investigación, como hemos visto y tratado a los creadores de los daños en Internet, también hay que apreciar y conocer lo que son los virus informáticos, y lo las consecuencias que traen consigo en los equipos de computo.

---

[65] Idem.
[66] Idem.

2.10.1. Los Virus Informáticos.

Los Virus Informáticos son principalmente amenazas en la Red de la Información de Internet, no son más que, meros programas para los Equipos de Computo, estos programas son de extensión relativamente pequeña, es decir, no son detectados tan fácil ya que no ocupan gran espacio en la computadora, son programas con las características de poder autorepetirse o bien con otras palabras son capaces de autoreproducirse, en todos los archivos de una computadora, este método lo que llega a provocar en si en los equipos de computo es que bloquea y satura el disco duro de la PC.

Otros Virus Informáticos poseen la capacidad de controlar tanto los ficheros como el sistema operativo de nuestro Equipo de Computo, esto provoca que no encontremos los archivos donde los hayamos guardado o bien que la computadora haga actividades que no le hemos ordenado.

Pero no todos los Virus Informáticos son malignos ya que también hay benignos los cuales solo muestran mensajes en la pantalla, pueden actuar simplemente haciendo mensajes sin sentido o bien que detectaron errores en los Equipos de Computo y automáticamente este Virus indica el error, sin causar daño alguno al Equipo de Computo.

Los Virus Informáticos poseen características esenciales que los hacen perfectamente reconocibles por la forma en que se desempeñan en los Equipos de Computo, aunque suene raro los Virus Informáticos poseen un proceso de la Vida, Creación, Contagio, Incubación, Reproducción y Ataque.

2.10.2. Vida y Creación de los Virus Informáticos.

Como hemos visto los Virus Informáticos se crean o nacen en el Sistema de Computo como subprograma o microprograma ejecutable. Una vez creado este se va a soltar en la Red de la Información de Internet dentro de un programa comercial de gran difusión, esto claro con el fin de asegurar un contagio rápido y masivo.

"Después de la primera fase que es la creación del Virus Informático, vienen las más importantes a cumplir de forma automática e independiente del control del creador del Virus, que son las fases de contagio, incubación, multiplicación y ataque."[67]

2.10.3. Contagio e Incubación de los Virus Informáticos.

El contagio es la fase más fácil de todo este proceso. Solo hay que tener en cuenta que el Virus Informático debe introducirse o soltarse en la Red de la Información de Internet. El Virus Informático debe de ir incrustado en un archivo de instalación o en una simple pagina Web.

Las vías de infección son también principalmente disquetes, programas copiados, Internet o el propio correo electrónico.

"En la Incubación, normalmente los Virus Informáticos se crean de formas específicas que atiende a una serie de instrucciones programadas, como es el esconderse y reproducirse mientras se cumplen unas determinadas opciones predeterminadas por el creador del Virus. Así el Virus permanece escondido reproduciéndose en espera de activarse cuando se cumplen las condiciones determinadas por el creador. Este proceso puede ser muy rápido en algunos casos y bastante largo en otros, según el tipo de virus."[68]

2.10.4. Reproducción y Ataque de los Virus Informáticos.

La reproducción del Virus Informático consiste en la producción del Virus de una copia de si mismo, que se situara en otro archivo distinto al que ocupa. De esta forma el virus se contagia en otros archivos y otros programas, asegurándose que el proceso de multiplicación esta asegurado. Además el Virus se asegura automáticamente de pasar a otros Sistemas de Cómputo y esto lo debe de hacer de la forma más discreta y rápida que posible. Durante este proceso os virus no se van a manifestar en los Sistemas de Computo ya que únicamente se están instalando y esto entre más lugares donde se puedan dispersar es aun mucho mejor para este programa, ya que de esta forma tendrán muchísima más posibilidad de dañar un mayor numero de Sistemas de Cómputo.

---

[67] HERNÁNDEZ, Claudio. Los Clanes de la Red, Revista Española Hackers 1999. Pág. 29.
[68] Idem

En cuanto se cumplen los comandos anteriores del los Virus Informáticos, este entra en su actividad esencial que puede ser de destrucción. Aquí en este punto el Virus Informático realiza la actividad de borrar la Información del disco Duro o memoria o borra archivos de nuestra PC.

Este ataque es el ultimo punto de actividad de los Virus Informáticos, cuando se llega a este punto el trabajo se a culminado y cumplido con el objetivo. *"El Equipo de Cómputo se encuentra infectado y si no se dispone de un programa que elimine el Virus, jamás se podrán recuperar los archivos. Podremos reparar el Equipo de Cómputo pero e instalar un nuevo software pero de nuevo corremos el riesgo de que se destruya nuestra información inmediatamente se cumplan las características anteriores. Al igual que el Virus Informático, existen programas para destruir a estos que son denominados vacuna antivirus."*[69]

2.10.5. Tipos de Virus.

Los Virus Informáticos como hemos visto son programas creados con ideas y fines distintos dependiendo de la persona que los haya creado, los Virus Informáticos son denominados de esta manera para que todos tengamos un conocimiento común en relación a estos.

Existen Virus Informáticos que únicamente se encargan de robar las claves de los ordenadores, otros simplemente van a saturar el disco duro de información basura y otros tantos se dedicaran exclusivamente a mostrarnos multitud de publicidad de Internet o bien mandando esta misma a nuestro correo electrónico hasta saturarlo, esta clase de Virus Informáticos se citaran y dará una breve explicación de ellos.

2.10.6. Caballo de Troya.

> *"Son programas que normalmente ocupan poco espacio, se instala a voluntad en el interior de un ejecutable. Este subprograma se coloca en un lugar seguro del Sistema de Computo para no ser detectado y no modifica nada de los archivos comunes de el Sistema de Cómputos, y una vez realizado esto se deben de cumplir las*

[69] Ibidem. p30

especificaciones anteriores el Caballo de Trolla, muestran mensajes que sugieren o piden la contraseña al usuario de el Sistema de Cómputo al que se infecto. En otro de los casos simplemente lee el nombre de usuario y la clave personal cuando nos conectamos a la Red de la Información, inmediatamente lo copia y lo manda por correo electrónico al Hacker que lo creo sin que el usuario se de cuanta. Son programas fáciles de monitorear en la Red de la Información, dependiendo de que tan sofisticado sea el caballo de Troya."[70]

2.10.7. Bomba Lógica.

"Estos son especialmente hechos por los Crackers, al bomba lógica esta especialmente diseñada para dañar el Equipo de Computo. Existen dos tipos de bombas lógicas, una se instala nuestro Sistema de Cómputo después de ser bajado junto a un mensaje de E-mail, se incuba sin crear copias de si mismo a la espera de completar el ciclo, posteriormente el programa se activa y se autoreplica hasta dañar nuestro Equipo de computo. En el segundo caso, alguien en vía la bomba lógica por E-mail y este no es más que el mismo mensaje reenviado miles de veces hasta colapsar la PC."[71]

2.10.8. Worm o Gusano.

Son programas que tiene como fin el colapsar cualquier sistema, Se fábrica de forma análoga al virus, se infiltra en los programas ya sea para modificar o destruir los datos, pero se diferencia de los virus porque no pueden regenerarse. Las consecuencias del ataque de un gusano pueden ser graves, por ejemplo un programa gusano puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita y luego se destruirá.[72]

"Los Gusanos o Works. Suelen habitar en la Red de Información, a veces como respuesta de grupos de "Hackers"que pretenden obtener algo. La existencia de estos gusanos se hace notar, cuando la Red de Información se hace lenta

---

[70] Ibidem. p31

[71] Idem.

[72] VIEGA RODRÍGUEZ, María José. Delitos Informáticos, http://derecho.org/comunidad/mjviega/deli_inf.htm. miércoles 01 de octubre de 2003, 14:00PM.

considerablemente, ya que normalmente el proceso de autoreplicado llena normalmente el ancho de banda de trabajo de un servidor en particular."[73]

No estamos libres de estos, en cualquier momento nuestros sistemas de computo pueden ser victimas de estos gusanos, por ello es necesario contar con un sofisticado sistema Anti Virus, en cual los pueda detectar, pero claro esta este antivirus debe ser actualizado constantemente para así evitarlos.

2.10.9. Spam.

Es simplemente un bombardeo publicitario, es un envío masivo, indiscriminado de determinada publicidad la cual ni siquiera hemos solicitado, este envío es a través de nuestro correo electrónico.

Este no se trata en si de un programa dañino, pero si es bastante molesto, se trata de un simple programa que ejecuta una orden repetidas veces. Normalmente en correos electrónicos como hemos mencionado. Así un mensaje puede ser enviado varios cientos de veces a una misma dirección.

"En cualquier caso existen programas AntiSpam, ya que los Spam son empleados normalmente por empresas de publicidad directa."[74]

---

[73] HERNÁNDEZ, Claudio. Los Clanes de la Red, Revista Española Hackers 1999. Pág. 32

[74] Idem.

Capítulo III
Legislación en Materia de la Privasidad en Internet.

Capítulo III. Legislación en Materia de la Privacidad en Internet

3.1. Internet y su Regulación.

El mundo actual todos somos testigos de lo que ha sido el crecimiento del uso del la Red de Internet, este crecimiento se ha hecho de una manera matemática, es decir, se ha ido multiplicando desde un inicio hasta nuestros días, como hemos visto al inicio de esta investigación, todo fue evolucionando y ha traído muchísimos cambiado consigo el Internet, de ser una Red de Información exclusiva de Científicos, Militares, Diplomáticos o Jefes de Estado, hoy en día los nuevos pobladores de está o mejor llamados cibernautas, son gente común y corriente, es gente muy variada la cual tiene la necesidad de conectarse a la Red de Información de Internet, para obtener información de diversos tipos, son usuarios los cuales van a buscar desde la dirección de un restaurante, revisar su correo electrónico, buscar datos en relación a información de conocimientos generales, leyes y reglamentos, hasta la posible inversión en bienes raíces, traspasos bancarios, claro esta también sin dejar de visitar los diversos entretenimientos que ahí se encuentran.

Antes de iniciar el tema de las leyes que tratan de regular lo que es la Red de Información podemos hacer un recordatorio en relación a lo que ha sido en inicio de nuestra civilización, al recordar diversas clases en las cuales se estudia el origen de la civilización recordamos que al inicio de la vida social del hombre este se reunía en muy pequeños grupos de los cuales se regían bajo las leyes del padre o la madre, o se de un patriarcado o matriarcado, estos grupos se aislaban unos de otros, en donde no habían casi conflictos, pero con el pasar del tiempo como siempre a sido, todo evoluciona y se transforma, requiriendo nuevas necesidades para todos, como es el caso de que los pueblos crecen a tal grado que ya no son tribus unidas por la sangre sino que se empiezan mezclar las aldeas y se requiere la creación de normas que puedan evitar los conflictos entre estos habitantes ya sea por tierras ganado o entre ellos mismos, ya que no era lo mismo el que las familias tenían su modos y reglas de conducta a el empezarse a mezclar con diferentes personas ajenas a su familia

Los habitantes ya no solo eran ascendente y descendientes sino que llego un momento en que se empezaron a unir vecinos, amigos de otros pueblos y hasta extranjeros con distintos idiomas y costumbres, es aquí en donde no bastó que existiera una ley del más viejo, o la ley creada para una familia, sino que gracias a la evolución del proceso social

surge el derecho como la respuesta a la regulación de la actividad social del hombre, como nos dice Eugene Petit:

> *"El hombre está dotado de una voluntad libre que le permite desenvolver sus facultades naturales. Pero, en sociedad, esta libertad está forzosamente limitada por el respeto de la libertad de otros. De aquí deriva la necesidad de reglas que garantice a cada miembro del cuerpo social, con una medida igual, el ejercicio de su actividad. La teoría de estos principios constituye el derecho, en su aceptación más extensa. La palabra derecho se deriva, en efecto, de dirige, e implica una regla de conducta. De este modo considerado, el derecho es el conjunto de reglas que rigen las relaciones sociales."*[75]

Todo lo anterior proviene a que, en la actualidad estamos viviendo un proceso de crecimiento similar al que se presentó en nuestra sociedad debido al crecimiento de Internet, es decir, de ser una pequeña Cibercomunidad aislada exclusiva para determinadas personas, a pasado a ser, un gran numero de usuarios, es decir una Cibersociedad, de grandes grupos con perfiles e intereses diversos entre si, es aquí en donde entra la historia de nuestra sociedad aplicada al desarrollo de la Red de la Información de Internet, ya que esta cuenta con reglas de protocolo en si, es decir, no hay reglas explicitas, sino reglas de conducta para los que lo usan, y que están por demás decirlas, que es el respeto a todos y todo lo que hay en Internet.

Como hemos visto no tiene una regla para crearse o para regirse, es simplemente algo que se creó y que todos pueden entrar hacer y ver, es aquí en donde entran estas reglas como lo podemos ver en esta misma publicación hecha por Internet:

> *"la red ha ido desarrollando reglas muy simples de convivencia que se conocen como Netiquette (o reglas de etiqueta para la red) y que están basadas en usos y costumbres que han tratado de prevalecer entre algunos usuarios de Internet. Sin embargo, estas normas mínimas, poco a poco han empezado a ser rebasadas por la sociedad virtual. Por ejemplo, baste citar que una de esas reglas, tal vez la más elemental, que es la de abstenerse de enviar correos electrónicos a quien no lo pide, está francamente anulada por las compañías generadoras de "spam" que atosigan con anuncios de toda clase (algunos sexualmente explícitos) a los usuarios de correo electrónico, que en ocasiones encuentran decenas de estos anuncios."*[76]

---

[75] PETIT, Eugéne. Tratados Elementales de Derecho Romano. 13ª edición. Editorial Porrúa, México 1997. Pág. 15.

[76] CISNEROS RUIZ, Juan Carlos. Internet y su regulación. http://www.interclan.com/fenasem/lexmatic/regular.htm. miércoles 26 de febrero de 2003. 12:00 PM.

Podemos encontrar en la Red de la Información de Internet, que hay publicaciones que señalan que Internet es un sistema público que no debe de ser regulado por leyes, sino que debe continuar con normas de conducta, podemos apreciar también que nos dicen:

> *"Aquí habría que hacer una reflexión: existen dos tipos de normas en una comunidad, las "morales" que tienen que ver con los usos y costumbres y las normas "legales" que derivan de leyes, reglamentos o disposiciones que son de observancia obligatoria; en caso de las normas morales (como pudieran ser las normas de cortesía) estas pueden ser seguidas o no por los ciudadanos; en cambio las normas legales, si no son cumplidas se establecen sanciones y se utiliza la fuerza del Estado para obligar su cumplimiento."*[77]
>
> *"Hasta estos momentos Internet vive sin normas legales, sino con simples normas de cortesía, que poco a poco han pasado a ser letra muerta. Este hecho, que en un principio no molestaba a nadie, la comunidad de Internet era tan pequeña y selectiva que prácticamente la actividad era residual- actualmente se está incluyendo en la agenda legislativa de muchos países como una prioridad a tratar para su inmediata regulación, cuando hace apenas unos años desconocían siquiera su existencia."*[78]

3.2. Legislación en Materia

Para poder desarrollar este capítulo cabe señalar que desgraciadamente no hay suficiente legislación que regule la privacidad de los individuos, al ser fácilmente vulnerados por los agresores en el momento de que su información es robada, cambiada o simplemente borrada de los equipos de cómputo. En el desarrollo de estos capítulos vamos a poder apreciar la legislación que regula administrativa y penalmente las conductas ilícitas las cuales están relacionadas con el punto de la informática, pero hay que resaltar que a pesar de esto, aún no contemplan en sí los Delitos Informáticos.

Como hemos dicho en la mayoría de los casos hablan y protege los derechos de autor, más no, en si la privacidad de los usuarios comunes los cuales son los que mas tiempo se encuentran en la Red de la Información, y quienes la hacen crecer, las leyes que veremos a continuación son leyes que están más encaminadas a proteger a aquellos que

[77] Idem.
[78] Idem.

dejan es si dinero a las arcas de los gobiernos, pero también hay que reconocer que si se provoca un daño, o destrucción de información o equipo de computo se esta propiciando la piratería, por el hecho de que al dañar un equipo es caro el nuevamente renovarlo o adquirirlo nuevo.

3.3. Tratado de Libre Comercio de América del Norte (TLC).

En este sentido, hay que tomar en cuenta el artículo 133 Constitucional en el cual establece: *"ART. 133.-Esta Constitución, las leyes del Congreso de la Unión que emanen de ellas y todos los Tratados que estén de acuerdo con la misma, celebrados y que se celebren por el Presidente de la República, con aprobación del Senado, serán la ley Suprema de toda la Unión. Los jueces de cada Estado se arreglarán a dicha Constitución, leyes y tratados, a pesar de las disposiciones en contrario que pueda haber en las Constituciones o leyes de los Estados."*[79]

El Tratado de Libre Comercio de América del Norte. Es un instrumento internacional firmado por el Gobierno de México, de los Estados Unidos y Canadá en 1993, contiene un apartado sobre propiedad intelectual, a saber la 6a. parte capítulo XVII, en el que se contemplan los derechos de autor, patentes, otros derechos de propiedad intelectual y procedimientos de ejecución en relación a estos. Debemos señalar que haremos una simple explicación del contenido del tratado, debido a que desgraciadamente habla más de lo que es la protección de la propiedad intelectual y no en si de lo relevante a delitos informáticos.

Así bien, como hemos señalado hay un apartado en el artículo 1714 del citado Tratado, en el cual los tres Estados Parte de este contemplaron la defensa de los derechos de propiedad intelectual esto es con el fin de con esto el derecho interno del tratado contenga procedimientos de defensa de los derechos de propiedad intelectual, así también para que permitan la adopción de medidas eficaces contra cualquier acto que infrinja los derechos de propiedad intelectual comprendidos en el capítulo específico del tratado. Debemos destacarse el contenido del párrafo 1 del artículo 1717 titulado Procedimientos y Sanciones Penales en el que de forma en este expresa se contempla la figura de piratería de derechos de autor a escala comercial, siendo que puede aplicarse a la informática

[79] Constitución Política de los Estados Unidos Mexicanos. 145ª edición. Editorial Porrúa. México, 2003. p175.

Por lo que se refiere a los anexos del capitulo que mencionamos cuenta con anexo que es el artículo 1718.14, titulado defensa de la propiedad intelectual, se estableció que México haría su mayor esfuerzo por cumplir tan pronto como fuera posible con las obligaciones del artículo 1718 relativo a la defensa de los derechos de propiedad intelectual en la frontera, haciéndolo en un plazo que no excedería a tres años a partir de la fecha de la firma del TLC.

Luego entonces, cabe mencionar que en el artículo 1711, que es relativo a los secretos industriales y de negocios sobre la provisión de medios legales para impedir que estos secretos, sean revelados, adquiridos o usados sin el consentimiento de la persona que legalmente tenga bajo su control la información. Hay un párrafo en cual se acerca un poco a lo que es teman de nuestro estudio, esto lo vamos a encontrar en el mismo artículo pero en el párrafo 2, el cual habla sobre las condiciones que se requieren para otorgar la protección de los secretos industriales y de negocios, uno de estos requisitos, es algo muy importante que se puede adecuar a lo nuestro, que es que toda la informaciones se debe de contener en medios electrónicos o magnéticos, los cuales van concatenados con la Informática.

3.4. Acuerdo General de Aranceles Aduaneros y Comercio (GATT).

El Gobierno de México es parte de este acuerdo que se celebró en el marco deL GATT.- Acuerdo de la Ronda Uruguay de Aranceles Aduaneros y Comercio, que como podemos destaca en lo anteriormente no habla mucho en relación a los delitos informáticos como tales, pero si podemos encontrar algo que pudiera ser aplicado dependiendo del punto de vista de quien lo vea, como lo algunos autores en la Red de la Información, podemos hacer un análisis leve de lo que es el *"Art. 10 relativo a los programas de ordenador y compilaciones de datos, serán protegidos como obras literarias de conformidad con el Convenio de Berna de 1971 para la protección de obras Literarias y Artísticas, y que las compilaciones de datos posibles de ser legibles serán protegidos como creaciones de carácter intelectual."*[80]

Es aquí en donde podemos hacer un subrayado en el cual señala que los datos y recopilación de carácter privado deberían de ser protegidos también, o sea habar un poco en

[80] Supremo Tribunal de Justicia del Estado de Sinaloa, Derechos Reservados 1998. http://www.stj-sin.gob.mx/Delitos_Informaticos2.htm#CAPÍTULO%20I, miércoles 01 de octubre de 2003, 12:00 PM.

cuanto a la privacidad de las personas para así poder acercarnos a algún medio que nos proteja como tales y de esta manera tener un medio de protección, o sea en otro punto de vista podemos decir que si tenemos información propia y personal podemos alegar a este Artículo en relación al GATT, pero este Artículo en si que lo único que protege es, Convención para la Protección y Producción de Phonogramas, Convención relativa a la Distribución de Programas y Señales.

De lo único en relación a Delitos Informáticos vamos a encontrar algo en relación a lo que es un análisis del tribunal de Justicia del Estado de Sinaloa que dice: *"Asimismo, en la sección u, denominada procedimientos penales, en particular el artículo 61, se establece que para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial, se establecerán procedimientos y sanciones penales además de que, los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias."*[81]

3.5. Constitución Política de los Estados Unidos Mexicanos.

En Nuestra Carta Magna, por obvias razones no vamos a encontrar nada en relación directa a nuestro tema, pero podemos citar el: *"ART: 16-nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, si no en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento."*[82]

En relación a este párrafo que es parte de nuestra Carta Magna, en la cual se consagran garantías individuales de las cuales todos los ciudadanos tienen el derecho a gozar, y desglosando un poco, hablar de una privacidad en nuestras posesiones, como lo que es tema de nuestra investigación, cabe señalar que tendrá que ser un tema de estudio en nuestra Constitución Política de los Estados Unidos Mexicanos se pueda desprender Artículos en los cuales podemos interpreta alguna regulación del tema de investigación de este tema, nuestras garantías deben de ser custodiadas aún en una Cibersociedad como es el caso de Internet.

---

[81] Idem.

[82] Constitución Política de los Estados Unidos mexicanos, 145a Edición. Editorial Porrúa. México, 2003.

3.6. Ley Federal de Telecomunicaciones.

En nuestro país existe una ley que esta encargada de garantizar la integridad de las vías de comunicación, a lo cual podemos decir que todo lo relacionado con la Red de la Información de Internet esta concatenado con esta Ley, a donde podemos dirigir nuestra investigación es a este artículo el cual citaremos de manera integra:

"ARTICULO 71.- las infracciones a lo dispuesto en esta Ley, se sancionará por la Secretaría de conformidad con lo siguiente:

A. Con multa de 10,000 a 100,000 salarios mínimos por:

I. Prestar servicios de telecomunicaciones sin contar con concesión por, parte de la Secretaría;

II. No cumplir con las obligaciones en materia de operación e interconexión de redes públicas de telecomunicaciones;

III. Ejecutar actos que impidan la actuación de otros concesionarios o permisionarios con derecho a ello;

IV. No llevar contabilidad separada por servicios de acuerdo a las disposiciones de esta Ley o sus reglamentos, y

V. Interceptar información que se transmita por las redes públicas de telecomunicaciones.

B. Con multa de 4,000 a 40,000 salarios mínimos por:

I Operar o explotar comercializadoras de servicios de telecomunicaciones en contravención a lo dispuesto en esta Ley y sus reglamentos;

II. Interrumpir, sin causa justificada o sin autorización de la Secretaría, la prestación total de servicios en poblaciones en que el concesionario sea el único prestador de ellos;

III. Cometer errores en la información de base de datos de usuarios, de directorios, y en el cobro de los servicios de concesionarios de redes públicas, no obstante el apercibimiento de la Secretaría, y

IV. No cumplir con las obligaciones o condiciones establecidas en los títulos de concesión o permiso;

C. Con multa de 2,000 a 20,000 salarios mínimos por:

I. Contravenir las disposiciones tarifarias;

II. Contravenir las disposiciones sobre la conexión de equipos y cableados;

III. Operar sin permiso estaciones terrenas transmisoras;

IV. Incurrir en violaciones a las disposiciones de información y registro contempladas en la presente Ley, y

V. Otras violaciones a disposiciones de esta Ley y las disposiciones reglamentarias y administrativas que de ella emanen.

En caso de reincidencia, la Secretaría podrá imponer una multa equivalente hasta el doble de las cuantías señaladas

Para los efectos del presente capítulo, se entiende por salario mínimo, el salario mínimo general diario vigente en el Distrito Federal al momento de cometerse la infracción."[83]

Como podemos ver este artículo sanciona algunas actividades ilícitas que se pueden realizar con las Vías de Comunicación, este Artículo es algo sumamente importante para nosotros por lo que vamos a analizarlo más delante de manera directa.

3.6. Ley Federal de Derechos de Autor.

En relación a esta ley no hay mucho de que hablar, por que habla exclusivamente de lo que es el Registro ante la Ley de determinadas Obras, las sanciones que esperan a los que hacen una copia de este o lo falsifican. Los programas de computación, las bases de datos y las infracciones derivadas de su uso ilícito se encuentran reguladas en la Ley Federal del Derecho de Autor del 24 de diciembre de 1996, que entró en vigor el 24 de marzo de 1997.

Esta ley no nos dice nada en relación a los hechos ilícitos de nuestros tiempos que buscamos legislación en cuestión a la protección de las personas que usan Internet.

Lo que realmente buscamos no son Derechos de Autor, sino derecho a la privacidad y a impedir el sabotaje, robo de información, daño a nuestros equipos de computo por otras personas, así también el espionaje a nuestra intimidad como usuarios de Internet, la Ley Federal de Derechos de Autor, nos van a dar la protección de programas de cómputo, y la falsificación de estos.

El punto anterior también es tema de los Delitos Informáticos, pero no exactamente de el tema que nos interesa en este tema de investigación que es el caso de la privacidad de los usuarios, lo que más protege la Ley Federal de Derechos de Autos es la falsificación,

---

[83] Ley Federal del Derecho de Autor. Diario Oficial de la Federación. Martes 24 de diciembre de 1996. Actualización en: Ley Federal de Derechos de Autor, http://www.cerlalc.org/documentos/mexint.htm domingo 30 de noviembre de 2003, 23:00 PM

que es un tema importante, pero es uno de los que esta ya legislado tanto por nuestro país, así mismo por tratados internacionales que se han firmados como ya lo hemos visto, además que este teman también esta cubierto por los demás países que protegen los Derechos de Autor.

3.7. Código Penal para el Distrito Federal, en Materia de Fuero Común y para toda la Republica en Materia de Fuero Federal.

Ponemos en primer lugar lo que nos va a señalar el Código Penal para el Distrito Federal, el cual nos va a hablar de determinados delitos que se apegan a los Delitos Informáticos que interesan a esta investigación:

"TITULO DECIMO TERCERO
DELITO CONTRA LA INTIMIDAD PERSONAL Y
LA INVIOLABILIDAD DEL SECRETO.
CAPÍTULO I
VIOLACIÓN A LA INTIMIDAD PERSONAL

Artículo 212. Se impondrá de seis meses a tres años de prisión, al que sin consentimiento de quien esté legitimado para otorgarlo y, para conocer asuntos relacionados con la intimidad de la persona:

I Se apodere de documentos u objetos de cualquier clase; o

II Utilice medios técnicos para escuchar, observar, grabar la imagen o el sonido.

Este delito se impondrá por querella.

CAPÍTULO VIII
DAÑOS A LA PROPIEDAD

Artículo 239. Al que destruya o deteriore una cosa ajena a una propia en perjuicio de otro, se le impondrá la siguiente pena:

I. De veinte a sesenta días multa, cuando el valor del daño no exceda de veinte veces el salario mínimo, o no sea posible determinar su valor.

II Prisión de seis meses a dos años y sesenta a ciento cincuenta días de multa, cuando el valor del daño exceda de veinte pero no de trescientas veces el salario mínimo;

III Prisión de dos a cuatro años y de ciento cincuenta a cuatrocientos días multa, cuando el valor del daño exceda de trescientos pero no de setecientos cincuenta veces el salario mínimo; y

IV Prisión de cuatro a diez años y de cuatrocientos a seiscientos días multa, cuando el valor del daño exceda de setecientas cincuenta veces el salario mínimo.

TITULO VIGESIMO TERCERO
DELITOS CONTRA LA SEGURIDAD Y EL NORMAL FUNCIONAMIENTO DE LAS VÍAS DE COMUNICACIÓN Y DE LOS MEDIOS DE TRANSPORTE

CAPÍTULO IV
VIOLACIÓN DE LA COMUNICACIÓN PRIVADA

"Artículo 334. A quien intervenga comunicación privada sin mandato de autoridad judicial competente, se le impondrán de dos a ocho años de prisión y de cien a mil días multa.
A quien revele, divulgue utilice indebidamente, o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le impondrá de tres a doce años de prisión y de doscientos a mil días multa."[84]

Como lo señala en anterior Código, nos da determinados delitos tipificados que nos dicen por lo que respecta al Artículo 212 en relación a la Intimidad, podemos apegarnos a el en razón a que todos somos sujetos de derecho a tener privacidad nos ayuda a poder dejar abierto el ámbito electrónico, en relación a que deja abierto al decir que cuentan todos los medios por los que disponga el agresor para violentar la intimidad de las personas.

El Artículo 239 referente al daño, solo podemos decir que es uno de los Artículos que nos van a ayudar a la defensa de propiedad y el valor que este tiene así como las sanciones por las cuales los legisladores deliberaron para imponer una sanción a este daño.

En relación al Artículo 334, nos va a remitir a las Vías de Comunicación, en la cual nos va a señalar que se impondrá sanción a quien robe información e imágenes en base a las Vías de Comunicación, esto es un tema muy importante ya que esta tomando en cuenta

[84] Nuevo Código Penal del Distrito Federal. Editorial Sista S. A. de C. V. México D. F. 2003.

los medios ocupado por la Red de la Información de Internet, que es uno de los medios por los cuales se puede robar información e imágenes.

Por lo que respecta al Código Penal Federal, cuenta con una legislación más completa en cuestiones de Delitos Informáticos y es un gran avance para nuestro país como podemos ver:

LIBRO SEGUNDO

TITULO NOVENO REVELACION DE SECRETOS Y ACCESO ILICITO A SISTEMAS Y EQUIPOS DE INFORMATICA

CAPÍTULO I

ARTÍCULO 211 BIS. A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

CAPITULO II

ACCESO ILICITO A SISTEMAS Y EQUIPOS DE INFORMATICA

ARTICULO 211 BIS 1. Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

ARTICULO 211 BIS 2. Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

ARTICULO 211 BIS 3. Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente modifique, destruya o provoque perdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

ARTICULO 211 BIS 4. Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

ARTICULO 211 BIS 5. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque perdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementaran en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

ARTICULO 211 BIS 6. Para los efectos de los artículos 211 bis 4 y 211 bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 bis de este Código.

ARTICULO 211 BIS 7. Las penas previstas en este capitulo se aumentaran hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno."[85]

Como podemos ver en el Código Penal Federal, nos va ayudar más en relación a que impone multas relevantes a la violación de la privacidad de los Usuarios de Internet, así como que no menciona directamente el Hacking pero podemos sobre entender esto, ya que señala que sancionara a quienes sin autorización destruyan, tomen información etc, de los equipos de computo también serán sancionados, pero no debemos tener solo en cuenta las sanciones penales, que son una gran apoyo y avance, pero nuestros sistemas penales ya están saturados, por que no tener ene cuenta también sanciones administrativas.

3.8. Código Penal y Procedimientos Penales de Sinaloa.

Ante la importancia que tiene que el Congreso Local del Estado de Sinaloa haya legislado sobre la materia de Delitos en Relación la Informática, podemos consideramos pertinente transcribir íntegramente el texto que aparece en el Código Penal Estatal.

Título Décimo

"Delitos contra el patrimonio"

Capítulo V

Delito Informático

"Artículo 217. Comete delito informático, la persona que dolosamente y sin derecho:

I. Use o entre a una base de datos, sistemas de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información; o

II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.

[85] Código Penal Federal, Compendio de leyes, reglamentos y otras disposiciones conexas sobre la materia 2003. grupo ISEF. México D. F. 2003.

En el caso particular que nos ocupa cabe señalar que en Sinaloa se ha contemplado al delito informático como uno de los delitos contra el patrimonio, siendo este el bien jurídico tutelado.

Consideramos que se ubicó al delito informático bajo esta clasificación dada la naturaleza de los derechos que se transgreden con la comisión de estos ilícitos, pero a su vez, cabe destacar que los delitos informáticos van más allá de una simple violación a los derechos patrimoniales de las víctimas, ya que debido a las diferentes formas de comisión de éstos, no solamente se lesionan esos derechos, sino otros como el derecho a la intimidad.

Capítulo IV
CONSIDERACIONES

Después del estudio de las experiencias adquiridas por diferentes países al enfrentar el delito informático y la forma en que está siendo regulada esta problemática en México, además del evidente incremento de esta situación, consideramos necesario a pesar de que en el país el delito informático no ha alcanzado el grado de peligrosidad existente en esos países regula penalmente las conductas ilícitas derivadas del uso de la computadora, como más adelante expondremos.

En primer término, consideramos que la difusión a las empresas, organismos, dependencias, particulares y a la sociedad en general, contribuirá notoriamente al nivel de concientizar sobre el problema que nos ocupa. El siguiente paso será dar a conocer las medidas preventivas que se deben adoptar para evitar estas conductas ilícitas.

Sin embargo, con base en que en la Ley Federal del Derecho de Autor se considera como bien jurídico tutelado la propiedad intelectual y que, el bien jurídico tutelado en los delitos informáticos es fundamentalmente el patrimonio, proponemos que en el Título Vigésimo Segundo sobre los "Delitos en contra de las personas en su patrimonio" del Código Penal para el Distrito Federal en Materia de Fuero Común y para toda la República en Materia de Fuero Federal se añada un capítulo especial para los delitos informáticos.

Teniendo en cuenta también la gravedad que implican los delitos informáticos, consideramos que es necesario que el Código Penal Federal incluya figuras delictivas que contengan los delitos informáticos ya que de no hacerlo, la ausencia de figuras concretas que se puedan aplicar en esa materia daría lugar a que los autores de esos hechos quedaran

impunes ante la ley, o bien, obligaría a los tribunales a aplicar preceptos que no se ajusten a la naturaleza de los hechos cometidos.

Por otra parte, teniendo presente que en nuestro país, el Estado de Sinaloa a través de su Congreso Local ha legislado sobre el tema de delitos informáticos, contemplando de forma general una amplia variedad de los mismos y estableciendo las sanciones correspondientes, consideramos que es necesario que con objeto de que se evite un conflicto de competencia entre los congresos locales y el de la Unión, éste con base en las facultades que la Constitución Federal le confiere, establezca los criterios necesarios para delimitar, dada la naturaleza de los delitos informáticos, que pueden emplear para su ejecución las vías generales de comunicación entre otros elementos, la jurisdicción federal y local de estos ilícitos."[86]

[86] Código Penal y de Procedimientos Penales del Estado de Sinaloa. Editorial. Anaya 1996. México, D. F.

Capítulo IV
Derecho Comparado

Capítulo IV. Derecho Comparado.

4.1. Organismos Internacionales.

El objetivo principal de este capítulo es presentar un breve análisis de acuerdos y legislaciones, así como todos aquellos elementos que han sido considerados tanto por organismos gubernamentales internacionales como por diferente legislación de otros Estados, para enfrentar la problemática en materia de los delitos informáticos, la siguiente información tiene como fin dar a conocer lo que otros países tiene a fin de combatir estos delitos y que a nosotros nos sirve a fin de que contribuir al desarrollo de esta investigación.

Luego en entonces, debemos tener en cuenta que durante los últimos años se ha ido desarrollando en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace las computadoras, de los programas de estos desarrollados con el fin de facilitar el espionaje y robo de información y mucho más, a lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales y administrativos de otras naciones.

4.1.1. Organización de Cooperación y Desarrollo Económico (OCDE)

Vamos a poder encontrar un Organismo en cual si trata un poco en relación al buen unos o mal uso que le podamos dar a una computadora como es;

> *"En 1983 la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales, a fin de luchar contra el uso indebido de los programas de computación."*[87]

Lo anteriormente mencionado nos dice que este organismo, trata en relación algo sobre lo que es el uso indebido de los programas de Computación, podríamos atrevernos a decir que si entendemos estas palabras, el darle un mal uso a un programa, también abarca a los programas de Hackers para dedicarse al espionaje, y poder robar información.

Como también lo podemos ver en que no se detuvo ahí, tratando de hacer un alcance a los países que están entrando a mas rápido a la era de las computadoras, solicitando a estos, que se realice legislación en relación, pero no hay que dejar a un lado el daño por los

---

[87] VIEGA RODRÍGUEZ, María José. Delitos Informáticos, http://derecho.org/comunidad/mjviega/deli_inf.htm. miércoles 01 de octubre de 2003, 14:00PM.

Hackers, que es lo que hace daños en información y bienes ajenos: *"En 1986 la OCDE publicó un informe titulado Delitos de informática: análisis de la normativa jurídica, donde se señalan las normativas vigentes y las propuestas de reforma en diversos Estados miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales."*[88]

Siendo este un Organismo de Cooperación para los países mas poderosos del mundo a tratado de tener en la mesa de las negociaciones todo lo relacionado a la estabilidad y desarrollo de estos para su bienestar como: *"En 1992 elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos."*[89]

4.2. Legislación en otros Países.

Se tiene en cuenta que la mayoría de los casos o de quienes hablan de un Delito Informático y los casos de abusos relacionados con la informática deben ser combatidos con medidas jurídico-penales, aunque también debemos tener presentes medidas administrativas. No obstante, para aprehender ciertos comportamientos merecedores de pena o sanciones con los medios del Derecho penal tradicional o Administrativo, existen, al menos en parte, relevantes dificultades para poder encuadrarlos. Estas proceden en buena medida, de la prohibición jurídico-penal de analogía y en ocasiones, son insuperables por la vía jurisprudencial. De ello surge la necesidad de adoptar medidas legislativas. En los Estados industriales y por que no decir de México que es una nación la cual tiene una gran cantidad de tratados con diversos países, y esto nos lleva a tener un gran contacto de manera Informática y a ser relacionados con el sistema de la gran Red de la Información de Internet, existe un amplio consenso sobre estas valoraciones, que se refleja en las reformas legales de los últimos diez años, de los cuales las naciones industrializadas se han preocupado por tratar de tener en cuanta en las mesas de legislación.

Hay algo muy importante que mencionar para efectos de esta investigación, pocos son los países que disponen de una legislación adecuada para enfrentarse con el problema

[88] Idem.
[89] Idem.

sobre el particular, de las cuales a continuación vamos a hacer un análisis de ellos para conocer un poco mas de esto, sobre todo que es lo que tiene en mesa otras naciones para ello y con objeto de que de tomen en cuenta las medidas adoptadas por ciertos países:

4.2.1. Alemania.

Alemania para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986, fue uno de los países en adoptar: *"La Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos:*

- *Espionaje de datos;*
- *Estafa informática;*
- *Falsificación de datos probatorios junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos ;*
- *Alteración de datos es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible;*
- *Sabotaje informático, destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa;*
- *Utilización abusiva de cheques o tarjetas de crédito.*
- *Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, acusación del error y disposición patrimonial, en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita."*[90]

---

[90] Supremo Tribunal de Justicia del Estado de Sinaloa, Derechos Reservados 1998. http://www.stj-sin.gob.mx/Delitos_Informaticos2.htm#CAPÍTULO%20I, miércoles 01 de octubre de 2003, 12:00 PM.

En relación a estos preceptos es necesario de la misma manera mencionar que esta solución de la cual fue citada de forma parcialmente abreviada, fue también adoptada en los Países Escandinavos y en Austria, para defenderse de los Delitos Informáticos.

Los legisladores alemanes han introducido estos nuevos preceptos penales, pero no ha llegado tan lejos como lo han hecho los Estados Unidos de Norte América. En el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de los llamados Delincuentes Informáticos, el gobierno alemán tuvo que reflexionar acerca de dónde radicaban las verdaderas dificultades para la aplicación del Derecho penal tradicional y hacer un análisis a los comportamientos dañosos en los que desempeña un papel esencial la introducción de lo que es el proceso Informático de datos, así como acerca de qué bienes jurídicos se deberían tutelar y ser merecedores de protección penal.

"Fue entonces cuando se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión, pero que en realidad tan sólo constituyen un nuevo modus operandi, que no ofrece problemas para la aplicación a determinados tipos."[91]

Por otra parte, sin embargo, la protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que éstos no pueden ser protegidos suficientemente por el Derecho vigente contra nuevas formas de agresión que pasan por la utilización abusiva de instalaciones informáticas.

Por otro lado podemos observar que, las diversas formas de aparición de lo que es la criminalidad informática las cuales ya hemos visto anteriormente van propician además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, que fue lo que en los legisladores alemanes tuvieron que tener en cuenta en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos así como también se trate del daño a sistema informáticos. Como podemos ver en las propuesta alemana va a protege bienes contra menoscabos en su estructura o función así como alteraciones de los Sistemas de Computo, esta propuesta trata de abarcar de manera importante la mayoría de los delitos Informáticos que no son tomados en cuenta o más bien como los que ya hemos visto anteriormente.

---

[91] Idem.

4.2.2. Australia.

Australia no tiene mucho en relación a sus propuestas de Leyes pero es uno de los países que tiene muy explicito el bien que quiere proteger, este país nos va a aportar: *"Ley de reforma del Código Penal de 22 de diciembre de 1987.*

Contempla los siguientes delitos:

- *Destrucción de datos, no solo datos personales sino también los no personales y los programas.*
- *Estafa informática, se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión."*[92]

Como podemos apreciar Australia es un país que también aporta gran información a nuestro trabajo de investigación en relación a la aportación jurídica, y sobre todo que estas propuestas permiten a los australianos el poder ejercer acto jurídico en contra de aquellos Hacker, a quienes nos hemos referido la mayor parte de el trabajo de investigación.

Esta propuesta por parte de Australia nos va a ayudar a proteger a los usuarios comunes quienes son los que realmente crean la Red de la Información de Internet, como podemos apreciar, el legislador australiano tomó en cuenta algo más que los que le dejan más dinero a el estado como son los derechos de autor.

4.2.3. Francia.

Francia es un país que va a hacer una gran aportación de la misma manera, ya que también toma en cuenta a los usuarios de Internet, así como en su propuesta legislativa, vamos a poder entender que no solo protege a estos sino a todos en general como la legislación del país anterior, es decir, todo aquel que tenga acceso a los medios Informáticos y sobre todo a

[92] VIEGA RODRÍGUEZ, María José. Delitos Informáticos, http://derecho.org/comunidad/mjviega/deli_inf.htm. miércoles 01 de octubre de 2003, 14:00PM.

los que usan el Internet pueden invocar en Francia estas leyes para proteger sus sistemas de Computo y ejercer en contra de aquellos que los dañen, Francia nos aporta:

"La Ley 88/19 del 5 de enero de 1988 sobre el fraude informático contempla:

- *Acceso fraudulento a un sistema de elaboración de datos. Se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.*
- *Sabotaje Informático. Falsear el funcionamiento de un sistema de tratamiento automático de datos.*
- *Destrucción de datos. Se sanciona a quien intencionalmente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos, suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.*
- *Falsificación de documentos informatizados. Se sanciona a quien de cualquier modo falsifique los documentos informatizados con intención de causar un perjuicio a otro."*[93]

4.2.4. Estados Unidos de Norte América.

Estados Unidos de Norte América es uno de los países, obviamente por ser uno de los líderes en el comercio, el que se ha dedicado un poco más a los Delitos Informáticos, y aún más en relación a lo que es el Hacking de equipos, espionaje, y daño a los sistemas de Información por los virus, gusanos y por lo llamado caballo de Troya, y esto por ser uno de los países mas atacados por ellos.

Consideramos importante mencionar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030) que modificó el Acta de Fraude y Abuso Computacional de 1986.

Para poder citar la información en relación a la aportación que nos hacen los Estados Unidos de Norte América debimos haber visto bien acerca de qué es y qué no es un virus, un gusano, un Caballo de Troya, y los demás que vimos y en que difieren uno de los otros, la nueva acta proscribe la transmisión de un programa, información, códigos o

[93] Idem.

comandos que causan daños a la computadora, al sistema informáticos, a las redes, información, datos o programas, así como quien es quien en relación a los individuos que realizan estas actividades, los legisladores norte americanos están muy interesados en evitar y luchar en contra de este tipo de actividades.

Los legisladores norteamericanos van a crear actas en relación a estos problemas, como vamos a mencionar de manera ligera y en primer lugar tenemos:

"El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. El acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión."[94]

En el Acta de 1994 aclara que el creador de un virus no escudarse en el hecho que no conocía que con su actuar iba a causar daño a alguien o que él solo quería enviar un mensaje, pero también podemos ver que aquellos que lo transmiten de manera imprudencias tienen una sanción, esta es una excelente propuesta, aunque esto ultimo también debe de tener en si que una persona que lo transmite de manera imprudencial en ocasiones ni siquiera tiene idea de que su computadora esta infectada de un virus, aquí debería de tener un perdón a aquellos que también hayan sido afectados y por medio de sus sistemas de computo se haya esparcido el virus.

Los legisladores estadounidenses, han contribuido a la nueva era con la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, ya que como se puede apreciar de manera específica que los legisladores no hacen una definición exacta de los que son los virus, lo que hacen los legisladores es hacer la descripción de el acto para dar cabida en un futuro, es decir a la nueva era de ataques tecnológicos a los sistemas informáticos y así dejar abierto el la modalidad de ataques por Internet que la manera mas frecuente que hay, así como, en cualquier forma en que se realicen. Esta ley da lugar a que se contemple qué se debe entender como acto delictivo sin ninguna duda.

---

[94] Supremo Tribunal de Justicia del Estado de Sinaloa, Derechos Reservados 1998. http://www.stj-sin.gob.mx/Delitos_Informaticos2.htm#CAPÍTULO%20I, miércoles 01 de octubre de 2003, 12:00 PM.

"En el Estado de California, en 1992 se adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta Ley.

"Consideramos importante destacar las enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en la que, entre otros, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de $10,000 por cada persona afectada y hasta $50,000, por el acceso imprudencial a una base de datos,... uno de los apartados de esta ley, se contempla la regulación de los virus (computer contaminant) conceptualizándose aunque no los limita a un grupo de instrucciones informáticas comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas."[95]

Lo que los legisladores al realizar estas enmiendas en el Estado de California, era la de aumentar la protección a los individuos, negocios, y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente. De la misma forma también, los legisladores consideraron que la el gran crecimiento en los ciudadanos de la tecnología de computadoras ha traído consigo la proliferación de creadores de virus, delitos informáticos y otras formas no autorizadas de acceso a las computadoras, como lo hemos podido apreciar anteriormente, de la misma forma como es objeto de nuestra investigación, podemos decir que esta enmienda norte americana va a tener en cuenta el espionaje y hacking a los sistemas y las bases de datos y que la protección legal de todos sus tipos y formas es vital para la protección de la intimidad de los individuos como es objeto central de nosotros, de la misma forma esta enmienda no sólo va a tener en cuenta a los individuos comunes y corrientes que hacen la población de la Cibersociedad, sino que también alberga en sí para el bienestar de las instituciones financieras, de negocios, agencias, gubernamentales y otras relacionadas con el estado de California que legalmente utilizan esas computadoras, sistemas y bases de datos, y sobre todo la Red de la Información de Internet.

---

[95] Supremo Tribunal de Justicia del Estado de Sinaloa, Derechos Reservados 1998. http://www.stj-sin.gob.mx/Delitos_Informaticos2.htm#CAPÍTULO%201, miércoles 01 de octubre de 2003, 12:00 PM.

Estas leyes creadas por los Estados Unidos de Norteamérica, son leyes muy importantes para nosotros, ya que en si trata de lo que realmente a nosotros nos interesa como es el espionaje y el hacking de los equipos de computo, estas leyes realmente aportan gran ayuda para la creación de nuevas normas en relación a la protección a usuarios.

4.2.5. Inglaterra.

En Inglaterra vamos a encontrar lo que se llama Computer Misuse Act del año 1990: introdujo el delito de acceso no autorizado. Dice "Pacheco Klein que: *"Esta cláusula de la ley fue, principalmente, una reacción a la publicidad y al medio en torno a los virus de las computadoras.*

- *El artículo 3° inciso 2° establece que la persona tiene que tener intención de "modificar el contenido de cualquier computadora", y de esa manera:*
- *Impedir la operación de cualquier computadora; o*
- *Impedir o dificultar el acceso a cualquier programa, o la confianza de esos datos.*
- *Impedir la ejecución de cualquiera de esos programas, o la confianza en esos datos."*

La ley fue criticada por su amplitud, sin embargo la obtención de evidencia desde lugares remotos ha creado problemas en la legislación inglesa.

En 1994 la ley fue reformada para permitir el acceso a la policía y a las agencias especializadas del orden a los boletines informativos."[96]

Como podemos apreciar en el análisis y la cita que tomamos del señor Pacheco Klein, estas normas inglesas no nos dicen mucho están muy a la interpretación, no están encaminadas y especificas como lo están las norte americanas, estas normas necesitan un poco de pulido ya que no cuentan con una descripción especifica de que realmente desean prohibir.

[96] PACHECO KLEIN, Jorge. Introducción a los delitos informáticos en el ciberespacio. Normas y Jurisprudencia comentadas. http://www.delitosinformaticos.com/noticias/archivo/arc6-2001.shtml. lunes 24 de febrero de 2003, 13:00 PM.

4.2.6. España.

España es uno de los países que también deja abierta la posibilidad a sancionar, esto es que no especifica las actividades pero las deja a la interpretación como vamos a ver por ello citaremos de manera integra los artículos 255 y 256 del Código Penal Español los cuales nos señalan:

"SECCIÓN 3.
DE LAS DEFRAUDACIONES DE FLUIDO ELÉCTRICO Y ANÁLOGAS

"Artículo 255.-Será castigado con la pena de multa de tres a doce meses el que cometiere defraudación por valor superior a cincuenta mil pesetas, utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos, por alguno de los medios siguientes:

1. Valiéndose de mecanismos instalados para realizar la defraudación.

2. Alterando maliciosamente las indicaciones o aparatos contadores.

3. Empleando cualesquiera otros medios clandestinos.

Artículo 256.-El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses."[97]

Este Código Penal español en el Artículo 255: sanciona cualquier actividad artificiosa o que induzca en error a una máquina como podríamos decir a un equipo de cómputo, como puede ser el ejemplo, abusar de sistemas informáticos o violar las reglas preestablecidas para el uso del teléfono; y sabemos muy bien que el sistema de Internet es a través de una línea telefónica.

De la misma manera señala la alterar en forma ilegal cualquier aparato de medición, interrumpiendo de esa manera dañosa el funcionamiento del mecanismo por cualquier medio, esto a través de la manipulación de la información como son los Caballos de Trolla que sirven para mandar información a otro sin que el usuario se de cuenta como es en los equipos de cómputo en el uso de cualquier otra forma secreta para alterar una máquina o mecanismo.

---

[97] Código penal de España, http://www.igsap.map.es/cia/dispo/cpenal-l2.htm. sábado 29 de noviembre de 2003, 12:30 PM.

En lo que respecta al Artículo 256, castiga a quienes cometan fraude a través de los sistemas de computación, y también es aplicable a los daños que pudieran causar los Hackers, ya que se puede interpretar que la actividad de navegación por la Red de la Información de Internet, la legislación de España nos manda directamente a que pertenece a las telecomunicaciones, por que el Internet es un medio en el cual nos vamos a conectar por medio de un sistema de telefonía.

4.2.7. Perú.

Por lo que respecta al ultimo de los países que cuenta con legislación especifica a los delitos informáticos que nos interesa tratar es Perú, ya que el ordenamiento jurídico peruano tipifica los siguientes delitos en relación a los equipos de cómputo, vamos a citar determinados Artículos del Código Penal peruano para su análisis como son:

"CAPITULO II
VIOLACIÓN DE LA INTIMIDAD

Artículo 154.

El que viole la intimidad de la vida personal o familiar ya sea observando, escuchando o registrando un hecho, palabra, escrito o imagen, valiéndose de instrumentos, procesos técnicos u otro medio, será reprimido con pena privativa de libertad no mayor de dos años.
La pena será no menor de uno ni mayor de tres y de treinta a ciento veinte días-multa, cuando el agente revele la intimidad conocida de la manera antes prevista.
Si utiliza algún medio de comunicación social, la pena privativa de libertad será no menor de dos ni mayor de cuatro años y de sesenta a ciento ochenta días-multa.

TITULO V
DELITOS CONTRA EL PATRIMONIO
CAPÍTULO I
HURTO

Artículo 186.

El agente será reprimido con pena privativa de la libertad no menor de tres ni mayor de seis años si el hurto es cometido:

1. En casa habitada.
2. Durante la noche.
3. Mediante destreza, escalamiento, destrucción o rotura de obstáculos.
4. Con ocasión de incendio, inundación, naufragio, calamidad pública o desgracia particular del agraviado.
5. Sobre los bienes muebles que formen el equipaje del viajero.
6. Mediante el Concurso de dos o más personas.

La pena será no menor de cuatro ni mayor de ocho años si el hurto es cometido:

1. por un agente que actúa en calidad de integrante de una organización destinada a perpetrar estos delitos.
2. sobre bienes de valor científico o que integren el patrimonio cultural de la Nación.
3. Mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general, o la violación del empleo de claves secretas.

CAPITULO IX
DAÑO

Artículo 205.

El que dañe, destruya o inutilice un bien, mueble o inmueble, total o parcialmente ajeno, será reprimido con pena privativa de libertad no mayor de dos años y con treinta a sesenta días multa.'[98]

Por lo que respecta a estos artículos, vamos a poder ver que el 154, nos va hablar en relación a los que nos interesa, que es la privacidad de las personas y nadie esta autorizado para violentarla, por ningún medio, de ser así será sancionado.

El Artículo 186, nos va tener en cuenta lo que es el hurto y el segundo párrafo en el punto numero tres va a tipificar el robo a través de medios electrónicos, y esto lo podemos encaminar a lo que son los delitos informáticos que nos pueden interesar para nuestra investigación.

Por lo que respecta a los Articulo 427 del citado Código, habla de la falsificación de documentos a los cuales no es directo a los documentos informáticos, pero puede interpretarse de tal manera que pudiera dirigirse a la falsificación de estos, no se lo

[98] Código Penal Peruano. http://www.leyes.congreso.gob.pe/Imagenes/Codigos. sábado 29 de noviembre de 2003, 15:00 PM.

Capítulo V
Propuesta
de
"Anexo al Artículo 71, en base a la fracción A, apartado V, de la Ley Federal de Telecomunicaciones."

considero relevante el citarlo por que no señala en si lo relevante a lo informático, pero puede dejar a la interpretación, lo que podríamos decir esta a interpretación.

Lo que podemos decir que el Artículo 205 de dicho Código es que lo encaminamos a el daño en los bienes personales y podemos interpretarlos a lo que es el daño del hardware y la pena que podría dar por el daño de estos bienes.

Capítulo V. Propuesta de "Anexo al Artículo 71 en base a la fracción A, Apartado V, de la Ley Federal de Telecomunicaciones."

5.1. Derecho a la Privacidad.

Como sabemos y tenemos entendido la privacidad es algo muy importante en nuestra vida los seres humano necesitan tener sus garantías así como tener todos nuestros derecho y uno de estos es el derecho a la privacidad, todos los ciudadanos debemos tener garantizado este derecho, La capacidad que se tiene en la red de información de Internet para que cada usuario de esta pueda colocar o subir en ella los contenidos o bien la información que este quiera, es tan amplia como también podemos decir que la posibilidad para que los mensajes que se envían a través de está red, así como de la misma forma la información personal que se almacena en los equipos de computo de los cuales cientos de usuarios no quiere que sea conocida por otros, esto puede ser la misma información personal, trabajos, de investigación, documentos personales, etc. En Nuestra Carta Magna, por obvias razones no vamos a encontrar nada en relación directa a nuestro tema, pero podemos citar el: *"ART: 16-nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, si no en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento"*[99]. Esto lo podemos interpretar de la manera de que los correos electrónicos, archivos o documentos de computadora, pueden ser aplicados a lo que señala nuestra Carta Marga, siendo así que de la misma forma estos documentos pueden ser robados copiados como ya hemos analizado, puedan ser vistos, como hemos visto otros usuarios se pueden infiltrar sin el consentimiento, este es un tema muy controversial como lo señalan los mismos usuarios de la red que nos dicen;

"La posibilidad de interferencia existe en prácticamente todos los medios de difusión. Pero las transgresiones a la privacia en la Internet han sido tan publicitadas que existe la sensación de que en ella todo el tráfico de mensajes, incluso el coreo electrónico, se encuentra constantemente abierto al escrutinio de mirones cibernéticos."[100]

Pero como usuarios de la Red de la Información de Internet podemos señalar que la privacidad absoluta no existe en Internet, ahora bien de la misma forma podemos citar los

[99] Constitución Política de los Estados Unidos mexicanos, 145a Edición. Editorial Porrúa. México, 2003.
[100] TREJO DELARBRE, Raúl. http://raultrejo.tripod.com/ensayosinternet/derechodelitosylibertades.htm, miércoles 26 de febrero de 2004, 13:30 PM.

sistemas de seguridad más sofisticados que especialistas han hecho, como por ejemplo en el empleo de claves y mensajes cifrados, tal ves son claves que para muchos no son importantes o no nos dicen nada pero estas claves o códigos pueden ser transgredidos y descifrados por especialistas en cibernética si así estos lo desean.

Ahí uno de los asuntos que no se han tratado en especial detalle ya que no es gran punto de este tema de investigación pero es necesario nombrar en un punto tan importante como es este de la privacidad, es exagerado hablar de que el ciberespacio o la Red Mundial de la Información es un amplio espacio el cual esta repleto de piratas informáticos dispuestos a violentar o bien a asaltar el primer correo electrónico que se les atraviesa cuando navegan, y es aquí algo que nos señala Raúl Trejo en su comentario que nos dice;

"Más que los hackers, la privacía en la Internet está amenazada por las grandes corporaciones que trafican con la información relativa a las preferencias y costumbres de los usuarios de la red de redes. Además, se sabe de la existencia de muy sofisticados sistemas patrocinados por los gobiernos de los países más poderosos para espiar los mensajes que transitan por el ciberespacio.

Recientemente, se ha confirmado la existencia de una vasta red de intercepción de mensajes patrocinada por los gobiernos de Estados Unidos, Canadá, el Reino Unido, Australia y Nueva Zelanda y con la contribución de Alemania y Japón. Gracias a un sistema de antenas satelitales instaladas en esos países y además en Italia y Turquía, entre otros sitios, se ha logrado una capacidad de intercepción capaz de reunir, y procesar, llamadas telefónicas, mensajes de correo electrónico, descargas de información en sitios en la WWW y transmisiones satelitales. A ese sistema de espionaje, se la ha llamado Echelon.

Algunos especialistas, consideran que Echelon tiene capacidad para interceptar 3 mil millones de comunicaciones todos los días. La información que recaba es analizada por sofisticados programas de inteligencia artificial en cuatro centros, ubicados en Estados Unidos (cerca de Denver), Inglaterra, Australia y Alemania. Se ha llegado a afirmar que Echelon tamiza el 90% de toda la información que circula por la Internet, en todo el mundo."[101]

Lo anterior nos esta señalando que los mismos Estados son los que están vigilando el movimiento de la Red de la Información, nos señala que estamos siendo vigilados para

[101] Idem.

ver saber que es lo que hacemos en esta, así como para saber en que tipo de páginas de Internet entramos, muchos podrían decir que es un medio de seguridad pero es también una violación a la privacidad. Por otro lado, no se hace gran mención de las empresas o industrias que trabajan por Internet las cuales saturan los equipos de computo con Spaw, que como ya hemos visto son una especie de publicidad que aparece en la pantalla sin que los usuarios lo hayan llamado, y es molesto que estos Spaw, saturen nuestros correos electrónicos, es otro medio por el cual se esta agrediendo a un usuario, el cual puede estar siendo bombardeado con información que ni pide y sobre todo si es información lasciva para este.

Por otro lado la red nos da otro tipo de información en el cual señala que medidas tomadas por países en contra de la delincuencia que nos dice;

> *"En otro asunto, en mayo de 2000 la cumbre mundial contra la delincuencia en la Internet del Grupo de los 8 que se reunió en París, aprobó 22 recomendaciones. Entre ellas, se encuentra la exigencia a compañías privadas de equipos de cómputo o proveedoras de acceso a la red para informar a sus respectivos gobiernos de los riesgos que adviertan a la seguridad en los sistemas informáticos. De esta manera, tales empresas se convertirían en informantes de agencias como el FBI estadounidense. Aunque se sugirieron medidas que tienden a reforzar la responsabilidad de los usuarios de la red, especialistas del grupo Privacy International consideraron que otras decisiones de la reunión en París, "reducirán la privacía en la Internet y no servirán para prevenir futuros ciberataques".*[102]

Lo anterior, es de cierta forma algo que apoya a los delitos Informáticos posiblemente depende del punto de vista con que se vea, pero esto no garantiza mucho, solo garantiza que los gobiernos se escuden para poder violentar la privacidad de los usuarios, esto podría ser que, con motivo de investigación podrán entrar en los equipos de manera clandestina, esto quiere decir que se estará justificando la violación a un equipo.

Una de los asuntos muy importantes en este tema es que en la Red de Internet se encontró a gente que son usuarios completamente similares a una persona común y corriente estos usuarios se encuentran conectados navegando buscando información o buscando a otros con intereses similares. Aquí lo que importa es "qué tipo de información están buscando" y "qué uso darán a dicha información", es aquí en donde se aplica la regla

---

[102] Idem.

de los Hakers que se encuentran navegando y viendo que información pueden encontrar, lo anterior nos dice que hay muchos navegantes anónimos;

"Debido a esto, muchas personas navegan de una forma que creen totalmente "anónima". No realizan compras por Internet, no dan información sobre su domicilio o intereses ni proporcionan algo que pueda comprometerlos o identificarlos aunque sea un poco. Evidentemente piensan que nadie se entera de lo que pueden estar realizando, las páginas que han visitado o las descargas realizadas.

Pero puede ser que estén equivocados. Muchas autoridades y organizaciones siempre han tenido la posibilidad de rastrear cualquier actividad realizada en Internet por cualquier persona común y corriente. Es posible conocer sus archivos, descargas, páginas visitadas y hasta sus conversaciones.

Esto ha ocurrido desde que empezó a utilizarse Internet de forma cotidiana pero se ha incrementado a raíz de lo que sucedió el 11 de septiembre del año pasado. Mucha de la comunicación para que se llevara a cabo este atentado de forma exitosa fue por medio de la red. Por eso ahora, con más razón se está rastreando y siguiendo a cualquier persona que pueda parecer sospechosa o que visite determinadas páginas (donde den datos para crear bombas por ejemplo."[103]

Lo anterior nos señala que el Internet puede ser una arma muy eficaz para poder controlar ataques grandes y con gran daño a una sociedad pero bueno estaríamos hablando de ataques muy contados, la mayor parte de los ataque y costos son invasiones pequeñas a Redes privadas o bien a los simples usuarios, que crean grandes costos en la Red Mundial. Ahora bien no podemos decir que con entrar a la Red de Información vamos a encontrar los problemas de seguridad en el primer momento que entremos a alguna página de Internet o bien cuando entras a un correo electrónico es decir los individuos que tiene como pasatiempo hakear y husmear en las maquinas de otros no están en todos los sitios, pero si frecuentemente escribes información personal en los mensajes de E-mail y Chat, seguramente alguien se aprovechará de esa información.

Ningún sitio puede transferir virus a tu disco duro automáticamente. Por el sólo hecho de revisar un mensaje de E-mail no le pasará nada en las computadoras. Sin embargo el acceder un attachment que no es más que un archivo adjunto en el correo, este archivo adjunto es como si a un domicilio llegara una carta y como complemento de esta carta

[103] IZA MARTÍNEZ, Paola. http://www.microasist.com.mx/noticias/internet/achin0703-2.shtml, miércoles, 12 de marzo de 2003, 1:25 PM.

llegara un paquete adicional, pero aquí lo aplicaríamos en el Internet, desde el E-mail, puede ser contraproducente en ciertas ocasiones. Para evitar esto, no abras attachments o archivos adjuntos si no se confía en el sitio que los envía o bien si se tiene duda de quien lo envía así como también si crees que pueda tener algún virus.

El Internet puede ser una fuente de información bastante extensa, educativa, entretenida así como también ociosa, pero también hay mucho contenido que no es recomendable que exploren, sobre todo si, se desconoce el contenido de las paginas o bien si no se tiene idea de que hacer en caso de entrara a una pagina la cual va a bombardear nuestra maquina con los famosos Spaw.

El Internet es una herramienta la cual se esta acoplando a la tecnología actual, muchas personas ven en la Red de la Información de Internet un modelo de cómo tendrán lugar los negocios en el futuro. Sin embargo, antes de que eso pueda ocurrir, los usuarios frecuentes tienen que sentirse seguros sobre el hecho de enviar números de tarjetas de crédito y otras informaciones financieras a través de la red. Ya que la información enviada a través de Internet como hemos visto anteriormente el Internet es una Red extensa de computadoras y por ende, la información que los usuarios transmiten pasa por muchas computadoras a lo largo de su camino, existe la posibilidad de que alguien pueda estar curioseando y robe información confidencial.

Pero de la misma forma, podemos no estar siendo objeto de espionaje por un Hacker, sino también como lo hemos visto anteriormente, podemos ser objeto de espionaje por autoridades o bien por organizaciones quienes cuentan con la posibilidad de rastrear cualquiera de las actividades que se realicen en la Red de Internet.

5.2. Centinelas Protección y sus Costos.

El poder hablar de Centinelas, es el tratar de hablar de atender de manera eficiente la seguridad de una red la cual es cada vez más difícil. A pesar de que las herramientas se mejoran día a día, los hackers también aumentan su nivel de conocimientos técnicos así como también se hacen más astutos en su ramo. En general y a raíz de todo esto, las empresas, las organizaciones y organismos tanto gubernamentales tienen muy concientes los riesgos y a razón de esto permanentemente tratan de aumentar los niveles de protección a sus empresas o instituciones.

5.2.1. La Inversión en el uso del Internet por los Usuarios.

En relación a los costos para la protección de los equipos de cómputo son diferentes tipos de herramientas de protección las cuales se están haciendo accesibles para todos, las cuales se pueden bajar algunos sin costo alguno en la mis a Red de Información de Internet, pero también si se requiere de algún sistema de seguridad mas sofisticado o que no sea común en la Red de información de Internet, se tiene que adquirir a empresas dedicadas a ello, en general, para todos los usuarios de esta, desde un simple usuario casero hasta para las organizaciones más pequeñas, mediana, grandes y las multinacionales más grandes. Esto hace que la implementación de mecanismos y sistemas de seguridad se de prácticamente en todos los niveles. Todas pueden acceder a las herramientas que necesitan y los costos a los que se adapte cada usuario, es decir, la inversión que cada empresa debe realizar va de acuerdo con la empresa y sus necesidades.

Pero no es sólo cuestione de costos, es también cuestión de de cultura y tecnología, como nos lo dicen en la Red, entre mas aumenta la tecnología aumentan los individuos que quieren superarla, como podemos ver en e cometario que nos dice; *"Pero no es sólo una cuestión de costos, Los constantes cambios de la tecnología hacen que para mantener un nivel parejo de seguridad cada empresa deba actualizar permanentemente las herramientas con las que cuenta. Como los hackers mejoran sus armas y metodologías de penetración de forma incesante, el recambio y la revisión constantes en los mecanismos de seguridad se convierten en imprescindibles. Y éste es un verdadero punto crítico".*[104]

Pero podemos hablar en este tema de los tipos de Centinelas que se tiene en México, Las oficinas de la policía cibernética mexicana, unidad de la Policía Federal Preventiva (PFP), cuentan con bastante actividad. En un moderno edificio situado en el sur de la ciudad de México, en sus oficinas especiales las cuales están dotadas de sofisticados y poderosos equipos de cómputo, los centinelas o policías del ciberespacio, patrullan la supercarretera de la Red de la Información de Internet con el objetivo de detectar y prevenir aquellos delitos que se cometen a través de Internet, en particular los ataques que afectan a las instituciones y a sector más vulnerable de la población, en general su especialidad es la detección de material pornográfico infantil y tratar de sacar de Internet este tipo de paginas.

---

[104] http://www.monografias.com/trabajos/hackers/hackers.shtml, miércoles 12 de marzo de 2003, 12:00 PM.

En México la policía Cibernética o Centinelas no tiene mucho de su creación fue creada en base a las necesidades que cada día se fueron haciendo mas recurrentes, de que habían violación, virus, pornografía, y alas exigencias de países que luchaban en contra de este tipo de delitos; *"La policía cibernética, dependiente de la Coordinación de Inteligencia para la Prevención, fue creada en 2000 para responder al fenómeno de la red y las nuevas formas de convivencia social surgidas en el ciberespacio, así como a los delitos novedosos originados en ese ámbito o propagados a través de él. Autoridades policiales de todo el mundo se han visto en la necesidad de ajustar y modificar las leyes y los procedimientos para prevenir, combatir y perseguir los ilícitos que se cometen en la red de redes: fraudes, intrusiones ilegales en sitios privados, y delitos del crimen organizado como la pornografía infantil, el tráfico de personas y de drogas, entre otros. La policía cibernética tiene que enfrentarse a muchos obstáculos para realizar su labor. En entrevista con CIBERSIVO, el coordinador de Inteligencia para la Prevención del Delito de la PFP, Nicolás Suárez Valenzuela, reconoce que la delincuencia siempre le lleva la delantera a las autoridades policiales. "Lo tecnológico cambia cada año, las leyes, cada 20 años", señala. En este sentido, explica que en la ley todavía no hay una tipificación de delitos como la pornografía infantil en Internet y lamentó que lo jurídico no evolucione a la misma velocidad que la tecnología".*[105]

Cantidad de veces, los delincuentes cibernéticos logran escapar aún cuando existen elementos sólidos para proceder en su contra, el problema que tiene la policía Cibernética es que por lo regular los delitos informáticos no son denunciados y esto nos dice que. Si ya no hay víctima o afectados, tampoco hay quien señale a los delincuentes. Lo que se requiere para este caso es que se deben denunciar y hacer valor lo derechos y se debe de sostener la denuncia hasta el final para hacer pagar los daños a los infractores. Para poder hacer esto también se requiere de educación y cultura de seguridad.

En la página de Internet de la Policía Federal Preventiva podemos encontrar información en relación a estos caso y además una gran explicación de sus logros u actividades;

> *"Un boletín de la PFP explica que entre las funciones de la oficina de la Policía Cibernética y Delitos contra Menores están promover esa cultura de la*

[105] http://portal.uaq.mx/seguridad/PFP-policia-cibernetica-entrevista-de-Nicolas-Suarez-Valenzuela.html, lunes 03 de noviembre de 2003, 20:03 PM:

seguridad, fomentar la denuncia anónima y realizar campañas de información sobre los delitos cibernéticos.

Además realiza operaciones "de patrullaje anti-hacker, detecciones de delincuentes que cometen fraudes, penetran en sitios privados y organizan sus actividades delictivas utilizando Internet".

También lleva a cabo operaciones en la red para detectar sitios de pornografía infantil y aquellos en los que un menor pueda ser contactado por pederastas.

La policía cibernética organiza y promueve la investigación de campo sobre las redes de pornografía infantil, en particular, y desarrolla "una base de datos para la identificación de patrones, rangos, preferencias y modus operandi de los protagonistas de los casos reportados".

Desde su creación, la policía cibernética ha tenido logros destacados. Recientemente, el director general de Tráfico y Contrabando de la PFP, Hervé Hurtado, dio a conocer que hasta la fecha, se han identificado plenamente 28 sitios de pornografía infantil, dos de venta de armas, 16 de clonación de tarjetas de crédito, tres de inhibición de exámenes toxicológicos y 36 comunidades de hackers.

Agregó que se ha desarticulado a 200 de las 257 comunidades mexicanas en Internet que intercambian material de pornografía infantil.

En uno de los casos destacados, en septiembre de 2000, la policía cibernética identificó y desarticuló la organización de abuso sexual a niños más extendida de México, que operaba desde Acapulco. Se expulsó del país a Robert Decker, ciudadano estadounidense que, según las evidencias, dirigía dicha organización.

En el caso de Decker, la policía cibernética colaboró con autoridades policiales de Estados Unidos, lo que revela la importancia de la colaboración internacional para perseguir esta clase de delitos...

Este cuerpo policial ha aprendido a sortear parte de los obstáculos con los que se topa en sus investigaciones. Uno de éstos es la falta de colaboración de proveedores de Internet como la empresa Uninet (filial de Telmex), que en un caso sostuvo como argumento que la PFP no contaba con facultades legales para obligarla a revelar los datos de sus clientes."[106]

El trabajo de esta policía especial es investigar navegar cuidar lo que se publica en ella, y sacar de está lo que consideran que no dañino para los navegantes así como detectar

[106] http://portal.uaq.mx/seguridad/PFP-policia-cibernetica-entrevista-de-Nicolas-Suarez-Valenzuela.html, lunes 03 de noviembre de 2003, 20:03 PM:

a los Hackers, lo que la PFP, nos dice es que es un trabajo difícil pare a fin de cuentas pueden encontrar elementos suficientes para poder rastrear a los delincuentes y así consignarlos, estos Centinelas con la nueva policía en una nueva colonia.

5.2.2. Costos de Protección en Internet.

Los costos de las diferentes sistemas y herramientas de protección se están haciendo accesibles, en general, incluso para las organizaciones más pequeñas las cuales las podemos encontrar en la misma Red de la Información de Internet, las cuales en muchos de los casos pueden ser hasta gratis, pero estos pueden ser muy vulnerables, estos mecanismos de seguridad se dé prácticamente en todos los niveles. Empresas grandes, medianas, chicas y las multinacionales más grandes, así también a los gubernamentales, y hasta los mismos usuarios comunes que navegan sin dolo alguno en la Red. Todos los usuarios pueden acceder a las herramientas que necesitan y hablar de los costos dependerá de la inversión que cada empresa debe realizar o bien de cada usuario común que navega en la Red, estos medios de protección van de acuerdo con las necesidades. De la misma manera el hablar sobre la Seguridad en Internet, tenemos que hablar también no solamente de los externos sino también hay que hacer mención al gran índice de inseguridad interna de la infraestructura informática de las empresas, ya que en muchas de las ocasiones van desde la misma piratería en las empresas, por ese lado, y externo por los sujetos que ya hemos visto anteriormente que tratan de hacer algún daño en la Red de Información de Internet.

Los costos que produce el proteger así como los daños que se producen son gastos que no deberían realizarse, la vulnerabilidad de la información transferida por la Internet y la facilidad de ataques externos e internos que se traducen en pérdidas que ascienden hasta miles de dólares en términos de información alterada, robada o perdida.

Como podemos ver los costos de perdidas y daños son muy altos; *"Los ataques a maquinas conectadas a Internet se incrementaron en un 260% desde 1994, se calcula una perdida de 1.290 millones de dólares anuales solo en los EEUU"*[107]

Según los estudios hechos en Internet las estadísticas están de la siguiente manera; *"Según una investigación realizada en 1700 empresas por la empresa, el 75 por ciento de estas han tenido algún problema de seguridad. De éstas el 40 por ciento ha enfrentado*

[107] http://www.ati.es/DOCS/internet/histint/histint1.html#conceptos, Viernes 17 de octubre de 2003. 14:00 PM.

problemas de seguridad debido a la falta de apoyo de la alta dirección para invertir en medidas y herramientas de seguridad y sólo el 38 por ciento se debió a la falta de herramientas adecuadas. Más que un problema de tecnología, la seguridad en la transmisión de la información por la Red se debe a la falta de cultura de las organizaciones y de las personas que la integran. El eslabón más débil de esta cadena en la seguridad la constituye el humano y no el tecnológico, lo cual destaca la importancia de tener una cultura de seguridad, porque no existe en muchas empresas un responsable de la seguridad."[108]

Estas empresas encargadas de la seguridad son en ocasiones demasiado caras, en la Red de la Información de Internet, podemos encontrar aun así manuales de Hackers, tal vez deberían los usuarios de aprender a responder a esas agresiones pero ese no es el caso, hay que empezar a abrirnos a la nueva cultura de Informática, para aprender a denunciar y defendernos de estas agresiones, ya que como podemos ver en los comentarios de la Red que nos dice que ;*"Hoy es imposible hablar de un sistema ciento por ciento seguro, sencillamente porque el costo de la seguridad total es muy alto. "Por eso las empresas, en general, asumen riesgos: deben optar entre perder un negocio o arriesgarse a ser hackeadas. La cuestión es que, en algunas organizaciones puntuales, tener un sistema de seguridad muy acotado les impediría hacer más negocios", "Si un hacker quiere gastar cien mil dólares en equipos para descifrar un sistema de claves de acceso, lo puede hacer porque es imposible de controlarlo. Y en tratar de evitarlo se podrían gastar millones de dólares".*[109]

Para entrar en una estadística de gastos o como podremos decir una guerra de gastos, tanto en usuarios a nivel empresas como usuarios comunes, hay que acercarnos a las leyes y denunciar como lo señala la policía especial de la Policía Federal Preventiva.

---

[108] http://www.monografias.com/trabajos/hackers/hackers.shtml, miércoles 12 de marzo de 2003, 12:00 PM.
[109] Idem.

5.3. Tipos de Delitos Cibernéticos en Relación a la Violación de la Privacidad.

El tema esencial de este tema de estudio es la Violación de la Privacidad a la cual están sujetos todos los usuarios de la Red de la Información de Internet, como hemos visto es uno de los temas mas discutidos por todas las partes interesadas, antes de poder mencionar los delitos cabe hacer mención y recordar brevemente lo que es el tema mas discutido, el cual es, Un virus que como ya no es necesario mencionar ampliamente solo que es un programa de computo que puede ingresar a los sistema computacionales a través de cualquiera de los métodos de acceso de información externa que ya hemos visto, se instala, se reproduce y causa daños estos sistemas, los cuales son en varias ocasiones de gran gravedad en materia de economía, además de que la gravedad de los virus son muy variables, como es que va desde una simplemente una molestia en la pantalla, como el caso del "ping-pong" que ya hemos visto anteriormente, hasta aquellos virus que pueden llegar a eliminar el contenido de una base de datos, programas y archivos que pueden ser importantes para los afectados.

Todo este tema de los virus de la mima manera es un tema muy controversial, hay publicaciones que hacen análisis del mismo origen de los virus; "*Actualmente existe una gran carrera entre aquellos que crean los virus y los que desarrollan los antivirus. Hasta ha llegado a decirse que los virus son desarrollados por los mismos productores de antivirus, ya que hoy en día es fundamental adquirir antivirus y los mismos deben ser renovados constantemente, por supuesto que no existe ninguna prueba concreta.*"[110]

Lo anterior es una publicación en base a que los mismos creadores de los antivirus son los que mandan los virus para hacer aun más extensas sus ventas, pero en base a esta investigación, no hay bases que puedas sustentar este comentario, ya que en capítulos anteriores, se ven los tipos de delincuentes informáticos, y estos no siempre son trabajadores de sistemas computacionales, hay varios que solo hacen un virus por experimentar, a continuación, veremos los tipos de actos hechos por estos delincuentes los cuales van a ser considerados como delitos en razón a la privacidad de los usuarios.

[110] VIEGA RODRÍGUEZ, María José. Delitos Informáticos, http://derecho.org/comunidad/mjviega/deli_inf.htm. miércoles 01 de octubre de 2003, 14:00 PM.

5.3.1 Gusanos.

Este es uno de los que esta considerado como lo vimos en lo que es un virus informático, pero, aquí es donde entra una des sus actividades esenciales como virus así como, una herramienta básica para los Hackes, tiene su creación e incubación, de la misma forma a los virus comunes que hemos visto, y recordando un poco de su actividad es; *"se infiltra en los programas ya sea para modificar o destruir los datos, pero se diferencia de los virus porque no pueden regenerarse. Las consecuencias del ataque de un gusano pueden ser graves, por ejemplo un programa gusano puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita y luego se destruirá."*[111]

Esta herramienta es muy básica para una persona que se dedica a robar números confidenciales, así como se encarga de mandar información, de datos y transferencia de dinero a cuentas, si este gusano no es localizado a tiempo puede causar grandes daños económicos.

5.3.2. Sabotaje Informático.

Este tipo de actividad, es la más frecuente por los Hackers, cualquiera desde las grandes empresas hasta los usuarios comunes que navegan inocentemente en la Red de la Información, están expuestos a este tipo de actividad y daño, el sabotaje informático es una actividad de la cual muchos de los Hackes, hacen alarde de esta actividad, muchas de las ocasiones, los saboteadores, comienzan con mandar mensajes a el usuario el cual están saboteando y husmeando en los equipos informáticos, pueden ser mensajes ofensivos o simples mensajes de amenaza, también tiene su actividad en borrar, suprimir o modificar sin autorización del usuario dueño de la información, así como en inhabilitar funciones o datos de computadora con la simple intención de obstaculizar el funcionamiento normal del sistema de cómputo o simplemente por borrar y hacer maldad a determinado usuario.

[111] Idem.

5.3.3. Acceso no Autorizado a Sistemas o Servicios.

En esta actividad no hay daños a los equipos informáticos, ni mucho menos borrar datos, es una actividad que es simplemente para revisar la información de otro usuario o empresa; *"Puede darse por motivos diferentes: desde la simple curiosidad, como en el caso de muchos piratas informáticos (Hacker) hasta el sabotaje o espionaje informático. Estos ingresos no autorizados comprometen la integridad y la confidencialidad de los datos. Podríamos llegar hasta actos de atentados terroristas, por ejemplo en el caso de intervenir sistemas de tráfico aéreo."*[112]

Esta actividad es usada por lo que roban la información para mas actividades como para venderla a los mejores postores a interesados en información confidencial de competencias en relación a las grandes empresas, así como podría ser que algunos gobiernos se valgan de esta actividad para hacer espionaje a otros, o bien a empresas objeto de investigación, siendo que esta actividad es ilícita, en conclusión el objetivo primordial de esta actividad es el posible lucro por esa información.

5.3.4. Espionaje Industrial y Fuga de Datos.

En esta modalidad de espionaje, el acceso se puede darse en una forma directa, por ejemplo se da en los casos de empresas cuando un empleado accede en forma no autorizada, a un sistema informativo, estamos frente a un riesgo interno. Pero se puede acceder en forma indirecta, esto es cuando se accede a través de una forma externa, esta modalidad como se ve es en las pequeñas y grandes empresas. Ya que el autor de este espionaje es casi siempre una persona la cual tiene acceso directo o indirectamente a la información confidencial.

"El delincuente puede aprovechar la falta de medidas de seguridad para obtener acceso o puede descubrirle las deficiencias a las medidas existentes de seguridad. A menudo, los hackers se hacen pasar por usuarios legítimos del sistema, esto suele suceder debido a la frecuencia en que los usuarios utilizan contraseñas comunes."[113]

La fuga de datos e información confidencial consiste es la versión informática de lo que conocemos tradicionalmente como prácticas de el espionaje industrial.

---

[112] Idem

[113] http://www.informador.com.mx/informa/depa/informatica/secciones/internet.html, lunes 03 de noviembre de 2003, 20:03 PM.

Los autores de este espionaje industrial crean accesos a los sistemas a través de códigos de acceso robados, o bien los copian para crear una puerta alterna desde su lugar de trabajo, y trabajar cómodamente,

De la misma manera utilizan un método llamado llave maestra; *"Consiste en el uso no autorizado de programas para modificar, destruir, copiar, insertar, utilizar o impedir el uso de datos archivados en un sistema informático. El nombre proviene de un programa de utilidad, que permite abrir cualquier archivo de una computadora aunque se halle protegido por medidas de seguridad."*[114]

Otra de las modalidades para crear el espionaje industrial es; *"Pinchado de líneas. Se realiza a través de la interferencia de las líneas telefónicas o telemáticas a través de las cuales se transmiten las informaciones procesadas en las bases de datos informáticas."*[115]

Este método es similar a que el espía tiene equipo especial para conectarlo a la línea telefónica, este equipo especial, va a interceptar la información de los equipos en los cuales se tiene la información confidencial y la roba automáticamente.

5.4. Propuesta de "Anexo al Artículo 71 en base a la fracción A, Apartado V, de la Ley Federal de Telecomunicaciones."

ARTICULO 71.- las infracciones a lo dispuesto en esta Ley, se sancionará por la Secretaría de conformidad con lo siguiente:

A. Con multa de 10,000 a 100,000 salarios mínimos por:

I. Prestar servicios de telecomunicaciones sin contar con concesión por, parte de la Secretaría;

II. No cumplir con las obligaciones en materia de operación e interconexión de redes públicas de telecomunicaciones;

III. Ejecutar actos que impidan la actuación de otros concesionarios o permisionarios con derecho a ello;

IV. No llevar contabilidad separada por servicios de acuerdo a las disposiciones de esta Ley o sus reglamentos, y

V. Interceptar información que se transmita por las redes públicas de telecomunicaciones.

---

[114] Idem.
[115] Idem.

Luego entonces, en este caso y tomando como referencia, anterior artículo, es posible buscar la necesidad de la reparación del daño pecuniariamente, por lo que, la siguiente propuesta y comentario en referencia, que daría una solución al problema.

A). Se considerará acto doloso al que en forma intencional, sin debida autorización o abusando de está, intercepte, interfiriera, reciba, use, altere, daña o destruya, un sistema o red de computadoras, programa de software o base de datos, en todo o en parte, independientemente del usuario al que se haya dañado, se le impondrá multa y reposición de daños.

B). Si el daño fue creado con el afán de lucro o beneficio propio o de terceros, así como si el infractor robara información sensible para el propietario, que tenga que ver con su intimidad, de la misma manera, se agravara la multa si este infractor es servidor publico;

En estos dos apartados se va a vigilar por la propiedad, así como también por la privacidad de los usuarios de la Red de la Información de Internet, que es distribuida en su general y obviamente por más barato a través de las líneas telefónicas y aun así siendo por otro medio le corresponde a las comunicaciones. Aquí como se especifica, se esta actuando de forma dolosa, ya que un usuario que tenga el conocimiento para realizar este tipo de actividades es obvio que es una persona que actúa con pleno conocimiento al realizar las actividades que ya se mencionaron como son; interceptar, recibir, usar, alterar o destruir. Sería importante establecer agravantes en la multa y en la destitución de funciones, al tener la calidad de funcionario público. También aquí se debe de tomar en cuneta la privacidad de los individuos siendo que a quien difunde o revela a terceros los datos obtenidos, y aun más cuando la violación de la intimidad personal, tenga por objeto datos personales sensibles que perjudiquen al afectado siendo por, cuestiones de ideologías, religión, sexuales, raciales.

C) Se tomara de Forma culposa, aquel usuario que por no prever un resultado, sin la debida autorización o excediendo la misma, acceda, intercepte, interfiera, altere dañe o destruya un sistema computo o red de computadoras, programa de software, o base de datos en todos sus aspectos, total o parcial.

En este apartado anterior va a proteger de la misma manera la propiedad y la privacidad, ya que se incrimina a título de culpa, por no prever un resultado previsible, debido a la negligencia, imprudencia, impericia o por desobedecer las leyes o reglamento.

D) Fraude informático. El que con intención de procurarse a sí mismo o a un tercero un beneficio patrimonial mal habido, y causando un perjuicio en el patrimonio de otro, operando un proceso de datos incorrectamente a su favor, configurando incorrectamente un programa de software en beneficio propio, empleando dolosamente datos falsos, incorrectos o incompletos, o a través de cualquier otra forma o manipulación ilegítima, sin la autorización o excediendo la misma.

Este apartado trata de proteger de la misma forma el patrimonio, tratando de prever la estafa, el lucro en el ámbito informático y de secretos Industriales y personales.

E) Hurto informático. Se considerará hurto informático a aquel usuario que utilizando un sistema de computación o software adecuado, sin autorización, o excediendo está, se apoderare de valores intangibles o incorporales ajenos, como puede ser depósitos monetarios, transferencias electrónicas de fondos, créditos, información y/o secretos industriales o comerciales, sustrayéndoselos a su tenedor, para aprovecharlos para si o terceros.

Este apartado tutela el patrimonio y la propiedad, tratando de abarcar el hurto común a un nuevo tipo de bien, que es el bien informático, el cual esta de novedad.

F) Actuara de forma dolosa aquel que empleando los medios de comunicación, como son; el correo, el teléfono, el fax, las fibras ópticas, la Red de Información de Internet a través del E-mail, u otro medio de comunicación o telecomunicación similar existente, se procurare para sí mismo o a un tercero un beneficio patrimonial indebido, ya sea a través del fraude, el hurto, la malversación de fondos, el soborno, el sabotaje, el espionaje, la conspiración, la extorsión, la difusión de material pornográfico, del ataque a la propiedad privada y el derecho a la privacidad de las personas, el terrorismo, y otras figuras delictivas similares existentes o por crearse.

Este apartado pretende tener como función evitar que los medios de comunicación sean utilizados con fines dolosos e ilícitos. Cave destacar que este apartado no solo los medios existentes, sino también los que se puedan crear con la actividad de los avances tecnológicos de nuestros tiempos.

G) Se constituye como una agravante el hecho de que los delitos previstos en la presente ley sean cometidos por funcionario público en ejercicio de sus

funciones, o que el objeto del delito recaiga sobre sistemas de computación, software o soportes lógicos de cualquier entidad estatal, y se someterán a las leyes respectivas. De la misma forma en todos apartados de este artículo se incluye la reposición de daños y trabajo social si así lo amerita, la autoridad.

Este apartado, trata de abarcar a los funcionarios públicos en ejercicio de sus funciones que traten de causar algún daño culposo o doloso a los sistemas federales y estatales, solicita la reposición de daño en todos los casos, y de la misma forma trata de que los agresores puedan realizar una especie de servició social, con horas de trabajo a la comunidad, realizando enseñanza en base a trabajando de lo que estos individuos tiene en mejor conocimientos ya sean clases o asesorando a la misma autoridad en sistemas de computo de el dañado, para que estos agresores, enseñen a la misma autoridad sus tácticas de trabajo, y tener de su parte el conocimiento de estos, esta sería un castigo optativo, serviría para tratar de no condenar a sujetos a una prisión, en la cual sólo aprenderían a delinquir más, dejando a un lado la pena privativa de la libertad, y dejando la opción del pago del daño, y que el mismo Estado aproveche dichos conocimientos.

Las presentes propuestas, tratan de llevar a las leyes de las comunicaciones a tratar de actualizarse en cuestiones de tecnología, la cual cada día esta siendo más alta, así como en tratar de llevar a los delincuentes informáticos a tratar de obtener una cultura de respeto por los demás y por las instituciones que nos crean como sociedad.

Conclusión.

Primera. En conclusión el primer capítulo. La importancia de que nuestra sociedad debe de tomar en cuenta, es que todas las personas que son usuarios del sistema de Internet, deben de tener por lo menos conocimientos básicos sobre los conceptos más importantes que se manejan en la Red de la Información de Internet. Podemos empezar por señalar que en este tema de estudios fue un tema muy importante el hablar de la palabra Informática; la cual como lo resaltamos en el capítulo primero, esta palabra tiene su origen en Francia, la cual nos dice que; Informática es simplemente el almacenamiento de la información autentica. Es entonces que la informática es el almacenamiento real de determinada información a una base de datos, esta información se obtiene, como hemos visto durante este tema de estudios por medio de determinado lenguaje que ha ido evolucionando a través de la creación de la computación e informática y de este punto, se desprende el análisis de la palabra informática, la cual es uno de muchos conceptos que se deben de conocer como básicos, y a su vez, esta palabra va concatenada con las telecomunicaciones ya que el desarrollo y evolución de nuestras vidas, nos lleva a relacionar esta palabra con las telecomunicaciones, a través de la Red de Información de Internet, ya que la informática, computadoras, servicios de suministro de Internet y obviamente a través de de la cual se suministra este servicio, las cuales son, las líneas de comunicación, reguladas por las telecomunicaciones. Debido a esto, el mundo esta sufriendo y resintiendo cambios económicos, políticos, sociales culturales y en relación a la regulación de leyes en todo el mundo, la informática a través de la tecnología esta tomando una gran fuerza, aunque no la podamos percibir físicamente, podemos concluir que la informática esta presente en todas las partes del mundo, a un en los países menos desarrollados y de la misma forma por obvia razón en todos los puntos de nuestras vidas

Segunda. La relación que hay con la Informática y la Red de la Información de Internet es que, gracias a la existencia de la primera, existe la segunda, es decir, gracias a todos el conocimiento almacenado en la Red de Información de Internet, se emplea la informática, y gracias a esto se crearon servidores o buscadores de información, los cuales dan el acceso al mundo de la información como por ejemplo; MSN, YAHOO y otros más, los cuales son parte de nuestra vida cotidiana, a través de estos buscadores y gracias a el Internet se puede obtener información de viajes, compras, Chat o foros de discusión,

conocer en relación de noticias, poder conocer cuestiones de información científica y laborales, satisfacer curiosidad y muchas más actividades en el sistema de Internet, según las necesidades de cada persona o el llamado usuario. La Red Mundial de Información, o Internet, como lo hemos visto en esta investigación, es simplemente un conjunto de computadoras interconectadas entre sí, esto es a nivel mundial, la red de Internet es un grupo de ordenadores conectados entre ellos, y así conectadas a computadoras de diversos países. Esta información nos lleva a la conclusión de que este desarrollo de información y tecnología, trae consigo conceptos nuevos, empleados por los usuarios comunes de este sistema de Información, como son la Cibernética que por mera mención ya antes visto en el capítulo uno es la ciencia encargada de los sistemas de control y de comunicación en las personas y en las máquinas, estudiando y aprovechando todos sus aspectos y mecanismos comunes. Además la Cibernética va a ser la unión de ciencias como la mecánica, electrónica, medicina, física, química y computación, y gracias a esta unión se creo la inteligencia artificial, la cual esta tomando gran en puje actualmente, por ejemplo; los autos ya tienen computadoras inteligentes, las lavadoras, toman el peso automático de la ropa a lavar, los edificios que se abren y cierran solos, etc. Podemos concluir que la informática y la Internet, traen consigo el nacimiento de nuevas ciencias y nuevos descubrimientos, mezclando también a la robótica y nuevos equipos computarizados que requieren de estos conceptos para crearse, y crear máquina especialmente diseñada para trabajos que faciliten la vida y menos desgaste del hombre, hay que señalar que durante el desarrollo de la humanidad y durante estos últimos años existe un gran desarrollo en la inteligencia artificial, que requiere aplicaciones de la cibernética aplicada a la informática y por que no, con el apoyo de la robótica para la creación de supercomputadoras con capacidad de ser programada para mejorar la vida del hombre y de su trabajo.

Tercera. Podemos concluir de la misma manera que el capítulo uno nos habla y dice que a raíz de la creación de este importante sistema de Información que es el Internet, obviamente, va a darnos un medios de expresión, el cual no es más que un Ciberespacio algo virtual, algo que no se puede tocar pero se puede ver, se puede captar el espacio que nos da Internet, pero también, el Internet, van a estar presentes las personas que lo usan y lo hacen parte de su vida diaria, ó sea; después de la creación del Internet, y los Ciberespacios, este medio dio la creación de Cibernavegante, los cuales son los usuario de Internet, son aquellas personas las cuales entran a la Red de la Información en Internet para así formar

parte de ella, y crear una Cibersociedad, que en conclusión, si vemos con detenimiento es una cadena de objetos y sujetos, para que en base a esto se cree un gran medio de Información. El cual es una gran herramienta para la humanidad, quien lo utilice teniendo grandes ampliaciones de información, consulta y de la misma forma tiene otros medios de esparcimiento y distracción. Hacemos mención de por lo que respecta a su funcionamiento del Internet, es que este esta formado por redes que tiene su propia directriz, esto es que no tiene una regla directa que las ordene, pero tampoco lleva un desorden, por sí misma esta ordenada, requiere una mínima organización para que pueda subsistir, en conclusión es una herramienta que existe por si misma establece una serie de normas propias para su orden y para los usuarios.

Cuarta. En el capítulo uno nos va a señalar que es un delito, que ley va a hacer su definición, pero de la misma forma vimos lo que son los Delitos Informáticos, que también se desprenden de el genero de delito, haciendo un cometario general los delitos son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, pero anexando a la Informática, es lo anterior más señalar a el uso indebido de cualquier medio informático, durante este tema de estudio de la misma forma señalamos que los Virus Informáticos son susceptibles de ser Delitos Informáticos, ya que desgraciadamente durante la historia el hombre a sido blanco de los virus que causan las enfermedades, durante décadas lucharon contra estos, creando medicamentos, métodos para poder evitarlos y protegerse de ellos, evolucionando de tal manera que se han creado medicamentos que pueden ayudar a la salud del hombre, para así hacerlo más inmune a tales ataques. Pero los virus no sólo se quedaron en enfermedades sino que también son ahora enfermedades de las máquinas o equipos de computo, se hizo la mención de los tipos de virus y de los Delitos Informáticos, haciendo la conclusión de este tema en que los delitos están ahora más haya de lo tangible y real, ahora esta en lo virtual. Este tema da una conclusión de que a raíz de el nacimiento de la nueva tecnología, el Internet, los usuarios, también nacieron nuevos delitos, y nuevos conceptos, y como todo, los que usan el sistema de la Red de Internet, se debería de tener por lo menos un conocimiento básico de los conceptos más usados en este medio, ya que hay demasiados, como lo apreciamos en el capitulo primero.

Quinta. En conclusión en el segundo capítulo de este tema de estudios, México, en relación a las telecomunicaciones, es un tópico el cual a ido avanzando con lentitud, en relación a este tema y a el resultado de su estudio la comparación que se puede hacer en

Latinoamérica la telefonía básica en México, es de lo más alto en costo para los usuarios, hablar te comunicación en México es hablar del monopolio que se puede señalar que actualmente no es un monopolio pero aun así como si lo fuera, ya que en México las telecomunicaciones continúan en manos de unos pocos, y de la misma forma la mayoría de usuarios la tiene Telmex y es la que rige los costos, hasta nuestros días es servicio a mejorado con el paso del tiempo pero aún hay mucho que hacer por parte de las grandes empresas para mejorar sus servicios, tanto en telefonía local como en telefonía móvil.

Sexta. Se puede concluir que en nuestro mundo se están viviendo cambios muy drásticos en cuanto a la sociedad actual, se desarrollo una gran evolución en la tecnología de las comunicaciones, como es el desarrollo de las computadoras, y que gracias a esto, nos están acercando a los lugares más apartadas del mundo, la evolución de las máquinas las cuales fueron desde los simple ábacos, que se pudieron apreciar durante el desarrollo de del capítulo dos, gracias a la gente que se preocupo por los cambios en la cibernética y la informáticas a el desarrollo que llevo muchos años de evolución, la cual llevo a una marcha directa a la computalización acelerada en el mundo, y que en relación a este desarrollo de la tecnología en general, nos estamos encarrilando a una sociedad electrónica, apoyada así como también por que no controlada por las computadoras. Los quipos de computo son una herramienta que actualmente y en el futuro nos ofrecerá muchas características que nos va a ahorrar tiempo dinero y esfuerzo en todas las actividades, y esto es gracias a su evolución y al desarrollo de las generaciones de computadoras, que gracias a sus creadores podemos encontrar en el mercado actual diferentes tipos de estas que van desde una computadora de uso común casera hasta una súper computadora, junto al desarrollo de la Red de Internet, esta conclusión, nos llevar a entender que necesitamos actualizarnos en lo personal en el manejo y uso de las computadoras para no quedarnos rezagados en conocimientos y tecnología que apoyan a nuestra sociedad para mejora y facilitar la vida cotidiana.

Séptima. Concluyendo que todo el gran desarrollo que hay en la actualidad en cuestión de informática se debe a el descubrimiento de el Internet, que surgió, hace más de veinticinco años, a raíz de un proyecto militar en el cual se desarrollo durante la guerra fría entre los Estados Unidos de Norteamérica y la Unión Soviética, esto fue a fines de los años sesentas, durante el año de 1969 el Departamento de Defensa de este país, pudo percatarse que durante este período los sistemas de comunicación era muy vulnerable, ya que se

detectaba que la Unión Soviética podía realizar interferencias a las comunicaciones del país y realizar espionaje, durante este período los equipos militares se dieron a la tarea de poder desarrollar un sistema en el cual pudiera ser más difícil o bien no poder descifrar las comunicaciones que se tenían internamente entre dirigentes y militares. Este fue un sistema el cual tal vez no se pensaba que durante el paso de los años llegaría a ser parte de la vida de los seres humanos conectados a la tecnología, este fue un sistema pensado para los militares y para el gobiernos, y ahora en día todos podemos tener acceso a la Red de la Comunicación de Internet, y de la misma manera podemos obtener un ciberespacio para poder tener un lugar de expresión, buscar información o bien simple ocio, este sistema de Internet tiene gracias a si origen militar y gubernamental, una exactitud, fácil distribución de información, y hecha a lenguaje entendible para todos, y de la misma manera cada día se estima un crecimiento del censo de usuarios de Internet. Todo este crecimiento se debe a la gran cantidad de información real que ahí se puede encontrar, de la misma forma podemos decir que el sistema de Internet no es más que una conexión entre los países en donde hay documentos textuales, así como imágenes, que nos pueden ayudar a resolver problemas de información, y no sólo eso sino que a pesar de poder encontrar diferentes autores que publicaron sus obras.

Octava. En conclusión del funcionamiento de Internet. Es una relación comercial de un cliente y un servidor, es un conjunto de computadoras, una que tiene el objeto de servidor o proveedor de información, por el otro lado el que van a actuar como receptor de esta información, que llega a los quipos como son dispositivos inalámbricos como teléfonos celulares, computadoras de mano o las conocidas computadoras de escritorio o llamadas "PC". Todo este sistema se hace por diversos medios de conexión para los equipos cada día más avanzados, pero también son en ocasiones caros.

Novena. En conclusión a los usuarios de de la Red de Internet, va a dar el desarrollo de nuevas culturas calificada en este trabajo de investigación como Cibersociedad. Es un concepto que en la actualidad la mayoría de los navegantes de Internet saben a que se refieren al mencionarlo. Pero también se señalo que como en una sociedad moderna, en esta sociedad virtual, vamos a encontrar la popularización del uso de los diversos instrumentos y hábitos en Internet. Y como en todo lo que hay en nuestras vidas los cambios son frecuentes tanto en lo real como en lo virtual, nadie puede negarse o cerrarse a lo que vivimos, tiempos de grandes cambios de una nueva revolución tecnológica.

Son cambios que han marcado a las Sociedades Modernas, las cuales se están organizando en torno a la tecnología y a la información, esta Cibersociedad dependiendo de quien lo hace trata de tener control social y de la dirección de las innovaciones y más a un garantiza los cambios en nuestro mundo, este cambio social es la aceptación que da el hombre a todo este impacto social, creador de la nueva sociedad virtual o Cibersociedad que hay que tratar de conocer y sobre todo, entender el impacto en nuestras vidas, esta Cibersociedad es muy importante para el Internet ya que hacen y coordinan lo que existe en el Ciberespacio. Durante el desarrollo de la Red de Información de Internet la creación de la Cibersociedad fue algo inevitable, evoluciono día a día, es más que un conjunto de máquinas y cables, también tiene relacionados como hemos mencionado durante el desarrollo de este tema tiene cuestiones de carácter económicos, políticos, jurídicos, históricos y socioculturales, en conclusión es un nuevo carácter social.

Décima. Podemos tener en conclusión la característica y naturaleza de la Cibersociedad, es la misma que tiene cada uno de los usuarios, es decir esta creada con las características de cada persona, es como la creación de una ciudad la cual esta hecha dependiendo de las necesidades y deseos de quienes la construyen, obviamente esta es una mezcla entre tecnología e información y no sólo eso sino también en el orden social y psicológico. Como características es que es similar a una Sociedad Real, la que todos vivimos, esta enfocado a una Civilización Virtual o Cibersociedad, vamos a encontrar estructuras institucionales, legislaciones, ofertas y demanda, bolsa de trabajo, emergencias de nuevos conflictos como también desigualdades sociales, marginación y mucho más. La Cibersociedad ha producido una auténtica revolución que va a transformar radicalmente a la sociedad moderna.

Décima Primera. Como se podría decir que todo lo bueno siempre tiene algo malo, se concluye que como sucede en todas las comunidades del mundo vamos a encontrar gente que se encarga de dañar la estabilidad, gente que se encarga de cometer los delitos los cuales son sancionados por la sociedad, la cual crea reglas de buenas costumbres, y estar reglas son para salir a flote como sociedad, pero junto a esta Cibersociedad, que esta en Internet de buena fe, existen navegantes con el ánimo de causar daño y poder sacar provecho de otros sin remunerarle o bien reponerle por ese beneficio, o de la misma manera vivir de ellos por medio del delito, esta Red de Información de Internet, aparte de dar a la

humanidad una gran aportación en cuestiones de información, ha surgido una generación de nuevos personajes peligrosos que difunden el miedo en Internet.

Décima Segunda. Los tipos de sujetos en el sistema de Internet, tenemos en conclusión que son dos, los sujetos activos y los sujetos pasivos, los primeros: son los usuarios encargados de cometer los Daños y Delitos Informáticos, los Sujetos Activos son los Delincuentes Informáticos, son personas que poseen características que no presenta la mayoría de los delincuentes, esto se debe a que los Sujetos Activos cuentan con excelentes habilidades para el manejo de los sistemas Informáticos, y a consecuencia de esto y por su posible situación laboral se encuentra en lugares estratégicos donde tiene a su alcance el manejo de información a través de la Red de Comunicación de Internet, o bien son jóvenes que por simple ocio y su habilidad en el uso de los medios de Información, se encuentran todo el día conectados a esta Red y cuentan con los medios económicos para poder adquirir medios tecnológicos para facilitarle esta labor de daño o comisión del delito, en conclusión son personajes que utilizan este medio para crear un daño.

Por lo que respecta al Sujeto Pasivo. Que es la víctima o la persona en la que recae la conducta delictiva que realiza el Sujeto Activo. El Sujeto Pasivo es un individuo común que navega en la Red de la Información, y este daño puede estar dirigido a una Institución de cualquier tipo, financiera, crediticia, gobierno u otras, de la misma manera los usuarios comunes, y esto lleva a crear Cifras Negras de perdidas económicas, en conclusión hay dos tipos de individuos y estos son los que le dan el ser a la Red de Información de Internet

Décima Tercera. Hay que señalar en esta conclusión que los sujetos más importantes en nuestro trabajo son lo en cuestión de los agresores son los Hackers, es una persona compulsiva y con una gran obsesión por acumular o obtener información, son las personas que suelen abrir todos los apartaos eléctricos, de la misma forma en aparatos informáticos, suelen revisar su computadora en cuestiones de ordenador y modificarla, aun cuanto no conozcan la consecuencia de su acto. Una Persona con tendencia a ser un excelente Hacker prueba y modifica las cosas que pudieran llegara sus manos y se pasa largas horas pensando en ello analizando, tratando de sacar un por que, que pasaría si le faltara algún componente, y hay dos de estos individuos catalogados como los Hackers en sí y los Hardware Hakers. Los cuales ya hemos analizado en el segundo capítulo, los primero de ellos solo obtiene el conocimiento para practicar con los ordenadores y equipos, para introducirse en los sistemas de otros usuarios, y el segundo tienen interés por el

sistema electrónico, pero en si ambos tiene los mismo conocimientos. Los Hackers son aquellos personajes comunes y corrientes que podemos encontrar en cualquier lugar, concluyendo que pueden ser cualquier vecino.

Décima Cuarta. En la conclusión de lo que son las clasificaciones de los agresores informáticos, como vimos durante en desarrollo del tema existen bastantes, los cuales tienen su propio medio de actuar y de causar un determinado daño a nuestros equipos de cómputo, información o bien a nuestra privacidad. Y que la conclusión en cuanto a estos actores es que cada día más comunes los que se autodenominan Hackers sin siquiera tener el conocimiento de ello, y en ocasiones causan daños como soltar virus en la red y probar programas de Hacking sin llegar a tener el conocimiento pleno. El objetivo de este capítulo es que se conozcan los diferentes tipos de agresores informáticos, sus actividades, ya que en ocasiones esto confunde a las personas en ubicarlos.

Décima Quinta. Como objetivo de conclusión es dar a conocer cuales son los métodos más comunes que se utilizan para realizar ataques a la seguridad informática como es confidencialidad, integridad y disponibilidad de la información de una organización o empresa, de la misma forma hace mención a los objetivos de ataque como fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar un sistema. Se pudo apreciar que tipo de usuario puede ser el posible perpetrador del daño como empleados, personas externas o eventuales. Como conclusión la mayoría de estos agresores son jóvenes que apenas pasan los veinte años, se lanzan desafíos para quebrar tal o cual programa de seguridad, captar las claves de acceso a computadoras remotas y utilizar sus cuentas para viajar por el ciberespacio, ingresar a redes de datos, sistemas de reservas aéreas, bancos, o cualquier otra lugar más o menos peligroso. En conclusión, estos individuos son personas que cuentan con muy buen equipo para poder realizar estos ataques, gastan para obtener equipo, así como hay unos que roban información para venderla y de la misma forma recuperarse en ganancias.

Décima Sexta. En el apartado de la clasificación de delitos Informáticos, vamos a hacer una conclusión genérica en relación a que debemos de tener conocimiento de los diferentes tipos de delitos Informáticos, para así podamos tener un amplio criterio de las diferentes modalidades delictivas que podemos encontrar en la Red de la Información. Se hace una enumeración de estos delitos y como se realizan, de la misma forma señalamos que este capítulo nos va a dar a conocerlos, como actúan y desarrollan, concluimos que son

como parte de nuestra sociedad moderna, es decir hay diferentes tipos de delitos como por ejemplo, si un individuo roba documentos confidenciales los foto copia, es un mismo delito que lo podemos canalizar a nuestro tema como Manipulación de los Datos de Entrada o como lo pudimos apreciar en este trabajo que es conocido como Insiders.

Décima Séptima. Conclusión del apartado relacionado a los daños o modificaciones de programas o datos de los sistemas de cómputo. Es principalmente un tema esencial de este trabajo de investigación, son los daños que sufren los usuarios por los agresores, esto lo nos va a dar la conclusión de que es un apartado que habla de los delitos en contra de la Intimidad, de los Virus Informáticos y que tipo de actividad tienen en el Sistema de Computo nos va a decir que es el daño a las personas y bienes.

Décima Octava. Vamos a concluir que los virus informáticos son los principales programas que causan el daño tanto a la economía de un individuo, empresa o gobierno, como lo vimos en el capítulo segundo son programas que funcionan para robar información o bien para obtener claves secretar de los usuarios a los que se les introduce dicho virus. Vamos a tomas en conclusión que este es el mayor de los problemas que afectan a la Cibersociedad. Debido a que como hemos visto los Virus Informáticos son principalmente amenazas en la Red de la Información de Internet, claro unos más que otros y son meros programas que afectan los Equipos de Computo, muchos de estos programas no son detectados tan fáciles ya que no ocupan gran espacio en la computadora, y de la misma forma tiene la característica de que pueden auto repetirse. Tenemos por aclarado que los virus Informáticos poseen la capacidad de controlar tanto los ficheros como el sistema operativo de nuestro Equipo de Computo en el caso de los virus malignos, pero también hay virus que no causan daño solo muestran mensajes sin sentido en la pantalla, o bien que detectaron errores en los Equipos de Computo. En conclusión los virus son los mayores objetos de daño a los usuarios así como a la economía, suelen tener diferentes actividades en los equipos cuentan con período de desarrollo. Son programas con un proceso de vida y creación, contagio, incubación, reproducción y Ataque, siendo estos de gran cuidado para nuestras actividades cotidianas en la Red de Información de Internet.

Décima Novena. En conclusión a el capítulo relacionado con Internet y su regulación, podemos decir que el mundo actual todos somos testigos de lo que ha sido el crecimiento del uso del la Red de la Información, que no es más que le Internet, todo fue evolucionando y ha traído demasiados cambios consigo de de tener carácter Científicos,

Militares, Diplomáticos o Jefes de Estado, a la actualidad en que la mayoría de los navegantes son gente común y corriente, sin privilegios o posición social, es gente muy variada, buscando datos en relación a información de conocimientos generales, leyes y reglamentos, hasta la posible inversión en bienes raíces, traspasos bancarios, claro esta también sin dejar de visitar los diversos entretenimientos que ahí se encuentran. Esto dice que el los hombres tienen la libertad de realizar diversas actividades en el mundo, siendo que las libertades de los hombres están limitadas hasta donde no dañes a segundas personas, esto a llevado a la sociedad a crear leyes y reglamentos para regular la vida social de nuestro mundo, aquí en Internet paso de ser Cibercomunidad aislada exclusiva para determinadas personas, a pasado a ser, un gran número de usuarios, o una Cibersociedad, de grandes grupos con perfiles e intereses diversos entre si, ya que esta cuenta con reglas de protocolo como lo vimos en este tema de investigación, no hay reglas explicitas, sino reglas de conducta para los que lo usan, es decir, la Red de Internet, es hasta el momento un sistema el cual no esta regulado al cien por ciento, urge una regulación mas explicita y plasmada para que todos las puedan ver y conocer, aun siendo reglas de protocolo.

Vigésima. Concluimos que la legislación que hay en materia o en su gran mayoría es para protege los derechos de autor, más no, en si la privacidad de los usuarios comunes los cuales son los que más tiempo se encuentran en la Red de la Información, y quienes la hacen crecer, como se pudo apreciar en las leyes que se citaron en el capítulo tercer, urgen normas para tratar más a fondo los daño, o destrucción de información, por el hecho de que al dañar un equipo es costoso el renovarlo o adquirirlo nuevo. Todas la leyes vistas nos hablan de protección al Derecho de Autor, y si mencionan la privacidad no es completo o sin gran importancia, como lo hacen otros países, este capítulo tercero trata de tomar en cuenta lo que dice el artículo 16 de nuestra Constitución Política de los Estados Unidos Mexicanos, que señala que a grandes rasgos, y señalando lo que puede interpretarse a este tema; nadie puede ser molestado en su persona,..., papeles,... este caso podemos tomarlo como papeles virtuales o archivos privados de las computadoras, las cuales son posesiones personales de los usuarios, lo cual debe tomarse en cuenta.

Vigésimo Primera. Concluyendo el capítulo tercero de nuestro tema de estudios, hay que tocar un tema importante que es la ley a la cual se dirige la propuesta de este tema, en el ámbito administrativo, la Ley de Telecomunicaciones, esta ley en nuestro país esta encargada de garantizar la integridad de las vías de comunicación, de lo cual se saca en

conclusión que por su naturaleza tiene en su cargo todo lo relacionado con la Red de la Información de Internet, por estar íntimamente ligado a la comunicación además de que su suministro es por cualquier medio que regula dicha ley.

Vigésima Segunda. En conclusión a lo que respecta al capítulo cuarto, uno de los temas más importantes es, sobre los Organismos internacionales. El objetivo principal de este capítulo es dar un breve análisis de leyes, acuerdos y legislaciones, existentes en otros países, en donde van a tomar varios elementos, entre los cuales son tema de de estudio de este trabajo, tanto por organismos gubernamentales de otro países así como internacionales, lo cual tiene como objetivo el enfrentar la problemática presente, de nuestros días en materia de los delitos informáticos, este tema da a conocer lo que otros países tiene, a fin de combatir estos delitos y que del cual se debes conocer para poder tomar en cuenta para un futuro en nuestras leyes.

Vigésima Tercera. El Organización de Cooperación y Desarrollo Económico (OCDE), es un organismo en cual si trata un poco en relación al buen o mal uso que le podamos dar a una computadora sobre uso indebido de los programas de Computación, el darle un mal uso a un programa también abarca a los programas de Hackers para dedicarse al espionaje, y poder robar información. Nos da una conclusión de que lo visto anteriormente en este capítulo, es que hay Organismos Internacionales que trata y toma en consideración el daño que causa el mal uso de una computadora, es decir, trata de proteger el posible daño a los usuarios y da una normatividad a este tema.

Vigésima Cuarta. La legislación en otros países, es por lo regular encaminada al castigo penal, hablando de los Delito Informático y los casos de abusos relacionados con la informática, existen, al menos en parte, dificultades para poder encuadrarlos. Estas proceden en buena medida de la prohibición jurídico-penal. De ello surge la necesidad de adoptar medidas legislativas, pocos son los países que disponen de una legislación adecuada para enfrentarse con el problema, concluyendo en este tema que los países más industrializados, son los que cuentan con una legislación que cubre todo los aspectos de daño, robo o espionaje en Internet a través de un equipo de computo, por lo tanto debemos tomar algo de otros países, aun que no tengamos la infraestructura y el desarrollo, pero debido al rápido neoliberalismo de nuestro país y a la gran cantidad de tratados que tenemos y al aumento de la tecnología, debemos por lo menos conocer el aspecto informático de otros países y tratar de adecuar y legislar no sólo en los penal, ya que

nuestras cárceles están llenas sino también tomar en cuenta lo administrativo en nuestras leyes.

Vigésima Quinta. Podemos concluir en el capítulo quinto en relación de la privacidad, que es algo muy importante en nuestra vida los seres humano necesitan tener garantías así como todos nuestros derecho y uno de estos es el derecho a la privacidad, todos los ciudadanos tanto de nuestro país como del otros debemos tener garantizado este derecho, en la Red de Internet, hay una gran capacidad de expresión así como los contenidos o bien la información, es tan amplia para decir que la posibilidad para que los mensajes de información personal que se envían a través de está Red de Internet así como se almacena en los equipos de computo de los cuales cientos de usuarios no quiere que sea conocida por otros por que es personal como pueden ser, trabajos, de investigación u otros, la interferencia se da en todos los medios los cuales están regulados pero este tema nos dice que es urgente conocer y tratar el tema de la falta de privacidad en el sistema de Internet por ser una de las herramientas más usada y cada día más creciente entre los ciudadanos.

Vigésima Sexta. La Inversión económica en el uso del Internet por los Usuarios, es un tema muy controversial, en relación a este tópico, es que entre más crece el Internet, también crece el uso de la tecnología. Esto hace que la implementación de mecanismos y sistemas de seguridad se de prácticamente en todos los niveles. Todas pueden acceder a las herramientas que necesitan así como a los costos que se adapte cada usuario, la inversión que cada empresa debe realizar va de acuerdo con sus necesidades, así como que debe de tenerse actualizado para garantizar su seguridad. Este tema va muy relacionado con los costos de los diferentes sistemas y herramientas de protección que se están haciendo accesibles, en general. Los costos que produce el proteger los sistemas de cómputo, así como los daños que se producen son gastos que no deberían realizarse, si hubiera una cultura de respeto a los otros usuarios, la vulnerabilidad de la información transferida por la Internet y la facilidad de ataques externos e internos que se traducen en pérdidas económicas que ascienden hasta miles de dólares en términos de información alterada, robada o perdida.

La inversión y costos de la protección de los equipos de cómputo en ocasiones son elevados y en conclusión los costos de la inversión para la protección son muy altos y estos debe de estimular a legislar para tratar de crear una cultura y una educación de respeto a la información de los demás y al mismo Estado.

Vigésima Séptima. Los delitos cibernéticos en relación a la violación de la privacidad a la cual están sujetos todos los usuarios de la Red de Internet, es un tema muy controversial. La violación a la privacidad es que, cualquier usuario con conocimientos amplios en computación puede hacerlo, o bien a través de un virus informático que se reproduce y causa daños a estos sistemas como mencionamos con anterioridad los virus roban información para mandarla a quien lo creó. En la conclusión de este tema hay que resaltar que la privacidad en Internet a lo que tenemos derecho, y la violación a este derecho es algo que debemos conocer así como los medios por los cuales se produce, y que como este tema nos hizo mención hay diferentes formas de agredir la privacidad, se trataron tópicos los cuales van a ser considerados como delitos en razón a la privacidad de los usuarios, en si nos da a conocer la manera de cómo se comete este acto, y dejar abierto para que se conozca como una lesión a los usuarios.

Vigésima Octava. Como conclusión a la Propuesta de "Anexo al Artículo 71 en base a la fracción A, Apartado V, de la Ley Federal de Telecomunicaciones." En cual se enfoca al artículo antes mencionado, tiene como objetivo primordial, dar como base de esta propuesta para que este tipo de conducta sea canalizada y legislada a una Institución Administrativa que se encargue de sancionarla.

Nuestras Instituciones de Readaptación Social están llenas de individuos que cometieron delitos tal vez no graves tal vez sí, pero este trabajo trata de enfocar este tipo de conductas a un nivel administrativo, con el fin de no saturar a un más las cárceles, con individuos los cuales cometieron un delito que se puede reparar el daño, al afectado, de la misma forma, la Secretaria de Comunicaciones y Transportes, podría tomar en consideración que si es meritorio, el obligar al agresor a cumplir aún a pesar de la reposición del daño, a que cumpla con una especie de trabajo social, dándole cursos de capacitación a quien lo necesite en la misma institución, es decir por que recluir a una persona a una cárcel, cuando se pueden aprovechar sus conocimientos para algo más benéfico a nivel Institucional. En conclusión la Secretaría de Comunicaciones y Transportes, a través de la Ley Federal de Telecomunicaciones, sería la encargada de sancionar, ya que esta es quien regula los medios de comunicación y son a través de estos por los cuales el servició de Internet es suministrado por lo tanto es la que debe tomar cartas en el asunto para llevar una armonía en nuestra sociedad en Internet, la cual ya es parte de la vida cotidiana y que nadie podrá escapar a este desarrollo tecnológico.

Bibliografía.

ACEDO QUEZADA, Octavio R. Cursos de Informática en la escuela de Derecho, en Revista Tribunal, Poder Judicial de Jalisco, 1997.
TÉLLEZ VALDÉS, Julio. Derecho Informático. Segunda Edición. Editorial McGraw-Hill, México 1999.

Diccionarios.

GARCÍA PELAYO Y CROSS, Ramón. Pequeño Larousse Ilustrado, Edición Larousse, S. A. DE C. V. MARCELLA, 53, MÉXICO,

Diccionario Web.

http://www.podernet.com/2000/glosario/indice.html. Miércoles 05 de marzo de 2003. 13:50 PM.

Hemerografía.

Cobertura regional de los satélites para servicios de televisión y video. Fuente GAO, Telecommuinacatiosn issues in international satellite communications, October, 1996. (Artículo aparecido en el periódico Reforma en el Suplemento especial de Telecomunicaciones, noviembre de 1996.
HERNANDEZ, Claudio. Los Clanes de la Red 2000. En Revista Kriptopolis. Número 02 España 1999.
PETIT, Eugéne. Tratados Elementales de Derecho Romano. 13ª edición. Editorial Porrúa, México 1997.
H. SCHILLER, El poder informático, Madrid, Gustavo Gili, 1983.
BELL, Daniel, El advenimiento de la sociedad post-industrial, Madrid, Alianza, 1976.

Hemerografía Páginas Web.

CARENA, Juan C. y FERRANTI, Liliana. Universidad Católica de La Plata –Unidad Académica Rosario Moreno 1056-200 Rosario. http://www.psicologia-online.com/ciopa2001/actividades/59/. Martes 14 de octubre de 2003, 15:30 PM.

CISNEROS RUIZ, Juan Carlos. Internet y su regulación. http://www.interclan.com/fenasem/lexmatic/regular.htm. Miércoles 26 de febrero de 2003. 12:00 PM.

Código penal de España, http://www.igsap.map.es/cia/dispo/cpenal-12.htm. Sábado 29 de noviembre de 2003, 12:30 PM.

Código Penal Peruano, http://www.leyes.congreso.gob.pe/Imagenes/Codigos. Sábado 29 de noviembre de 2003, 15:00 PM.

FERNÁNDEZ CALVO, Rafael. Glosario básico ingles-español para usuarios de Internet, versión HTML4.0 (julio 2001) de la cuarta edición (mayo2001),

FERNÁNDEZ MUERZA, Alex. Observatorio para la Cibersociedad, http://www.elprincipe.com/teleformacion/notas/index55.shtml, Lunes 13 de octubre de 2003. 12:00 PM.

http://www.informador.com.mx/informa/depa/informatica/secciones/internet.html, lunes 03 de noviembre de 2003, 20:03 PM.

http://portal.uaq.mx/seguridad/PFP-policia-cibernetica-entrevista-de-Nicolas-Suarez-Valenzuela.html, lunes 03 de noviembre de 2003, 20:03 PM.

http://websperu.wperu.com/internet.html, Domingo 12 de octubre de 2003. 12:14 PM.

http://www.ati.es/DOCS/internet/histint/histint1.html#conceptos, Viernes 17 de octubre de 2003. 12:00 PM.

http://www.atlas-iap.es/~pepcardo/index.shtml?http://www.atlas-iap.es/~pepcardo/historia.htm. Miércoles 02 de octubre de 2003, 13:30 PM.

http://www.baquia.com/com/20001113/art00014.html, Martes 21 de octubre de 2003. 12:00 PM.

http://www.ciberconta.unizar.es/LECCION/INTRANET/INICIO.HTML, Viernes 17 de octubre de 2003. 15:30 PM.

http://www.cronis.com/kids/okids1a2.html, Domingo 12 de octubre de 2003. 13:30 PM.

http://www-etsi2.ugr.es/alumnos/mlij/abaco.htm. Miércoles 02 de octubre del 2003, 19:00 PM.

http://www.monografias.com/trabajos/hackers/hackers.shtml, miércoles 12 de marzo de 2003, 12:00 PM.

http://www.monografias.com/trabajos/cibernetica/cibernetica.shtml, Martes 14 de octubre de 2003. 12:30 PM.

http://www.monografias.com/trabajos/computacion/computacion.shtml, miércoles 24 de septiembre de 2003, 10:30 AM.

http://www.nodo50.org/manuales/internet/1.htm, Domingo 12 de octubre de 2003. 15:30 PM.

http://www.podernet.com/2000/glosario/indice.html#arpanet, Domingo 26 de octubre de 2003, 15:00 PM.

http://www.pchardware.org/historia/primera.php, Martes 01 de octubre de 2003, 12:30 PM.

http://www.pchardware.org/historia/cuarta.php, Miércoles 24 de septiembre de 2003, 13:00 PM.

http://www.servisoft.es/htm/base_datos.htm, Jueves 16 de octubre de 2003. 12:30 PM.

http://www.stj-sin.gob.mx/Delitos_Informaticos2.htm. Miércoles 26 de febrero del 2003, 14:55 PM.

IZA MARTÍNEZ, Paola. http://www.microasist.com.mx/noticias/internet/achin0703-2.shtml, miércoles, 12 de marzo de 2003, 1:25 PM.

JOYANES AGUILAR, Luis. Cibermaneras. Revista Vivat Académica, Abril 2000. http://www2.uah.es/vivatacademia/anteriores/catorce/cibermaneras.htm#NOTA%2059, Lunes 13 de octubre de 2003. 13:00 PM.

MAYA I PLANELLS, Joan. Comunicaciones Electivas, Nota sobre la virtualización de lo comunitario en el tiempo de desterritorialización, http://cibersociedad.rediris.es/mayans/mayans_12.php, Lunes 13 de octubre de 2003. 12:30 PM.

PACHECO KLEIN, Jorge. Introducción a los delitos informáticos en el ciberespacio. Normas y Jurisprudencia comentadas. http://www.delitosinformaticos.com/noticias/archivo/arc6-2001.shtml. Lunes 24 de febrero de 2003, 13:00 PM.

PÉREZ LOZANO, José Manuel. Universidad de Granada España, Delitos Informáticos, http://comunidad.derecho.org/plozano/webs_sobre_delitos_inform%E1ticos.htm, Domingo 26 de octubre de 2003, 12:00 PM.

Supremo Tribunal de Justicia del Estado de Sinaloa, Derechos Reservados 1998. http://www.stj-sin.gob.mx/Delitos_Informaticos2.htm#CAPÍTULO%20I, miércoles 01 de octubre de 2003, 12:00 PM.

TREJO DELARBRE, Raúl.

http://raultrejo.tripod.com/ensayosinternet/derechodelitosylibertades.htm, miércoles 26 de febrero de 2004, 13:30 PM.

VIEGA RODRÍGUEZ, María José. Delitos Informáticos, http://derecho.org/comunidad/mjviega/deli_inf.htm. Miércoles 01 de octubre de 2003, 14:00 PM.

Legislación.

Nuevo Código penal del Distrito Federal. Editorial Sista S. A. de C. V. México D. F. 2003

Código Penal Federal, Compendio de leyes, reglamentos y otras disposiciones conexas sobre la materia 2003. Grupo ISEF. México D. F. 2003.

Código Penal y de Procedimientos Penales para el Estado de Sinaloa, Porrúa, tercera edición. México 1997.

Constitución Política de los Estados Unidos Mexicanos. 145ª edición. Editorial Porrúa. México, 2003.

Ley Federal del Derecho de Autor. Diario Oficial de la Federación. Martes 24 de diciembre de 1996.