INSTITUTO UNIVERSITARIO NEZAHUALCOYOTL
INCORPORADO A LA UNIVERSIDAD NACIONAL
AUTONOMA DE MEXICO

LA NECESIDAD DE ADECUAR LA LEGISLACION Y LA JUSTICIA MEXICANA FRENTE A LOS DELITOS INFORMATICOS ACTUALES

T E S I S

QUE PARA OBTENER EL TITULO DE

LICENCIADO EN DERECHO

P R E S E N T A :

JAFET ISRAEL RAFAEL ARREOLA GONZALEZ

ASESORA : LIC. MARIA ANGELICA DOMINGUEZ MARTINEZ

NEZAHUALCOYOTL, ESTADO DE MEXICO 2004

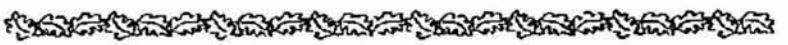
DEDICATORIAS

A DIOS.

Dedico mis plegarias en poesías
al Creador, Padre Omnipotente,
cual sahumerio de alegrías
vertiendo lo que mi alma siente.

Es para ti mi adoración
ya que eres Poder inagotable
¡Alabado seas en todo corazón...
Dios eterno y perdurable.

CON RESPETO Y ADMIRACIÓN



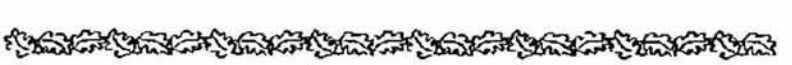
A MI MAMI JUDITH GONZÁLEZ CHAVEZ.

Tengo tanto que agradecer, a ti mamá,
todo lo que llegue a ser, por ti será;
en los momentos más difíciles
siempre hemos estado juntos,
conoces mas de mi, que yo mismo
conoces todos mis errores y mi dirección.

A ti te doy gracias por todos tus cuidados y
porque siempre creíste en mí. Eres la mejor
mujer que conozco. Te dedico este trabajo
porque es algo que sin tus desvelos no hubiera
podido ser.

A MI PADRE, RAFAEL ARREOLA YÁNEZ.

Te agradezco por haberme dado la vida,
no puedo expresar aquí mismo
todo lo que siento por ti, así es
que solamente digo GRACIAS.



AL SEÑOR JESÚS GONZÁLEZ CHAVEZ.

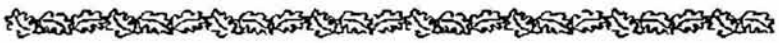
Por que supiste escucharme y me brindaste
ayuda cuando era necesario,
por que te has ganado
mi afecto, admiración y respeto

Que con abnegación y cariño me
dio siempre ánimo para no desmayar
y culminar con la meta que me propuse,
te dedico este trabajo Papá Chuchito.

A MI HERMANA ADLAI JUDITH ARREOLA GONZÁLEZ.

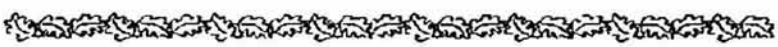
Desde que naciste, eres la persona
que mas quiero en esta vida
Gracias por todo tu apoyo
y tu confianza hermanita,
por ser el aliento que me da ánimo
para seguir siempre adelante,
sin ti no lo hubiera logrado.

AL INSTITUTO UNIVERSITARIO NEZAHUALCÓYOTL

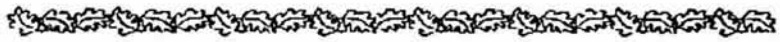


Por abrir mi mente al conocimiento universal
que en sus recintos sagrados se contiene.

Su grandeza subsistirá pese a todo y a todos.
Mi veneración y respeto por el resto
de mis días.

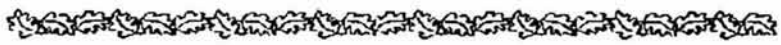


A LOS LICENCIADOS.

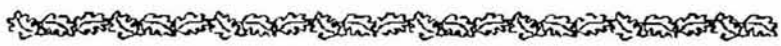


A dos almas superiores que unidas
consolidad el sueño de todo profesionista,
mi agradecimiento eterno a los Abogados
María Angélica Domínguez y Jesús Yáñez Mirón.

Por todo su apoyo y confianza que
me brindaron, nunca olvidare lo que me
dijo un día de que un favor no se le niega
a un amigo, es por ello que cuenten con
un amigo para toda la vida



Al Lic. **Rodolfo Calvillo Popoca**
por el apoyo, confianza y paciencia que me brindo
en la elaboración y tramitación del presente trabajo.



A MIS MAESTROS QUE SUPIERON GUIARME A TRAVÉS DE MI CARRERA, CON SU SABIDURÍA Y EN ESPECIAL A LOS SIGUIENTES LICENCIADOS:

Angélica Alfaro Ramírez

Rebeca Almendáriz Ortiz

Dector García Romeo

Noé González Figueroa

José Luis Gutiérrez De La Rosa

Israel Landín Flores

Enrique Mendoza Oropeza

Mario Montes Real †

Oscar Pimentel García

Yanet Rodríguez Acosta

Juan Carlos Romero Avila

Raúl Sánchez Piña

Raúl Soto Mendoza

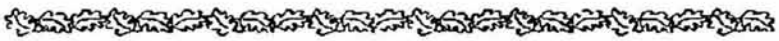
Fernando Solares Cortes

Octavio Vargas Nuñez

Francisco Moisés Vázquez Reyes

Y con mucho cariño
a la Lic. **Adela Ramírez Alonso,**
le estoy agradecido eternamente
por haberme dado ese impulso,
en esos momentos cuando
mas lo necesitaba.

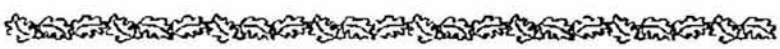
EN UNA FORMA MUY ESPECIAL, DEDICO TODOS MIS ESFUERZOS
EN MEMORIA DE LA SEÑORA PETRA CHÁVEZ DE GONZÁLEZ.



Gracias madre mía
en la tierra o en el cielo
por todo lo que me diste
en esta vida.

Palabras no encuentro
para decirte lo que siento
expresar mi sentimiento
darte mi agradecimiento

Jamás olvidare
lo que me pediste,
es por ello que te brindo
este momento maravilloso
de mi vida



"LA NECESIDAD DE ADECUAR LA LEGISLACIÓN Y LA JUSTICA MEXICANA FRENTE A LOS DELITOS INFORMÁTICOS ACTUALES"

ÍNDICE GENERAL

ÍNDICE GENERAL

CAPITULO IV
DERECHO COMPARADO Y MARCO JURÍDICO NACIONAL EN LOS DELITOS INFORMÁTICOS.

INTRODUCCIÓN

INTRODUCCIÓN.

El presente trabajo lo he considerado novedoso y de gran interés, ya que cada vez con mayor intensidad se ha hablado de los beneficios que los medios de comunicación y el uso de la informática han aportado a la sociedad actual, pero el propósito del mismo es analizar la otra cara de la moneda, es decir, las conductas delictivas que puede generar del gran avance tecnológico, sobre todo en el campo de la informática.

Empleo el método de investigación de campo, donde consulto a personas especialistas en materia informática, también empleo el método bibliográfico donde se consulto diferentes tipos de libros de dicha materia y de Derecho y otras fuentes de información.

Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales. En los últimos tiempos, ha sido evidente que la sociedad ha utilizado de manera benéfica los avances derivados de la tecnologia en diversas actividades; sin embargo, es necesario que se atiendan y regulen las cada vez más frecuentes consecuencias del uso indebido de las computadoras y los sistemas informáticos en general.

Debido a su peculiar naturaleza, realizo una serie de

exposiciones las cuales son las siguientes:

En el Capítulo Primero se realiza un esbozo de la historia de la computación, donde se describen cada una de las computadoras, maquinas y objetos que la antecedieron, iniciando desde el comienzo de la historia hasta la época actual.

En el Capitulo Segundo se comprenden algunos conceptos fundamentales del Derecho informático, relacionándolos con los delitos informáticos.

El Capitulo Tercero se hace una perspectiva de lo que es el Internet, tanto en sus orígenes, concepto, el origen del Internet en México, así como todos los servicios que ofrece dicho sistema. Además se analiza los ilícitos que pueden ser cometidos en el Internet y los delitos típicos que pueden introducirse a la red.

En el Capitulo Cuarto comprende el análisis realizado a las legislaciones de otros paises en materia de delitos informáticos, así como también de la legislación nacional comprendiendo desde la Constitución Política de los Estados Unidos Mexicanos, la Ley Federal de Derechos Autor, la Ley de las Vías Generales de Comunicación y principalmente el Código Penal Federal Vigente y Código Penal para el Estado de Sinaloa.

Los tipos penales que contemplan el Código Penal Federal Vigente, no son suficientes, toda vez que hasta el momento existe

lagunas, para sancionar a los delitos informáticos ya que no contempla las modalidades actuales de dichos ilícitos.

Asi, llegamos al "Capitulo Quinto" donde concretamente me aboco a analizar la situación que guardan actualmente los delitos informáticos sea como instrumento, fin, objetivo y actualmente los cometidos vía Internet. Por lo mismo realizo una serie de propuestas para que se llegue a adecuar la legislación mexicana a las necesidades de los delitos informáticos actuales.

Por ende, el objetivo de este trabajo es probar que la delincuencia informática en México es una realidad palpable, y como tal debe dársele la importancia necesaria en todos los ámbitos para combatir eficazmente esta actividad ilícita y perjudicial para toda la comunidad informática y de negocios del país, analizando el impacto de las nuevas tecnologías a través de diferentes modalidades delictivas

Los llamados Delitos Informáticos, como se desarrollara más adelante, son cometidos por la computadora, a través de la conducta del hombre, es decir, que éste es quien los comete con ayuda de aquella. En ese entendido, el presente trabajo lo dirijo al análisis y propuestas de las posibles medidas preventivas y penas aplicables, sean de carácter administrativo o penal que considero deben ser tomadas en cuenta para evitar la comisión de este tipo de infracciones o delitos en México y con ello que los niveles de peligrosidad que se han dado en otros países puedan ser

contrarrestados en nuestro país, teniendo una legislación que se adecue a las necesidades informáticas.

Para finalizar mi introducción quiero hacer ver que este trabajo contiene la información que a mis amplias posibilidades de investigación pude encontrar, toda vez que como este tema es de vanguardia y prácticamente con carencia de información, tuve que remontarme a diversas legislaciones de alrededor del mundo para el desarrollo del mismo, por lo tanto no es una obra legislativa, más bien es un trabajo sencillo con el propósito que sirva de orientación para quienes traten de hacer temas de esta naturaleza.

CAPITULO PRIMERO

ANTECEDENTES GENERALES DE LA COMPUTACIÓN

CAPITULO I

ANTECEDENTES GENERALES DE LA COMPUTACIÓN.

La Computación surge de la misma inquietud racional del hombre, el cual, ante la cada vez más creciente necesidad de información para una adecuada toma de decisiones, es impulsado a formular nuevos postulados y a desarrollar nuevas técnicas que satisfagan dichos propósitos.

Por toda la historia, el desarrollo de máquinas matemáticas ha ido de mano en mano con el desarrollo de computadoras. Cada avance en uno es seguido inmediatamente por un avance en el otro.

Cuando la humanidad desarrolló el concepto del sistema en base diez, el ábaco fue una herramienta para hacerlo más fácil. Posteriormente apareció diferentes invenciones como el Telar de Jacquard, la Pascalina, calculadoras mecánicas, computadoras programables, computadoras electrónicas, computadoras personales, las IBM PC e IBM/ PC/XT, las computadoras ópticas hasta las computadoras modernas.

Cuando las computadoras electrónicas fueron construidas para resolver ecuaciones complejas, campos como la dinámica de fluidos, teoría de los números, y la física química floreció. Una breve reseña ilustrara tal información:

1.1.- Comienzo de la Historia.

Los primeros hombres que existieron en la humanidad, "... al verse en la necesidad de cuantificar sus pertenencias, animales, objetos de caza, pieles, etcétera..."[1] tenían que contar con los dedos, piedras y palitos almacenando toda esa posible información en su memoria.

El ejemplo claro de ello, lo podemos encontrar con el hombre de Neandertal, que data de los 6.500 años A.C , cuya especie antecede al hombre moderno, donde tenia un cerebro con mucho mayor capacidad mental por lo cual se presupone, tenia conocimientos de cálculo y mecánica.

1.2.- Período del año 500 A.C. al 1822 D.C.

Esta sección comienza desde la aparición del ábaco en China y Egipto, alrededor de 500 años a.C. hasta la invención del Motor Diferencial por Charles Babbage, en 1822. El descubrimiento de los sistemas por Charles Napier, condujo a los avances en calculadoras, por convertir multiplicación y división en suma y resta, un número de máquinas (incluyendo la regla deslizante) puede realizar estas operaciones. Babbage sobrepasó los límites de la ingeniería cuando inventó su motor, basado en este principio.

---

[1] **TÉLLEZ VALDÉS, Julio.** Derecho Informático. 2a. ed. México. Ed. Mc Graw-Hill 1996. P. 5.

Entre las primeras creaciones del hombre dirigidas a facilitar las operaciones de cálculo tenemos las siguientes:

1.2.1.- Ábaco.

El ábaco fue la primera máquina conocida que ayudaba a ejecutar computaciones matemáticas. Pelotas redondas, usualmente de madera, se resbalaban de un lado a otro en varas puestas o alambres, ejecutaban suma y substracción.

"Apareció en Mesopotamia, aproximadamente en el año 3500 A. C.; posteriormente fue descubierto otro en China, que data de 2600 A. C., el cual evoluciono rápidamente y adoptó el nombre de Suan-Pan. En la Edad Media, el ábaco se conocía en toda Europa, durante el siglo XVI este instrumento de cálculo llegó a Japón con el nombre de Soroban, y fue utilizado hasta el siglo XVII, donde ya entonces era empleado hábilmente para asiáticos y árabes."[2]

El gran aporte del ábaco fue la introducción de la llamada notación posicional, que es la que se utiliza hoy en día. Dicha notación, facilita mucho los cálculos aritméticos, y su principal ventaja se hace más evidente cuando se piensa en lo trabajoso que sería realizar una multiplicación usando números romanos.

---

[2] **TIZNADOS, Marco Antonio.** Informática. Ed, Mc Graw-Hill. 1ª Edición, México. 1997. P.2.

1.2.2.- Huesos de Napier (Napier Bones).

Justo antes de morir en 1617, el matemático escocés John Napier (mejor conocido por su invención de logaritmos que posteriormente fueron introducidos en las matemáticas con el propósito de facilitar, simplificar o incluso, hacer posible complicados cálculos numéricos donde se podían convertir productos en sumas, cocientes en restas, potencias en productos y raíces en cocientes) desarrolló un juego de palitos para realizar operaciones de multiplicación y división, a las que llamó "Napier Bones".

Así llamados porque se tallaron las ramitas de hueso o marfil, los "Bones" incorporaron el sistema logarítmico.

El método de radiología o huesos de Napier, consiste en unas tablas de hueso o marfil, con números grabados sobre ellas. Su método de la multiplicación (método de la celosía que consistía en un método de multiplicación), en el que los números a multiplicar se disponen digito a digito situándose a coincidencia de ambos dígitos del producto, con las decenas en la mitad superior y las unidades en la inferior sumando en diagonal se obtiene el producto. Mediante dos tablas adicionales se puede extraer raíces cuadradas y cúbicas.

El uso de las tablas de Napier se extendió rápidamente y en pocos años se encuentran ejemplos desde Europa hasta China, gracias a la difusión que provenía de los jesuitas.

1.2.3.- Regla Deslizante.

En 1621 la primera regla deslizante fue inventada por el matemático Inglés William Oughtred. La regla deslizante (llamado Círculos de Proporción) era un juego de discos rotatorios que se calibraron con los logaritmos de Napier.

Era una máquina que aparte de sumar, restar, multiplicar y dividir, adicionalmente, calculaba exponentes, funciones trigonométricas y otras funciones matemáticas de mayor complejidad.

Fue uno de los primeros aparatos de la informática analógica, la regla deslizante se usó normalmente (en un orden lineal) hasta que a comienzos de 1970, cuando calculadoras portátiles comenzaron a ser más popular.

1.2.4.- Reloj Calculador (Calculating Machine).

En 1623 fue diseñada la primera calculadora mecánica por Wilhelm Schickard en Alemania, cuya función era realizar operaciones de suma y resta llamado: Reloj Calculador, la máquina incorporó los logaritmos de Napier, hacia rodar cilindros en un albergue grande. A Schickard, se le acredita el haber comenzado el estudio formal de la lógica, la cual es la base de la programación y

de la operación de las computadoras.

1.2.5.- La Pascalina.

En 1642 la primera calculadora automática mecánica fue inventada por el matemático francés y filósofo Blaise Pascal, llamado la Pascalina, el aparato podía multiplicar y substraer.

Originalmente Pascal, desarrollo esta maquina para ayudar a su padre al momento de cobrar los impuestos. La sumadora mecánica, como también se le conocía funcionaba como maquinaria a base de engranes y ruedas, utilizando un sistema de cambios para pasar a dígitos.

A pesar de que Pascal fue enaltecido por toda Europa debido a sus logros, la Pascalina resultó ser un desconsolador fallo financiero, pues para esos momentos, resultaba más costosa que la labor humana para los cálculos aritméticos. Pero fue útil en generaciones subsecuentes de calculadoras mecánicas.

1.2.6.- Máquina de multiplicar.

"En 1666, el matemático ingles Samuel Morland desarrolló una máquina muy similar a la de Pascal que realizaba operaciones de

suma y resta, y la llamó máquina aritmética de Morland."[3] El aparato constó de una serie de ruedas, cada una representaba, dieses, cientos, etc.

Funcionaba por medio de un alfiler de acero que movía los discos para ejecutar las calculaciones. A diferencia de la Pascalina, el aparato no tenía avance automático en columnas.

1.2.7.- Máquina Calculadora.

La primera calculadora de propósito general fue inventada por el matemático alemán Gottfried Von Leibniz en 1673. El aparato era una partida de la Pascalina, mientras opera usa un cilindro de dientes (La Rueda de Leibniz) en lugar de la serie de engranaje.

Aunque el aparato podía ejecutar multiplicación y división, padeció de problemas de desconfianza que disminuyeron su utilidad.

1.2.8.- Máquina Lógica.

Se inventó la primera máquina lógica en 1777 por Charles Mahon, el Conde de Stanhope. El Demostrador Lógico era un aparato tamaño bolsillo que resolvía silogismos tradicionales y

[3] **TIZNADOS, Marco Antonio.** Op. Cit. P. 2.

preguntas elementales de probabilidad. Mahon es el precursor de los componentes lógicos en computadoras modernas.

1.2.9.- Telar de Jacquard (Jacquard Loom).

El Jacquard Loom fue inventado "En el siglo XIX, aproximadamente en 1805, Joseph Marie Jacquard construyo un telar que utilizaba tarjetas perforadas para controlar los gráficos o dibujos que debía realizar. Esta máquina se considera la primera programada, ya que ejecutaba órdenes prescritas en una tarjeta perforada."[4]

El Telar Jacquard era una máquina para tejer muy ingeniosa. Tenia unas varillas que se introducían en los agujeros de tarjetas perforadas; así se obtenían una forma especial en el tejido. La tejedora podía programarse de distintas formas, demás la tarjeta perforada transmitía a la máquina las instrucciones para su funcionamiento.

Aunque Jacquard no diseñó la maquina hiladora pensando en realizar cálculos, este invento revolucionó el hilar de seda, pues contribuyo a la formación de bases de muchos aparatos de informática e idiomas de programación.

---

[4] **TIZNADOS, Marco Antonio.** Op. Cit. P. 3.

1.2.10.- Artefacto de la Diferencia.

En 1822, "Con el apoyo del gobierno británico, Babbage inició la construcción del Engineer Difference. Que permitiría calcular tablas matemáticas, al sumar números hasta con seis dígitos."[5]

Dicho aparato era una asamblea compleja de ruedas, engranajes, y remaches. Utilizaba un dispositivo complejo de cálculo que usaba dos pares de tarjetas perforadas, un par daba las instrucciones a la máquina mientras que el otro par grababa los números a ser usados en los cálculos. Esta máquina podía recibir instrucciones, procesar y guardar información e imprimir los resultados.

Babbage sentó las bases de las computadoras, al grado de que se le considera hoy en día, el padre de las computadoras modernas.

1.3.- Período de 1823 – 1936.

Durante este tiempo, muchas de las culturas del mundo fueron avanzando desde sociedades basadas en la agricultura a sociedades basadas industrialmente.

---

[5] **FOURNIER, María de Lourdes,** Computación, México, 11ª Edición, Limusa, P. 16.

Con los diferentes tipos de avances matemáticos e ingeniería, hicieron posible máquinas electrónicas que pueden resolver argumentos lógicos complejos.

Comenzando con la publicación de Boolean Algebra de George Boole y terminando con la fabricación del modelo de la Máquina de Turín para máquinas lógicas, este periodo fue muy próspero para computadoras. Mismas que serán mencionadas en este capitulo.

1.3.1.- Calculadora Guiada por Teclas.

En 1885 la primera calculadora guiada por teclas exitosas, se inventó por Dor Eugene Felt. Para preservar la expansión del modelo del aparato, llamado el "Comptómetro" (era una calculadora con columnas diferentes para los diversos dígitos).

Felt compró cajas de macarrones para albergar los aparatos, aproximadamente en los siguientes dos años, Felt vendió ocho de ellos al gobierno estatal de Nueva York y al gobierno de los Estados Unidos.

Se usó el aparato principalmente por contabilidad, pero muchos de ellos fueron usados por la Marina de los Estados Unidos de Norte América en computaciones de ingeniería, y era probablemente la máquina de contabilidad más popular en el mundo

en esa época.

1.3.2.- Tubo al Vacío.

El avance más importante en el desarrollo de la electrónica fue dado por el científico americano llamado Lee De Forest en 1906, al introducir en el tubo al vacío un tercer electrodo reticulado, llamado rejilla, que permite el paso de electrones. Originalmente De Forest llamó a su dispositivo Audión, aunque más tarde se le llamó tríodo.(válvula electrónica). Tenía tres elementos dentro de una bombilla del vidrio evacuada. Los elementos eran capaces de hallar y amplificar señales de radio recibidas de una antena.

Por supuesto, como ocurrió muchas veces, De Forest tuvo que trabajar con diferentes dispositivos que no funcionaban adecuadamente antes de conseguir el tríodo. El tubo al vacío encontraría uso en varias generaciones tempranas de computadoras, a comienzos de 1930, con la creación de la compañía de máquinas tabuladoras.

1.3.3.- Flip-Flop.

En 1919 el primero circuito multivibrador bistable (o flip-flop),

fue desarrollado por inventores americanos W.H. Eccles y F.W. Jordan. El flip-flop dejó que un circuito tuviera uno de dos estados estables, que estaban intercambiables.

Formó la base por el almacenamiento del Bit-Binario (unidad de datos pequeña que puede manejar un ordenador) estructura de computadoras modernas de hoy en día.

1.3.4.- Computadora Analógica (Para Ecuaciones Diferenciales).

En 1931 la primera computadora capaz de resolver ecuaciones diferenciales analógicos fue desarrollada por el Dr. Vannevar Bush y su grupo de investigación. El Analizador Diferencial, como se llamaba, usaba engranajes diferenciales que fueron hechos rodar por motores eléctricos.

Se interpretaron como cantidades los grados de rotación de los engranajes. Las Computaciones, desarrolladas por dicha máquina, fueron limitadas por la precisión de medida de los ángulos.

1.3.5.- Máquina Lógica.

En 1936 el primer modelo general de máquinas de la lógica

fue desarrollado por Alan M. Turing. El papel, lo tituló "Números calculables," se publicó en 1937 en la Sociedad de Procedimientos Matemáticos de Londres y describió las limitaciones de una computadora hipotética. Números calculables eran esos números que eran números reales, capaz de ser calculados por medios del lo finito.

Turing ofreció prueba que mostró que al igual cuando usa un proceso finito y definido por resolver un problema, problemas seguros todavía no se pueden resolver. La noción de las limitaciones de tal problema tiene un impacto profundo en el desarrollo futuro de ciencia de la computadora.

1.4.- Período de 1939 – 1949.

Durante la Segunda Guerra Mundial, estudios en computadoras fueron de interés nacional. Un ejemplo de ello es el "Coloso", la contra Inglesa a la máquina Nazi de códigos, llamada "Enigma". Después de la guerra, el desarrollo empezó su nido, con tecnología eléctrica permitiendo un avance rápido en computadoras.

Tanto los Nazis como los aliados, buscaban diferentes tipos de tecnología para poder sorprender en los ataques que sostenían. Finalizando dicha guerra, apareció lo que es la Guerra fría, donde florecía la estrategia, que los combates.

En esta etapa se inventaron las siguientes computadoras:

1.4.1.- Computadora Electrónica Digital.

"En 1939, el profesor John Atanasoff de la Universidad del Estado de Iowa, con el objeto de encontrar una herramienta que ayudara a sus estudiantes de postrado a resolver las largas y complejas ecuaciones diferenciales, creó lo que pudo haber sido el primer computador digital electrónico, el computador Atanasoff-Berry Computer (ABC)."[6]

Fue la primera calculadora numérica electrónica del mundo. Incorporó varias innovaciones importantes en computar incluyendo el uso de la aritmética binaria, de la memoria regeneradora, del proceso paralelo, de la separación de las funciones de la memoria, el computar y usar los tubos al vacío como circuitos de lógica.

1.4.2.- Computadora Programable.

En 1941 la primera controladora para computadora para

---

[6] **BEEKMAN, Gerorge.** Computación e Informática, Hoy una mirada a la tecnología de mañana. Ed. Adisson Wesley Longman. México. 1993. P. 5.

propósito general usada se construyó por Konrad Zuse y Helmut Schreyer. El "Z-3," como se llamó, usaba retardos electromagnéticos y era programada usando películas agujereadas.

Era un computador electromagnético programable mediante cinta perforada, contaba con 2000 relés (electroimanes), 1000 kg. de peso, memoria para 64 palabras de 22 bits y un consumo de 4000 watts.

En este computador una suma demoraba 0.7 segundos, y una multiplicación o división 3 segundos. También fue un prototipo de laboratorio, pero ya incluía en sí diseño las ideas centrales que conforman a las computadoras actuales.

1.4.3.- Electrónica Ingles.

En el diciembre de 1943 se desarrolló la primera calculadora inglesa electrónica para criptoanálisis (ciencia que descifra informaciones transferidas ó almacenadas que se encuentran cifrada). "El Coloso", como se llamaba, entre su diseñadores estaban Alan M. Turing, diseñador de la Máquina Turing, quien había escapado de los Nazis unos años antes.

Era un computador capaz de descifrar los mensajes nazis generados por su contraparte, la máquina alemana "Enigma",

funcionaba con 2400 válvulas y 5 paneles de lectura óptica de cintas perforadas, con capacidad para imprimir resultados.

El Coloso tenía cinco procesadores, cada uno podría operar a 5,000 caracteres por segundo. Por usar registros especiales y un reloj interior, los procesadores podrían operar en paralelo (simultáneamente) que esta le daba al Coloso una rapidez promedio de 25,000 caracteres por segundo.

Esta rapidez alta era esencial en el esfuerzo del desciframiento de códigos durante la guerra. El plan del Coloso era quedar como información secreta hasta muchos años después de la guerra.

1.4.4.- Integrado Electrónico Numérico Y Calculadora (ENIAC).

En 1946 la primera computadora electrónica digital a grande escala llegó a ser operacional, usó un sistema de interruptores y enchufes montados en forma externa para programarlo. El instrumento fue construido por Presper Eckert Hijo y ohn Mauchly.

"La máquina norteamericana conocida como ENIAC (Integrado Electrónico Numérico y Calculadora) no tenía partes mecánicas, utilizaba bulbos (alrededor de 18 000). Era capaz de realizar cinco

mil operaciones por segundo y fue utilizada principalmente para resolver problemas de balística y aeronáutica. Su mayor mérito fue el de tener gran cantidad de componentes y trabajar de manera simultánea con ellos; sin embargo, era demasiado grande y se calentaba con mucha rapidez."[7]

La ENIAC requería una gran cantidad de electricidad. La leyenda cuenta que la ENIAC, construida en la Universidad de Pensilvania, bajaba las luces de Filadelfia siempre que se activaba. La imponente escala y las numerosas aplicaciones generales de la ENIAC señalaron el comienzo de la primera generación de computadoras.

1.5.- Período de 1950 – 1962.

Desde 1950 hasta 1962, un número de desarrollos avanzaron en tecnología de computadoras. Una vez que la tecnología electrónica ha sido aplicada a máquinas de computo, computadoras pudieron avanzar lejos de sus habilidades previas. Guiadas por el modelo de Turín para máquinas lógicas, estudiosos de las computadoras integraron lógica en sus máquinas, programadores fueron capaces de explotar estas utilidades mejor una vez que los primeros lenguajes de programación, fueron inventados.

---

[7] **TÉLLEZ VALDÉS, Julio.** Op. Cit. P. 9.

1.5.1.- Computadora Interactiva.

En 1950 la primera Computadora interactiva en tiempo real, fue completada por un plan de diseño en Estados Unidos. Conocida también como la Computadora del Torbellino, fue adoptada para proyectos en el desarrollo de un simulador de vuelo por la Marina de ese mismo país.

El Torbellino usó un tubo de rayo de cátodo y una pistola de la luz para proveer interactividad. Además se conectaba a una serie de radares y podría identificar un avión poco amistoso e interceptores a su posición proyectada.

Tenia un transistor más pequeños, más baratos y mucho menos calientes que las válvulas de vacío, los transistores desplazaron rápidamente a éstas en todos los aparatos electrónicos, los computadores entre otros. Esta sería el prototipo para una red de computadoras y sitios de radar como un elemento importante de la defensa aérea de EUA por un cuarto-siglo después de 1958.

1.5.2.- Computadora Universal Automática (UNIVAC).

En 1951 se entregó la primera computadora comercialmente

disponible al Escritorio del Censo por el Eckert Mauchly Corporación de la Computadora. El UNIVAC (Computadora Universal Automática) fue la primera computadora que no era un solo disponible para laboratorios.

"... Entre sus características principales encontramos el uso de la cinta magnética para la entrada y salida de datos, la capacidad de aceptar y procesar datos alfabéticos y numéricos, así como el uso del programa especial capaz de traducir programas en un lenguaje particular a lenguaje de máquina. Estas máquinas constituyen en la llamada primera generación de computadoras, que utilizaron bulbos de alto vacío como componentes básicos de sus circuitos internos. Como consecuencia, eran demasiado voluminosas, consumían mucha energía y producían calor; no fueron tan confiables como se había esperado, eran rápidas pero no lo suficiente y tenían capacidad de almacenamiento interno pero limitado."[8]

El UNIVAC abrió el primer paso hacia la futura comercialización y masificación de los computadores, además de marcar el comienzo de lo que se llama la primera generación de computadoras.

---

[8] TÉLLEZ VALDÉS, Julio. Op. Cit. P. 10.

1.6.- Período de 1963 – 1971.

Una vez que la primera minicomputadora fue construida en 1963, y luego la primera triunfante en los negocios la supercomputadora en 1964, la revolución de la computadora comenzó.

Con la creación de cables de fibra óptica, semiconductores, lásers y bases de datos relacionados, la barrera fue derribada para los programadores. No sería hasta doce años después cuando la computadora, llega a los hogares, como a continuación se describe.

1.6.1.- Minicomputadora.

En 1963 aparecieron en el mercado las primeras minicomputadoras de la tercera generación, cuya característica principal fue que utilizaron circuitos integrados monolíticos, que aumentaron su velocidad, su confiabilidad y disminuyeron su costo y tamaño.

El primer miniordenador comercialmente exitoso fue distribuido por Corporación del Equipo digital (DEC). El DEC PDP-8 fue sucesor del advenimiento de la minicomputación comercial por tener una Influencia significante en el desarrollo de secciones en la

ciencia de la informática universitaria.

La distribución de la Computadora 12-bit PDP-8 abrió las compuertas del comercio de miniordenador en otras computadoras.

1.6.2.- Sistema IBM 360.

En 1964 la familia de computadoras Sistema/ 360 fue lanzada por IBM. El Sistema/ 260 reemplazó transistores con circuito integrado, o lógica sólida, tecnología.

"Los circuitos son bloques de silicio en los que, por medio de técnicas de fotograbado y difusión, se integran elementos activos (transistores y diodos) pasivos. Este bloque se empaca en cápsulas terminales que permiten interconectarlos con otros elementos electrónicos, lo que facilita el armado y mantenimiento."[9]

La IBM 360, fue una de las primeras computadoras comerciales que usó circuitos integrados, podía realizar tanto análisis numéricos como administración ó procesamiento de archivos. Los clientes podían escalar sus sistemas 360 a modelos

---

[9] **FOURNIER, María de Lourdes.** Op,. Cit P. 27.

IBM de mayor tamaño y podían todavía correr sus programas actuales.

Con la aparición del IBM 360 marca el comienzo de la tercera generación de computadoras, en donde aparece la multiprogramación el teleproceso se empieza a generalizar el uso de minicomputadores en los negocios y se usan cada vez más los lenguajes de alto nivel.

1.6.3.- Supercomputadora.

En 1964 la primera supercomputadora a estar comercialmente disponible se envió por la Corporación de Datos de Mando. El CDC 6600 tenia varios datos devana bancos y estaba a quedar en la computadora más poderosa por muchos años, después de su desarrollo.

La característica principal de esta computadora fue que desarrollo circuitos integrados (pastillas de silicio) en las cuales se colocan miles de componentes electrónicos, en una integración en miniatura.

Las computadoras nuevamente se hicieron más pequeñas, más rápidas, desprendian menos calor y eran energéticamente más eficientes.

1.6.4.- Minicomputadora de 16-BIT.

En 1969, la primera minicomputadora de 16-bit fue distribuida por Data-General Corporation. La computadora, llamada la Nova, fue un mejoramiento en velocidad y poder. Por lo que muchos historiadores consideran a esta invención, como el inicio de la cuarta generación de computadoras.

Fue una de las primeras computadoras comerciales que usó circuitos integrados, podía realizar tanto análisis numéricos como administración ó procesamiento de archivos. Los clientes podían escalar sus sistemas 360 a modelos IBM de mayor tamaño y podían todavía correr sus programas actuales.

1.6.5.- Computadora Personal.

En 1971 se construyó la primera computadora personal y distribuido por John Blankenbaker. La computadora, llamada el Kenbak-1, tenía una capacidad de memoria de 256 bytes, desplegaba datos lentos y era tedioso programarlo, y además llego a introducir la revolución de las computadoras personales.

Tenia un tamaño mediano, y no era tan costosas como las grandes (llamadas también como mainframes que significa también, gran sistema), pero disponían de gran capacidad de

procesamiento.

1.7.- Período de 1972 – 1989.

Una vez que la PC fue llegando a los hogares, la revolución de PC comienza. La competencia de los mercados entre manufactureros como IBM y Apple Computer avanzaron rápidamente en el campo. Por primera vez la habilidad de cálculos de alta calidad, estaba en la casa de cientos miles de personas, en vez que solo algunos privilegiados. Las computadoras finalmente se convirtieron en herramienta de la gente común.

1.7.1.- Altair.

En el enero de 1975 Micro Instrumentation Telemetry Systems (MITS) introdujeron el Altair. Era una minicomputadora mas personal, barata, no tenia un teclado y además no poseía un aparato del almacenamiento de memoria, pero llevó el microprocesador 8-bit Intel 8080.

Fue el primer computador destinado a aficionados, los programas que empleaba debían ser ingresados instrucción por instrucción usando los interruptores del panel frontal.

1.7.2.- Computadoras Personales.

En 1977, la primera computadora personal ensamblada fue distribuida por Commodore, Apple Computer y Tandy. Después de unos años, el PC (computadora personal) había llegado a ser un pedazo de la vida personal de cada uno de sus usuarios, y aparecería pronto en bibliotecas públicas, escuelas, y lugares de negocio.

Son computadores de bajo costo, con las dimensiones de una máquina de escribir, pero tan potentes como los computadores del tamaño de una habitación que les habían precedido. Los computadores personales o PC (computadora personal), como se conocen actualmente son herramientas diarias para las personas.

1.7.3.- IBM PC e IBM PC-XT.

En 1981 la revolución de la computadora personal ganó impulso cuando IBM introdujo su primera computadora personal. La primera IBM PC, era un sistema basado de un floppy el cual usó el microprocesador 8088 de Intel.

Las unidades originales tenían pantallas de sólo texto, gráficos verdaderos eran una alternativa que llegó más tarde. Se

limitó memoria también, típicamente sólo 128K, o 256K de RAM. Más tarde lanzó el IBM PC/ XT, está era una máquina extendida que añadió una unidad de discos duros y gráficos. Llego a ser un equipo ligero, y paulatinamente se apodero de una sección importante del público consumidor.

1.7.4.- Procesamiento Paralelo.

En 1981 la primera computadora del proceso comercial paralela fue distribuida por BBN Computers Advanced, Inc. La computadora, llamada la "Mariposa", era capaz de asignarles a partes de un programa hasta 256 diferentes procesadores, en consecuencia de esto la velocidad del proceso y eficacia incrementan.

1.7.5.- Macintosh.

Ahora en la segunda mitad de la década de 1980, decenas de millones de computadoras personales se encuentran en las estaciones de trabajo de oficinas, fábricas, escuelas, hogares, hospitales, agencias de gobierno, bancos, tiendas, además de los laboratorios. Fue entonces en 1984 el primer Macintosh computadora personal fue distribuido por Apple Computer, Inc.

Era el sucesor de un modelo llamado "Lisa" (pero que no tuvo aceptación debido a su costo y escasa capacidad), en el que se introducía por primera vez el concepto de interfaz gráfica, la analogía del "escritorio" y un nuevo periférico: el "mouse" o ratón, como herramienta para controlar al computador.

1.7.6.- IBM PC-AT.

En 1984 IBM distribuido el BM PC-AT, la primera computadora usaba el chip microprocesador (chips de silicio sobre aislante) Intel 80286. La serie Intel 80x86 adelantó el poder del procesador y flexibilidad de las computadoras IBM. Otra mejora de ello, fue que incluyeron un teclado extendido, un mejor suministro de energía y una caja del sistema más grande.

1.8.- Período de 1990 – Actualidad.

Por este tiempo, las computadoras han sido adaptadas a casi cada aspecto de la vida moderna. Desde controlar motores de automóviles hasta comprar en los supermercados, cada vez máquinas más rápidas y nuevas, son creadas. Esto hacen que las casas de programas tomen ventaja de estas nuevas máquinas, aunque estas tecnologías son las últimas máquinas viejas del futuro.

A continuación describo algunas computadoras de los años Noventa hasta la actualidad.

1.8.1.- Computadoras Ópticas.

En 1990 se construyó el primer procesador óptico en At&T Laboratorios de Bell. El procesador emplea pequeños, láseres semi-conductores para llevar información y guardar circuitos ópticos y procesan la información.

Usan luz, en lugar de electricidad, para llevar datos podía teóricamente hacer de las computadoras miles de veces más rápido. Era capaz de controlar el flujo de corriente eléctrica desplazando un átomo de xenón entre dos diminutos electrodos.

1.8.2.- Las Computadoras Modernas.

Una variedad de estilos de chasis está en uso hoy. Los principales son el chasis de mesa, torre, mini torre, laptop, notebook, y palmtop. Ellos sirven de soporte a los componentes principales de las computadoras. Estos incluyen, la fuente de poder, tarjeta madre, unidades, etc. El tamaño y estilo del chasis depende del uso del sistema. Laptops, notebooks, y palmtops proveen diferentes grados de portabilidad, pero sacrifican expandibilidad.

Un sistema laptop es más pequeño, portátil, con un monitor de bisagra y un teclado integrado. Ellos normalmente pesan entre 12 a 14 libras. Los sistemas notebooks aún son más pequeños. Pesan entre 4 a 7 libras. Un sistema palmtop es la más pequeña de todas, pesando menos que 2 libras. Sistemas palmtops tienen teclado y monitor integrado.

CAPITULO SEGUNDO

CONCEPTOS FUNDAMENTALES

CAPITULO II

CONCEPTOS FUNDAMENTALES.

No siendo el objeto de este trabajo el análisis profundo de los términos en informática, ya que sería pretencioso dados nuestros exiguos conocimientos, nos concretaríamos únicamente a realizar una exposición de elementos en la materia.

Luego entonces, sólo tocaremos algunos conceptos fundamentales en informática, acudiendo como a lo largo de todo el presente trabajo a las valiosísimas ideas de autores versados en la materia y exponiendo una sencilla opinión al respecto.

2.1.-Cibernética.

Antes de analizar a la informática propiamente dicha es menester, hacer una breve alusión a la ciencia de donde se desprende.

La cibernética proviene del vocablo griego "kybernes", que indica arte del gobierno, arte de guiar, fue originalmente la ciencia de los mecanismos del control y las comunicaciones, tanto en los seres vivos como en las máquinas.

Hoy es una hiperciencia que estudia el cerebro humano e interviene decisivamente en el diseño de los robots que exploran otros mundos.

Ahora bien, Grun Ernesto define a la Cibernética como :

> "...La inquisición interdisciplinaria hacia la naturaleza y base física de la inteligencia humana, con el propósito, de reproducirla en forma sintética..."[10]

Un objeto de estudio característico de dicha materia es el problema cerebro-mente. Como una ciencia híbrida surgida de las matemáticas y la neurofisiología, es una de las primeras ciencias abiertas del Siglo XX, fundacional en diversos campos: teoría del conocimiento, inteligencia artificial, bioelectrónica, robótica y computación, siendo este nuestro tema a desarrollar.

2.2.- La Computadora.

La Computación está inmersa en prácticamente todos los

[10] **GRUN, Ernesto.** Una Visión Sistémica y Cibernética del Derecho Ed. Abeledo Perrot. Argentina.1995. P. 35.

aspectos de nuestra vida, tanto en una forma indirecta como directa. Ejemplos los podemos encontrar tanto en la vida diaria, como en las áreas científicas y tecnológicas, teniendo la computadora no sólo como herramienta para resolver problemas, sino como medio de control, aprendizaje y comunicación.

Tim Duff, en su obra la Introducción a la Informática define a la computación de la siguiente forma:

> "La computación es un sistema electrónico de uso general que realiza operaciones aritmética-lógicos a gran velocidad de acuerdo con instrucciones internas, que se ejecutan sin intervención humana."[11]

Además, tiene la capacidad de aceptar y almacenar datos de entrada, procesarlos y producir resultados de salida automáticamente, su función principal es procesar datos.

2.3.- Informática.

La informática como tal, ha sido comúnmente considerada como una ciencia particular integrada a la cibernética, parte del

[11] **DUFF, Tim**. Introducción a la Informática. Ed, Ibero América. México. P. 5.

estudio de las computadoras, de sus principios básicos y de su utilización, comprende materia tales como programación, estructura de la información, ingeniería del software, lenguajes de programación, hardware, arquitectura de las computadoras entre otras.

En sentido general, "Es una ciencia del tratamiento racional, particularmente por máquinas automáticas, de la información, considerada como el soporte de conocimientos humanos y de comunicaciones en los aspectos técnico, económico y social."[12]

Dicha materia, concierne a todos los sectores de la vida, económica y social en forma destacada. Esta expansión hace nacer problemas jurídicos nuevos de carácter

Ante esto he considerado que el término informática, es la ciencia del tratamiento automático, o automatizado de la información, primordialmente mediante las computadoras

2.4.- Derecho Informático (Derecho a la Alta Tecnología).

El Derecho informático o Derecho a la Alta Tecnología, como término más genérico, tiene a la informática como objeto de estudio,

[12] **DICCIONARIO DE INFORMÁTICA** . SIN AUTOR. Ed. Acento. Col. Flash. P. 171. México 2002.

aplicando a la mismas reglas jurídicas, siendo una rama de las ciencias jurídicas que contempla la informática como instrumentos.

La clasificación la encontramos en la función de lo anterior que obedece a dos vertientes informática jurídica y derecho a la informática.

Dentro de la informática jurídica, la informática es un instrumento al servicio del Derecho. Se la clasifica en informática documental, orientada a la compilación y búsqueda de documentos jurídicos, informática jurídica administrativa o de gestión, concebida como ayuda a los procedimientos administrativos y jurídicos rutinarios y por último la informática jurídica decisional, que busca suplantar la toma de decisión humana a través del software adecuado.

Mientras que el Derecho a la Informática es el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática.

2.5.- Delitos Informáticos.

El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figurar típicas de carácter tradicional, tales como robos o hurto, fraudes,

falsificaciones, perjuicios, estafa, sabotaje, delitos cometidos a través del Internet etcétera. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho.

A nivel internacional se considera que no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aún cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas.

Por lo que se refiere a las definiciones que se han intentado dar en México, cabe destacar que Julio Téllez Valdés señala que :

"...No es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los Códigos Penales, lo cual en nuestro país, al igual que en otros muchos no ha sido objeto de tipificación aún...".[13]

[13] **Téllez Valdez. Julio.** Op. Cit. P. 103-104.

Para Carlos Sarzana, en su obra Criminalista e tecnología, los crímenes por computadora comprenden:

> "...Cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, como mero símbolo...".[14]

Rafael Fernández Calvo define al delito informático como:

> "...La realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos..".[15]

Julio Téllez Valdés conceptualiza lo siguiente:

> "... A los delitos informáticos en forma típica y

---

[14] **SARZANA, Carlos**. "Criminalitŕ e tecnologia" en Computers Crime. Rassagna Penitenziaria e Criminología. Nos. 1-2 Año 1. Roma, Italia. 1988. P.53.

[15] **FERNÁNDEZ CALVO, Rafael**. El tratamiento de llamado delito informático en el proyecto de ley Orgánico del Código Penal: reflexiones y propuestas de la CLI (Comisión de libertades e informática" en Informática y Derecho. España. 1988. P.150.

atípica, entendiendo por la primera a las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin y por las segundas actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".[16]

Por otra parte, debe mencionarse que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa la computadora, tales como delitos informáticos, delitos cibernéticos, delitos electrónicos, delitos relacionados con las computadoras, crímenes por computadora, delincuencia relacionada con el ordenador.

En este orden de ideas, en el presente trabajo se entenderán como Delitos Informáticos todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático.

2.5.1 Sujeto Activo.

Las personas que cometen los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes.

---

[16] **Téllez Valdez. Julio.** Op. Cit. P. 104.

Esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación labora se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados., aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Para algunos autores, el sujeto activo de estos delitos se encuentra conformado por un grupo de personas con una inteligencia y educación que superan el común, con vastos conocimientos informáticos.

La sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se consideran a sí mismos respetables.

Otra coincidencia que tiene estos tipos de delitos es que generalmente son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

Aunque es necesario señalar que estas aseveraciones pueden y deben ser objeto de un estudio más profundo, que dada la naturaleza de este tema, me veo en la necesidad de limitar y clasificar a los delincuentes informáticos de la siguiente forma:

2.5.1.1.- Hacker.

Es un Individuo que sin derecho penetra un sistema informático sólo por gusto o para probar sus habilidades, usualmente no tiene fines delictivos graves este tipo de intrusión. Sin embargo, ellos mismos se definen como:

1. Una persona que disfruta el explorar detalles de sistemas programables y cómo maximizar sus capacidades;

2. Alguien que programa entusiastamente;

3. Una persona que es buena programando rápidamente;

4. Un experto en un programa particular;

5. De manera despectiva, un intruso malicioso que trata de descubrir información sensible merodeando.

2.5.1.2.- Crackers.

Derivado del hacking. Este término fue acuñado por los

hackers para defenderse del mal uso periodístico del término hacker, el término cracker refleja la gran repulsión a los actos de robo y vandalismo perpetrados por los círculos de criminales conocidos como crackers.

Schwartau Winn, define a los crackers en la siguiente forma:

> "Es una persona que sin derecho penetra un sistema informático con el fin de robar o destruir información valiosa realizar transacciones ilícitas, o impedir el buen funcionamiento de redes informáticas o computadoras".[17]

Básicamente es alguien que viola la seguridad en un sistema, dicha definición presenta dos vertientes, el que se cuela en un sistema informático y roba información o produce destrozos en el mismo, y el que se dedica a desproteger todo tipo de programas, tanto de versiones de software para hacerlas plenamente operativas como de programas completos comerciales que presentan protecciones anticopia.

---

[17] **SCHWARTAU Winn** . "Cybershock". Surviving, Hackers, Phreakers, identy Thieves, Interten terrorists and weapon of disruption. Computer world Books. 2002. P. 66.

2.5.1.3.- Cybergangs (Ciberpandillas).

Son grupos de hackers o extremistas, se reúnen para cometer o planear delitos, para expresar ideas racistas, discriminatorias o xenofóbicas en contra de personas, organismos y en contra del gobierno.

2.5.1.4.- Cybergrafitti - Defacements - Web Hacks.

Es el tipo de hacking más común. Esta práctica es el equivalente del graffiti callejero que todos conocemos pero llevada a cabo en línea, es por eso que algunos expertos en seguridad informática han bautizado a los individuos que realizan este ilícito como ciber-cholos.

Ahora bien Schwartau Winn, los define de la siguiente manera:

> "Son hackers que penetran sitios web sin derecho para modificar su contenido, desplegando imágenes obscenas, amenazas, mensajes ridiculizantes, burlas, etc."[18]

[18] **SCHWARTAU Winn.** Op. Cit. P. 67.

2.5.1.5.- Phreaker.

Es aquella persona que realiza una actividad parecida a los crackers, aunque ésta la realiza por medio de líneas telefónicas y con o sin el auxilio de un equipo de cómputo. Es especialista en telefonía, empleando sus conocimientos para poder utilizar las telecomunicaciones gratuitamente.

2.5.1.6.- Piratas.

Muchas veces se confunden a los hackers con los piratas informáticos. La diferencia entre unos y otros es realmente abismal, y la culpa de este gran error lo tienen los medios de comunicación. El problema reside en que la mayoría de las veces los periodistas que escriben acerca de las actividades de los hackers desconocen totalmente el tema.

El mencionado autor lo conceptualiza en la forma siguiente:

> "Un pirata informático es quien hace copias de software, para luego comercializar con ellas. Si entra en un sistema, es simplemente por que hay algún algún tipo de software que le interesa. No dispone de unos conocimientos tan amplios como un hacker, sus conocimientos se limitan a la copia de

discos y romper algunos sistemas de seguridad mínima."[19]

2.5.1.7.- Lammers.

Son simples aficionados. No son novatos, porque no desean aprender. Disponen de algunos conocimientos sobre hacking, pero no saben lo que están haciendo realmente.

Estos personajes son los típicos que entran en un canal de hackers, y piden a voces un fichero con contraseñas y hosts. No disfrutan con la informática, ni aprendiendo cosas nuevas, solo quieren aprender lo justo para satisfacer sus intereses o bien para hacer creer a sus amigos que es un genio.

La mayoría de las veces utilizan sus precarios conocimientos indebidamente, y acaban con sus propias maquinas o con otras de la red.

2.1.5.8.- Virucker.

Es aquella persona que ingresa dolosamente o de un tercero, a un sistema informático ajeno, con el objetivo de introducir "virus" y

[19] **SCHWARTAU Winn**. Op. Cit. P. 64.

destruir, alterar o inutilizar la información contenida. Existen dos tipos de virus, los benignos que molestan pero no dañan, y los malignos que destruyen información o impiden trabajar.

Suelen tener capacidad para instalarse en un sistema informático y contagiar otros programas e, inclusive, a otros ordenadores a través del intercambio de soportes magnéticos, como disquetes o por enlace entre ordenadores.

2.5.2.- Sujeto Pasivo.

En primer término tenemos que distinguir que sujeto pasivo o víctima del delito, llegando ser el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros.

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.

Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.

2.6.- Criptología.

La criptología, etimológicamente significa esconder la escritura, es una disciplina matemática que en la era de la supercarretera de la información, se ha convertido en herramienta fundamental para la realización de todo tipo de operaciones económicas, industriales, políticas y financieras de muchos países, contra una nueva clase de delincuentes surgidos a la sombra de este avance tecnológico, como son los Hackers y Crackers informáticos o piratas de la información

Caballero Pino conceptualiza a la criptologia como:

> "...El estudio y práctica de los sistemas de descifrado destinados a ocultar el contenido de mensajes enviados, entre dos partes: emisor

y receptor..."[20]

La criptología se divide en dos: la criptografía, que se dedica a diseñar y estudiar sistemas de cifrado, y el criptoanálisis, que se dedica al estudio del descifrado no autorizado de mensajes (es decir, a "romper" sistemas criptográficos).

En la actualidad, hay muchos países que aunque en su territorio nacional permiten el uso de la criptología, desean que estos programas incluyan una puerta trasera (backdoor) o procedimiento parecido para poder intervenir el mensaje cuando así lo consideren oportuno. Es el caso del famoso chip de depósito de claves o Chip clipper (dispositivo de alcantarillado), para descifrar conversaciones telefónicas (los dos teléfonos participantes en una conversación deben tenerlo).

2.7.- Programas de Computo.

En sentido general, los programas de computo "Son un conjunto de programas, procesos y reglas eventualmente de documentación relativas al funcionamiento de un conjunto de un tratamiento de la información."[21]

---

[20] **CABALLERO, Pino.** Seguridad Informática Técnicas Criptográficas. Ed. Grupo Alfaomega México.1997. P. 12.
[21] **DICCIONARIO DE INFORMÁTICA.** Op. Cit. P. 236

La Ley Federal de Derechos de Autor de México Vigente define a los dichos programas como la expresión original, en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora realice una tarea o función específica; la protección incluye tanto los programas operativos como aplicativos y registra como única excepción los que tengan por objeto causar efectos nocivos a otros programas o equipos. (arts. 101 y 102 de la Ley Federal de Derechos de Autor).

Los programas de cómputo, conforme a ley citada son por definición, "instrumentos técnicos", no obras literarias; y lo que se protege son las instrucciones. Dice claro la definición, por otra parte, que los programas son un complemento de la computadora, una parte desmontable de la misma, que hace posible su utilización para múltiples usos. La computadora puede aceptar muchos programas y el usuario decidirá cuál es el que resulta más útil para lograr sus objetivos.

2.8.- Base de Datos.

La base de datos, es un archivo de computadora que tiene una estructura regular formada por registros, que a su vez están formados por campos, en los sistemas de archivo de papel, análogos a los de computadora, cada tarjeta corresponde a un

registro, y los campos son los elementos de información como nombre, dirección, fecha, etc.

Ahora bien, la base de datos son por definición "...Cualquier conjunto de datos organizados para su almacenamiento en la memoria de un ordenador o computadora, diseñado para facilitar su mantenimiento y acceso de una forma estándar."[22]

2.9.- Señales de Satélites.

Las señales de los satélites de comunicación, se emplean para retransmitir alrededor del mundo emisiones telefónicas o de televisión, enviadas desde una estación terrestre al satélite, donde se amplifican y se retransmiten, una vez reforzada, a otra estación terrestre.

Las señales de satélites son por definición "Señales sonoras o visuales que emiten las empresas que comunican obras, sonidos, o sonidos con imágenes, susceptibles de ser recibidas por numerosos receptores." [23]

---

[22] **ENCICLOPEDIA ENCARTA MICROSOFT 2003.**
[23] **ENCICLOPEDIA EVEREST DE LAS CIENCIAS**. Ed. EVerest., S. A. México. P.p. 12-13. 1995.

CAPITULO III

ENFOQUE PERSPECTIVO DEL INTERNET EN LA ACTUALIDAD A NIVEL NACIONAL E INTERNACIONAL

CAPITULO III

ENFOQUE PERSPECTIVO DEL INTERNET EN LA ACTUALIDAD A NIVEL NACIONAL E INTERNACIONAL.

Para adentrarnos al estudio de los llamados Delitos Informáticos, o en sus diferentes denominaciones como delitos cibernéticos, delitos relacionados con las computadoras, crímenes por computadora o delincuencia relacionada con el ordenador, etc, entraremos al conocimiento y manejo de lo que es la computadora en nivel operacional y de estructuración, (ya que ésta como se verá más adelante puede ser objeto o fin de dichos delitos), así como la noción de diferentes conceptos relacionados con el Internet, esto es para poder tener un mejor entendimiento del tema.

3.1 Antecedentes del Internet.

El Internet de hoy es el fruto de proyectos de investigación y colaboración entre Universidades norteamericanas por los años sesenta. Estos proyectos tuvieron un fuerte apoyo económico de empresas y entidades gubernamentales de los Estados Unidos.

Así, Internet inicialmente fue una red académica orientada a la colaboración e investigación entre las distintas Universidades que

conformaban esta red. Con el tiempo esta red académica evolucionó hasta lo que hoy es Internet, el medio de comunicación más masivo del planeta.

El inicio del Internet, se remonta a 1969, cuando la Agencia de Proyectos de Investigación Avanzada en Estados Unidos, conocida por sus siglas, "ARPA", desarrolló ARPANET, una especie de red que unía redes de computo del ejercito y de laboratorios universitarios que hacían investigaciones sobre la defensa.

Esta red, permitió primero a los investigadores de Estados Unidos acceder y usar directamente supercomputadoras localizadas en algunas universidades y laboratorios clave; después, compartir archivos y enviar correspondencia electrónica.

A finales de 1970 se crearon redes cooperativas descentralizadas, como UUCP, una red de comunicación mundial basada en UNIX y USENET (red de usuarios), la cual daba servicio a la comunidad universitaria y más adelante a algunas organizaciones comerciales.

En 1980, las redes más coordinadas, como CSNET (red de ciencias de cómputo), y BITNET, empezaron a proporcionar redes de alcance nacional, a las comunidades académicas y de investigación, las cuales hicieron conexiones especiales que permitieron intercambiar información entre las diferentes comunidades.

En 1986, se creó la NSFNET (red de la Fundación Nacional de Ciencias), la cual unió en cinco macrocentros de computo a investigadores de diferentes Estados de Norte América, de este modo, esta red se expandió con gran rapidez, conectando redes académicas a más centro de investigación, remplazando así a ARPANET en el trabajo de redes de investigación.

ARPANET se da de baja en marzo de 1990 y CSNET deja de existir en 1991, cediendo su lugar a INTERNET. Esta red se diseñó para una serie descentralizada y autónoma de uniones de redes de computo, con la capacidad de transmitir comunicaciones rápidamente sin el control de persona o empresa comercial alguna y con la habilidad automática de recabar datos, si en una o más uniones individuales se dañan o están por alguna razón inaccesibles.

Actualmente el Internet es como herramienta educativa y de investigación científica ha crecido aceleradamente debido a la ventaja que representa el poder acceder a grandes bases de datos, la capacidad de compartir información con otras personas y facilita la coordinación de grupos de trabajo.

3.2. Concepto de Internet.

El Internet ha puesto una revolución sin precedentes en el mundo de la informática y de las comunicaciones. Los inventos del

telégrafo, teléfono, radio y ordenador sentaron las bases para esta integración de capacidades nunca antes vivida. Internet es a la vez una oportunidad de difusión mundial, un mecanismo de propagación de la información y un medio de colaboración e interacción entre los individuos y sus ordenadores independientemente de su localización geográfica.

En términos generales, Internet se ha convertido en un polémico escenario de contrastes en donde todo es posible: desde encontrar información de contenido invaluable, de alcances insospechados en el ámbito de la cultura, la ciencia y el desarrollo personal, hasta caer en el terreno del engaño, la estafa o la corrupción de menores.

Barry M. Leiner, define al Internet como:

> "...La interconexión de redes informáticas que permite a las computadoras conectadas comunicarse directamente. El término suele referirse a una interconexión en particular, de carácter planetario y abierto al público, que conecta redes informáticas de organismos oficiales, educativos y empresariales...".[24]

---

[24] **BARRY M. Leiner, VINTON G. Cerf, DAVID D. Clark,** y **KLEINROCK Leonard**, Una breve historia de Internet, 13ª ed. Ed. Planeta, 1999. P. 18.

Ante esto he considerado que el Internet es una red gigante de intercambio de información que une a personas, instituciones, compañías y gobiernos alrededor del mundo, de manera casi instantánea, a través del cual es posible comunicarse, con un solo individuo, con un grupo amplio de personas interesadas en un tema específico o con el mundo en general.

3.3. Antecedentes del Internet en México.

Nuestro país fue el primer país latinoamericano en conectarse a Internet, lo cual ocurrió a finales de los 0chenta, exactamente en febrero de 1989, a través de los medios de acceso e interconexión de teléfonos de México (TELMEX).

Los primeros enlaces de Internet en el país, que tuvieron fines exclusivamente académicos, por cierto, se establecieron en el Instituto Tecnológico de Estudios Superiores de Monterrey, (TEC DE MONTERREY) el Instituto Politécnico Nacional(IPN), la Universidad de Guadalajara (U. DE G) y la Universidad de las Américas en Puebla (UDLA).

En este periodo el uso internacional del Internet origina una normativa no escrita, seguida por los usuarios de nuestro país, el cual se basaba en usos, sin reglas formales, fundada más bien en consideraciones de tipo ético entre la comunidad académica. En 1994 se incorporan instituciones comerciales en nuestro país,

dando lugar a una visión diferente del fenómeno de Internet.

La era de la información, impone en nuestro país, al igual que en el mundo globalizado, nuevas formas de organización, en los negocios, el mundo de la academia, los gobiernos y, cada vez más, en todas las actividades habituales a pesar de que la cultura de la informática y de la información en México se encuentran aún en sus inicios, hoy en día la tecnología de la información constituye para muchas empresas y universidades nacionales un instrumento insustituible para la realización de trabajos específicos.

"En marzo del 2002, la empresa Cyberatlas dio a conocer las estadísticas en cuanto a cantidad de usuarios con acceso a Internet".[25] México ocupo el número décimo quinto con 2 300 000 personas que cuentan con Internet. Como se muestra en la presente grafica.

TABLA. RELACIÓN DE PAÍSES CON ACCESO A INTERNET

No.	País	No. de usuarios
1.	Estados Unidos	149 000 000
2.	China	33 700 000

[25] http://cyberatlas.internet.com/ **THE WORLD'S ONLINE POPULATIONS**. Relación de países con acceso a Internet. Miércoles 10/04/03. 13:15 p.m.

3.	Reino Unido	33 000 000
4.	Alemania	26 000 000
5.	Japón	22 000 000
6.	Corea del Sur	16 700 000
7.	Canadá	14 200 000
8.	Francia	11 000 000
9.	Italia	11 000 000
10.	Rusia	7 500 000
11.	España	7 000 000
12.	Holanda	6 800 000
13.	Taiwan	6 400 000
14.	Brasil	6 100 000
15.	India	5 000 000
16.	Polonia	4 900 000
17.	Tailandia	4 600 000
18.	Suecia	4 500 000
19.	Hong Kong	3 900 000
20.	Turquía	3 700 000
21.	Suiza	3 400 000
22.	Portugal	3 055 000
23.	Austria	2 700 000

24.	Bélgica	2 700 000
25.	México	2 300 000
26.	República Checa	2 200 000

Los servicios mas importantes que brinda el Internet en nuestro país, son los siguientes:

3.3.1.- Correo Electrónico.

Es el servicio de mayor uso, de mayor tráfico y, por lo tanto, de mayor importancia para el surgimiento, en la actualidad, de diversas relaciones contractuales. Permite escribir y enviar mensajes a una persona o grupo de personas conectadas a la red. El correo electrónico, hace ver al correo y el telégrafo un medio arcaico de información.

3.3.2.- Transferencia de Archivos.

A través de ello, se permite transferir archivos, los cuales pueden ser de texto, gráficas, hojas de cálculo, programas, sonido y vídeo.

3.3.3.- Acceso Remoto a Recursos de Computo por Interconexión.

Es una herramienta interactiva que permite introducirse, desde una computadora en casa o en la oficina, a sistemas, programas y aplicaciones disponibles en otra computadora, generalmente ubicada a gran distancia y con gran capacidad.

3.3.4.- Word Wide Web.

Es el servicio más nuevo y popular de Internet, caracterizado por la interconexión de sistemas a través del hipertexto, por medio del cual pueden transmitirse textos, gráficas, animaciones, imágenes y sonido. Se le considera un elemento importante de mercadotecnia.

3.3.5.- Grupos de Discusión.

Son grupos de personas que se reúnen a través de foros donde se enfocan a analizar básicamente a diversos temas, en la actualidad, como es la pobreza, los conflictos bélicos de hoy en día, los problemas financieros de los países tercer mundistas, y problemas que afectan a su misma comunidad, entre otros. Estos

grupos contienden y alegan razones contra el parecer de otro.

3.3.6.- Comunicación en Tiempo Real.

Es lo que conocemos como el Chat, consiste en la posibilidad de establecer diálogos inmediatos en tiempo real, a través de Internet, permitiendo a dos o más personas dialogar simultáneamente por escrito, sin importar la distancia geográfica.

Esta forma de comunicación es análoga a la línea de teléfono, sólo que emplea el teclado o monitor en lugar del auricular.

3.4. Practicas ilícitas cometidas en el Internet.

En los albores del nuevo milenio, podríamos decir que el siglo XXI ya ha comenzado con la llamada revolución digital, la cual ha tomado forma mediante un complejo y laberíntico entramado de cables, satélites, redes, computadoras, televisores e impulsos electrónicos que constituyen la infraestructura de la red.

Esta revolución, que encuentra en Internet su máxima expresión, es posible gracias al fenómeno de la convergencia, es decir, en el uso combinado de las computadoras y las redes de

comunicación. Los efectos de semejante transformación ya se están haciendo sentir en la ciencia, economía, la política, la sociedad, la cultura, la educación y entretenimiento. La forma en que nos interrelacionamos con los demás está siendo socavada por nuevas prácticas (compras on-line, chats, e-mail, educación a distancia, foros de discusión, etcétera) y ya nadie puede ser capaz de predecir exactamente cuán profundos serán los cambios. Los que sí parece ser notorio es que el cambio debe ocurrir simultáneamente en todos los ámbitos a fin de lograr un proceso de transición armónico.

En esta era digital o de la informática, infinidad de instituciones, normas, leyes, costumbres, formas de pensar y de relacionarse resultan inadecuadas e inapropiadas y necesitan ser revisadas y actualizadas en forma urgente. Además de todos los beneficios que la revolución digital conlleva, que la red pueda ser también concebido como un ámbito propicio para la realización de conductas ilícitas. A partir de la existencia de nuevas formas de operar con la tecnología delitos que no son nuevos, y ya existían desde mucho antes de la aparición de la informática, han planteado serios interrogantes que nuestro derecho positivo parece no saber cómo resolver.

Cualquiera de nosotros puede ser víctima de delitos, tanto en el mundo real, por llamarlo de alguna manera, como del "virtual". Sin embargo, parecería que las conductas ilícitas realizadas en éste último ámbito gozan de cierta impunidad. Ciertas conductas como la destrucción de base de datos personales, el hurto o el fraude

informático pueden resultar impunes en virtud de la falta de adecuación de la normativa vigente a las nuevas situaciones.

El principio de legalidad expresado en la máxima "nullum crimen nulla poena sine lege" el que establece que no hay delito ni pena sin ley penal anterior. En el orden penal la ley debe contener la descripción precisa de las acciones delictuosas, únicas conductas susceptibles de ser penadas.

Caso contrario, se estaría sancionando como delitos hechos no descriptos en la ley, con motivo de una extensión extralegal del ilícito penal y violando garantías constitucionales, como la que prescribe la analogía en materia penal, entendida ésta como la aplicación de la ley a un caso similar al legislado pero no comprendido en su texto.

Así pues, la proliferación de conductas inadecuadas que no encuentran un castigo adecuado demanda una mayor y más rápida actividad por parte de los legisladores. Esta es la mejor solución si queremos contar con un sistema jurídico seguro, que no de lugar a soluciones injustas y castigos no previstos expresamente por la ley. Son precisos y urgentes acuerdos internacionales a fin de armonizar criterios y evitar incompatibilidades entre distintos sistemas legales. El anquilosado ordenamiento jurídico se nos presenta como un aparato demasiado "pesado", lento y obsoleto, como para seguir el desenfrenado e imparable ritmo impuesto por el desarrollo de las tecnologías y hacer frente a los desafíos planteados por la

revolución digital.

3.5. Delitos Típicos que pueden trasladarse a la Red del Internet

Al hablar de delitos convencionales, nos referimos a aquellos que tradicionalmente se han venido dando en la vida real, sin el empleo de medios informáticos y que con la irrupción de las autopistas de la información se ha producido también en el ciberespacio.

Por mencionar algunos delitos, que serán descritos posteriormente en otro capítulo, pueden ser tanto el robo, el espionaje a través de un acceso no autorizado a sistemas informáticos gubernamentales e interceptación de correo electrónico del servicio secreto, o el espionaje industrial, el terrorismo mediante la existencia de hosts que ocultan la identidad del remitente, convirtiendo el mensaje en anónimo, siendo aprovechado por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional, el propio narcotráfico ya que se ha utilizado a la red para la transmisión de fórmulas para la fabricación de estupefacientes, para el bloqueo de dinero y para la coordinación de entregas y recogidas; así como más delitos como tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

Una de las formas para tratar de establecer la incidencia delictiva en materia de ilícitos informáticos ha sido el uso de encuestas. "Las siguientes estimaciones corresponden a un diagnóstico de seguridad de delitos por computadoras realizado en 1999 en los Estados Unidos de América por el Instituto Nacional Computacional conjuntamente con el FBI."[26] Del 100% de empresas que contestaron se tiene que:

a. 14% reportó ser víctima de fraude financiero.

b. 19% experimentó sabotaje en redes de datos.

c. 26% mencionó robo de información de su propiedad.

d. 30% reportó penetración por hackers externos.

e. 32% reportó los incidentes a las autoridades de justicia.

f. 32% reportó negación de servicios por ataques masivos.

g. Del 51% de empresas que reconocieron sus pérdidas solo el 31% pudo establecer el monto del daño.

h. 55% reportó accesos no autorizados de empleados.

i. 57% reportó intrusión en conexiones de Internet.

---

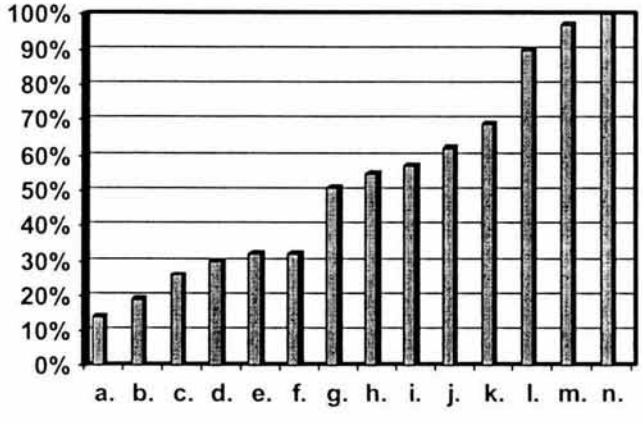
[26] http://www.alertra.com/ "ALERTRA WEB SITE MONITORING." Get Notified Anytime Your Website Goes Down!. Miércoles 30/04/03 21:30 p.m

j. 62% sufrieron violaciones a la seguridad informática.

k. 69% reportó pérdida y robo de laptops.

l. 90% tuvo incidentes de contaminación por virus.

m. 97% reportó abuso interno de privilegios de Internet.



Las pérdidas estimadas en 3 años consecutivos superaron los 100 millones de dólares.

CAPITULO IV

DERECHO COMPARADO Y MARCO JURÍDICO NACIONAL EN LOS DELITOS INFORMÁTICOS.

CAPITULO IV

DERECHO COMPARADO Y MARCO JURÍDICO NACIONAL EN LOS DELITOS INFORMÁTICOS.

En México existe legislación que tipifique el delito informático, que si bien es cierto tiene defectos y muchos puntos de mejora, sirve al menos como un inicio para protegernos contra ciertas actividades informáticas ilícitas.

Siendo la informática una actividad que en gran proporción se desarrolla en el campo internacional y, en virtud de que nuestro tema a estudio constituye un gran problema en la actualidad, conviene hacer una breve incursión en los ordenamientos de algunos países y de la legislación mexicana actualmente.

4.1 Análisis de la Legislación de otros Países sobre Delitos Informáticos.

Pocos son los países que disponen de una legislación adecuada para enfrentarse con el problema sobre el particular, sin embargo con objeto de que se tomen en cuenta las medidas adoptadas por ciertos países, a continuación se presenta los siguientes casos particulares:

4.1.1.- Alemania.

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

- Espionaje de datos.
- Estafa informática.
- Falsificación de datos probatorios 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 en este tipo de delitos.

- 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, causación del error y disposición patrimonial, llegando afectar a particulares, al gobierno y sistemas financieros.

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.

En opinión de estudiosos de la materia, el legislador Alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos, o Japón.

De esta forma, se menciona que no sólo ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos, aunque tenga lugar de forma cualificada.

4.1.2.- Chile.

En Chile mediante la ley 19.223, han sido tipificadas figuras penales relativas a la informática. Este país es uno de los únicos en América del Sur que ha actualizado su legislación en la materia que estamos estudiando.

El artículo 1º establece que el que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o sus componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio o máximo que es de 541 días a 5 años de presidio. Si como consecuencia de estas conductas afectaren los datos de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada de 5 años a 541 días de presidio en su grado máximo. A su vez el artículo 3º de la referida ley sanciona al que maliciosamente altere, dañe, o destruya los datos contenidos en un sistema de tratamiento de información, con presidio menor en su grado medio."[27]

El artículo 1º pretende cubrir cualquier nivel de daño tanto el hardware , como el software, incluyendo los datos almacenados en el sistema. Principalmente apunta a actos, directos que perjudiquen a alguna institución , pero también afectaría a los creadores de un virus. El artículo 3º en cambio es claramente destinado a los

[27] **Ley nº 19.223**, Relativa a Delitos Informáticos. Ed. Jurídica de Chile. Santiago, Chile . 1999.

fabricantes de virus, aunque no los nombre especificamente, ya que también castiga a quienes puedan causar daño por medios que no sean virus.

4.1.3.- Estados Unidos.

En los Estados Unidos, todos los Estados tienen leyes especificas de delitos informáticos. En 1986 se sanciono la primera ley Federal de Delitos Informáticos, denominada Fraude y Abuso Informático. Posteriormente en 1994 se adopto la Ley Federal de Abuso Informático que modifico la Ley de Fraude y Abuso Informático de 1986.

No fue hasta el 3 de octubre de 1996, en lo enmendado en la sección 1030, se sanciona el fraude y las actividades relacionadas con la conexión de computadoras" donde se describe principalmente lo siguiente:

"Tiene acceso intencionalmente a una computadora sin la autorización o excede el acceso autorizado, y de tal modo obtiene:

I. La información contenida en un expediente financiero de

una institución financiera, o de un emisor de la tarjeta información de cualquier departamento o agencia de los Estados Unidos; o

II. Información de cualquier computadora protegida por un código de seguridad, si la conducta implicó una comunicación de un estado a otro o extranjero;

III. Afecte a un particular

IV. Afecte a los sistemas bancarios

El castigo para una ofensa será una multa o encarcelamiento de diez o más de veinte años."[28]

En el 2002 se creo la enmienda de condenar pautas referentes a ciertos Delitos Informáticos. Citando a esta sección como el realce de la seguridad del Cyber 2002, estableciendo la divulgación de accesos, la buena fe de excepción, la publicidad de Internet en los dispositivos legales, ayuda del abastecedor, y se consolidan la penas para ciertas actividades Informáticas ilícitas.

---

[28] http://www.usdoj.gov/criminal/cybercrime/compcrime.html "COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION CCIPS". Lunes 03/03/03 19:32 p.m

4.1.4.- Italia.

En Italia con la reforma de 1995, la figura básica del daño fue modificada para dar cabida a los bienes intangibles. Así, el artículo 635 bis del Código Penal Italiano, bajo el nombre de daddeggiamento de sistemi informatici a telematici, ("Daños a los Sistemas de Informática y Telemática") establece en su texto original que:

"Chiunque distrugge, deteriora o rende, in tutto o in parte, inversible sistemi informatici altrui, ovvero programmi, información o dati altrui, é´ punito, salvo che il fatto constitusca piû grave reato, con la reclusione da sei msesi a tre anni. Se ricorre una o piû delle circostanze di cui al secondo comma dellárticolo 635, ovvero se il fatto e´commesso con abuso della qualitä di operatore del sistema, la pena e´della reclusione da uno a quattro anni."[29]

Esto quiere decir que cualquier persona destruya, o deteriore, en todos o en parte invertible, sistemas informáticos o telemáticos, programas de información será penalizado de seis meses a tres años de prisión o de uno a cuatro años.

---

[29] **http://www.studiocelentano.it/codici/cp/codicepenale.htm** "Codice Penale". Libro Secondo. DEI DELITTI IN PARTICOLARE. Titoli VIII e XIII. **Lunes 03/03/03 21:30 p.m.**

Y además se incluyó en el artículo 420 un delito denominado attentao a impianti di pubblica utilita que sanciona con pena de prisión a quien dañe o destruya un sistema informático o telemático de utilidad pública.

El artículo 615 quienquies establece que el delito de difusión de programas dirigidos a producir daños o interrumpir un sistema informático (Diffusione di programi diretti a danneggiare o interrumpere un sistema informático). Cualquiera que difunda un programa informático que tenga por objeto el daño a un sistema informático o telemático, datos o programas , o la interrupción total o parcial de funcionamiento puede ser condenado hasta dos años de prisión.

4.1.5.- Japón.

En Japón se creo la Ley prohibición de actos de acceso desautorizados de la computadora, entrando en vigor el 3 de febrero del 2000.

"El Artículo Tercero hace mención de que ninguna persona conducirá un acceso desautorizado de la computadora significando ello, un acto de hacer disponible un uso específico que es restringido por una función de control de acceso, haciendo la

operación en una computadora especifica ya sea por vía línea de telecomunicación, por medio de otro código de identificación de personas, u ordena que puedan evadir las restricciones puestas por esa función de control de acceso en ese uso específico. Se castigará a la persona que haya cumplido dichos supuestos con la Servidumbre penal para no más de un año o una multa de no más que 500.000. Yenes."[30]

4.2 Análisis de la Legislación Mexicana en materia de Delitos Informáticos.

La legislación Mexicana en materia de delitos informáticos dista mucho de ser perfecta, es sólo un primer paso para lograr un ambiente sano y seguro para los negocios y comunicaciones electrónicas en nuestro país.

Para el desarrollo de este capitulo se analizará la legislación que regula administrativa y penalmente las conductas ilícitas relacionadas con la informática, pero que, aún no contemplan en si los delitos informáticos actuales.

---

[30] http //www nii ac jp/sokuho/articles/ncid/ html 法學論叢 (Kyoto- Law Review) / 京都帝國大學法科大學 Domingo 26/01/03 17 08 p m

4.2.1.- Constitución Política de los Estados Unidos Mexicanos.

Algunos de los artículos de la Constitución Política de los Estados Unidos Mexicanos en los cuales se trazan las bases fundamentales para legislar en materia de informática los delitos derivados de la misma y que dan pauta al derecho de información que a la letra dicen:

> **ARTICULO 5° P. I.** A ninguna persona podrá impedirse que se dedique a la profesión, industria, comercio o trabajo que le acomode, siendo lícitos. El ejercicio de esta libertad sólo podrá vedarse por determinación judicial, cuando se ataquen los derechos de tercero, o por resolución gubernativa, dictada en los términos que marque la ley, cuando se ofendan los derechos de la sociedad. Nadie puede ser privado del producto de su trabajo, sino por resolución judicial.

El Artículo aludido hace referencia a que ningún trabajo debe ir en contra de la ley ni de los intereses legítimos de otras personas; tampoco debe lesionar la libertad o dignidad de quien presta el servicio. Esta garantía para dedicarse al trabajo, profesión o

empresa que el individuo desee, se considera como garantía de libertad. Es decir, cualquier persona se puede dedicar a lo que desea siempre que no lastime los intereses de los demás, aquí tenemos el caso de los "hackers" los cuales entran en sistemas que se consideran seguros, pero que ellos pueden infringir y por lo tanto están lastimando a terceros, al violar la privacidad de los demás.

> **ARTICULO 6º.** La manifestación de las ideas no Será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito o perturbe el orden publico; el derecho a la información será garantizado por el estado.

El Artículo citado señala que la manifestación de ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito, o perturbe el orden público; además que el derecho a la información será garantizado por el Estado.

Asimismo se encuentran contempladas dos garantías de orígenes diversos como son la libertad de expresión y el derecho a estar informados, este último es una garantía de conquista social relativamente nueva. Esto es que nadie puede negar el derecho de tener una propia página en Internet, claro que siempre y cuando

esta no ataque a la moral o algún tercero, además de que todos tenemos el derecho de acceso a medios de información como el Internet, para mantenernos al día en las noticias.

> **ARTICULO 14 P. II.** Nadie podrá ser privado de la vida, de la libertad o de sus propiedades, posesiones o derechos, sino mediante juicio seguido ante los tribunales previamente establecidos, en el que se cumplan las formalidades esenciales del procedimiento y conforme a las leyes expedidas con anterioridad al hecho.

El artículo referido nos menciona que nadie puede ocupar la computadora de una persona sin su autorización o al menos que se vaya a utilizar con un fin público, y eso con un pago previo de indemnización.

4.2.2.- Código Penal Federal.

El Código Penal Vigente fue reformado el 17 de mayo de 1999, aunque el lapso de tiempo que ha transcurrido desde entonces es relativamente corto, los avances tecnológicos han sido vertiginosos y radicales en algunos casos.

Solamente o protege a unos cuantos en materia de "Acceso Ilícito a Sistemas y Equipos de Informática", y aún no contempla muchos tipos de ataques informáticos como delitos.

Dicho Código divide en tres categorías a los Delitos informáticos. Ya sea por acceso ilícito a sistemas y equipos informáticos de particulares, de gobierno y del sistema financiero mexicano. La única variante son las sanciones y algunas agravantes especiales, todo ello se encuentra establecido el Libro Segundo, capitulo dos, Título Noveno cuyo nombre es la "Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática" comprendiendo desde el artículo doscientos once bis uno hasta el doscientos bis siete", que a continuación son descritos en sus textos originales:

TÍTULO NOVENO
CAPÍTULO II
ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

ARTÍCULO 211 bis 1. Al que sin autorización modifique, destruya o provoque pérdida 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 dichos sistemas o equipos, se le impondrán de tres meses

a un año de prisión y de cincuenta a ciento cincuenta días multa.

ARTÍCULO 211 bis 2. Al que sin autorización modifique, destruya o provoque pérdida 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 dichos sistemas o equipos de informática del Estado, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

ARTÍCULO 211 bis 3. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida 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 dichos 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.

ARTÍCULO 211 bis 4. Al que sin autorización modifique, destruya o provoque pérdida 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 dichas instituciones, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

ARTÍCULO 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 pérdida 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 dichas instituciones, 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 incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

ARTÍCULO 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 articulo 400 bis de este código.

ARTÍCULO 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.

Por lo que refiere al 400 bis de este código, se entenderá por Instituciones que integran el Sistema Financiero, las señaladas en el Artículo Cuatro Cientos Bis Párrafo Séptimo de este mismo Código como son las Instituciones de Crédito, de Seguros y de Fianzas, Almacenes Generales de Deposito, Arrendadoras Financieras, Sociedades de Ahorro y Préstamo, Sociedades Financieras de Objeto Limitado, Uniones de Crédito, Empresas de Factoraje Financiero, Casas de Bolsa y otros Intermediarios Bursátiles, Casas de Cambio, Administradoras de Fondos de Retiro y cualquier otro Intermediario Financiero o Cambiario.

4.2.3.- Ley Federal del Derecho de Autor.

Los Programas de computación, las bases de datos y las infracciones derivadas de su uso ilícito se encuentran reguladas en la Ley Federal del Derechos de Autor del 24 de diciembre de 1996, que entró en vigor el 24 de marzo de 1997.

Esta Ley regula todo lo relativo a la Protección de los Programas de Computación, a las Bases de Datos y a los Derechos Autorales relacionados con ambos.

Se define lo que es un programa de computación, su protección, sus derechos patrimoniales, de arrendamiento, casos en los que el usuario podrá realizar copias del programa que autorice el autor del mismo, las facultades de autorizar o prohibir la reproducción, la autorización del acceso a la información de carácter privado relativa a las personas contenida en las bases de datos, la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, establece las infracciones y sanciones que en materia de derecho de autor deben ser aplicadas cuando ocurren ilícitos relacionados con los citados programas y las bases de datos, etcétera.Todo ello se encuentra establecido en el Capitulo Cuarto cuyo titulo son los "Programas de Computación y Base de Datos", artículos Ciento uno al Ciento catorce, que continuación son descritos algunos artículos principales sobre la materia:

ARTÍCULO 101. Se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función especifica.

ARTÍCULO 102. Los programas de computación se protegen en los mismos términos que las obras literarias. dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de computo que tengan por objeto causar efectos nocivos a otros programas o equipos.

ARTÍCULO 103. Salvo pacto en contrario, los derechos patrimoniales sobre un programa de computación y su documentación, cuando hayan sido creados por uno o varios empleados en el ejercicio de sus funciones o siguiendo las instrucciones del empleador, corresponden a este.

Como excepción a lo previsto por el articulo 33 de la presente ley, el plazo de la cesión de derechos en materia de programas de computación no esta sujeto a limitación alguna.

ARTICULO 105. El usuario legitimo de un programa de computación podrá realizar el numero de copias que le autorice la licencia concedida por el titular de los derechos de autor, o una sola copia de dicho programa siempre y cuando:

I. Sea indispensable para la utilización del programa, o

II. Sea destinada exclusivamente como resguardo para sustituir la copia legítimamente adquirida, cuando ésta no pueda utilizarse por daño o pérdida. La copia de respaldo deberá ser destruida cuando cese el derecho del usuario para utilizar el programa de computación.

ARTICULO 110. El titular del derecho patrimonial sobre una base de datos tendrá el derecho exclusivo, respecto de la forma de expresión de la estructura de dicha base, de autorizar o prohibir:

I. Su reproducción permanente o temporal, total o parcial, por cualquier medio y de cualquier forma;

II. Su traducción, adaptación, reordenación y cualquier otra modificación;

III. La distribución del original o copias de la base de datos;

IV. La comunicación al público, y

V. La reproducción, distribución o comunicación pública de los resultados de las operaciones mencionadas en la fracción II del presente artículo.

ARTICULO 113. Las obras e interpretaciones o ejecuciones transmitidas por medios electrónicos a través del espectro electromagnético y de redes de telecomunicaciones y el resultado que se obtenga de esta transmisión estarán protegidas por esta ley.

ARTICULO 114. La transmisión de obras protegidas por esta ley mediante cable, ondas radioeléctricas, satélite u otras similares, deberán adecuarse, en lo conducente, a la legislación mexicana y respetar en todo caso y en todo tiempo las disposiciones sobre la materia.

4.2.4. Ley de las Vías Generales de Comunicación.

Fue Publicada el 19 de Febrero de 1940 y reformada el 29 de junio de 2001. Dentro de esta ley podemos encontrar la protección que se da a los correos electrónicos, y habla sobre la red nacional que es la encargada de manejar todo lo que es el Internet, en este

caso solamente manejaremos tres artículos que se relacionan con lo ya mencionado.

> **ARTÍCULO 378.** Queda prohibido interceptar, divulgar o aprovechar sin derecho, los mensajes, noticias e informes que no estén destinados al domino público y que se escuchen por medio de aparatos de comunicación eléctrica.

El Artículo aludido hace referencia ninguna persona puede utilizar para ningún fin, información que no sea suya o del dominio público.

> **ARTÍCULO 381.** Las oficinas de comunicaciones eléctricas sólo son responsables, en los casos de transmisión de mensajes, por error, alteración o demora, y su responsabilidad se limitará únicamente a la devolución del importe de mensaje o a su repetición.

El Artículo citado hace referencia, de que ninguna empresa que preste el servicio de correo electrónico se hará responsable en caso de que algún mensaje transmitido por este medio contenga

material que pueda afectar moralmente a los usuarios de este servicio.

> **ARTÍCULO 386.** La Red Nacional está integrada por las instalaciones de comunicación eléctrica pertenecientes a la Federación y destinadas al servicio público. Son servicios de dicha red la expedición de telegramas, giros, la transmisión de conferencias, cotizaciones mercantiles, comunicaciones telegráficas y demás servicios especiales que señalen los reglamentos.

Por lo que respecta al presente Artículo, la Internet no está integrada a las instalaciones de comunicación eléctrica pertenecientes a la federación, pero la Red Nacional es la encargada de administrar este servicio en nuestro país.

4.2.5.- Código Penal para el Estado de Sinaloa.

Ante la importancia que tiene que el Congreso Local del Estado de Sinaloa haya legislado sobre la materia de delitos, siendo el único Estado del País que le ha dado más importancia a los

Delitos Informáticos, considero 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.

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. Considero que se ubicó ha dicho delito 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.

CAPITULO V

PROBLEMÁTICA DEL SIGLO XXI EN CUESTIÓN DE DELITOS INFORMÁTICOS EN MÉXICO

CAPITULO V

PROBLEMÁTICA DEL SIGLO XXI EN CUESTIÓN DE DELITOS INFORMÁTICOS EN MÉXICO.

En el presente capitulo, se analiza cada uno de los Delitos Informáticos que existen en México y el mundo en la actualidad, ya sea por la utilización de las computadoras o un medio electrónico de comunicación de grandes alcances como lo es el "Internet".

Así como también se analizan los Organismos de Prevención en dicha materia y se realizan una serie de propuestas para mejorar tanto la legislación como la aplicación de la justicia en nuestro país.

5.1.- Delincuencia Informática en México.

En el mundo en que vivimos actualmente y el que seguramente nos encontraremos en el Nuevo Siglo, la Informática ocupa una gran diversidad de ámbitos en nuestra vida diaria, seguramente inimaginables.

La Informática avanza a grandes pasos en la cultura mundial, invade todos los ámbitos de las relaciones sociales y consecuentemente el derecho debe enfrentarse a impresionantes

cambios y México no es la excepción aunque exista legislación al respecto no se ajusta a las necesidades y problemáticas que hoy en día enfrentamos, porque no existe una cultura computacional consistente.

La delincuencia informática en nuestro país es una realidad palpable. desafortunadamente todavía no hay estadísticas oficiales que nos permitan ver con claridad el tema.

Cabe mencionar al respecto que los Delitos Informáticos se dividen en tres categorías:

a) Acceso ilícito a sistemas equipos informáticos de particulares,

b) Acceso ilícito a sistemas equipos informáticos de gobierno

c) Acceso ilícito a sistemas equipos informáticos del sistema financiero mexicano.

Actualmente proliferan los llamados "Delitos Informáticos cometidos a través del Internet", como son los fraudes bancarios, lanzamientos de virus o acoso a correos electrónicos, mismos que se incrementarán de manera significativa en los próximos Veinte años.

Sin embargo, un estudio realizado bajo los auspicios de la Academia Mexicana de Derecho Informático, A.C., ha revelado cifras alarmantes, ..."más de 843 Portales de Internet mexicanos han sido hackeados durante el 2003. Redondeando los números, tenemos que cada día más de 1.5 sitios mexicanos (o más bien dicho, el servidor en que éste se aloja) son penetrados y modificados por delincuentes informáticos". [31]

Un ejemplo claro de este tipo de ataques lo podemos encontrar en el artículo publicado en el periódico Reforma del día 12 de julio del 2003, donde nos señala:

,.." a la par del lanzamiento de la Ley de Transparencia y Acceso a la Información Pública Gubernamental por parte del Ejecutivo, en el Sistema Internet de la Presidencia de la República de México, cuyo servicio ha sido objeto de múltiples ataques informáticos desde el inicio de la administración. El ataque al servidor de Internet llegó a volúmenes equivalentes a cientos de miles de usuarios simultáneos, algo que podría saturar la página e inutilizarla, el ataque, según se logro identificar, proviene de un servidor de Estados Unidos, todo con el propósito de afectar contenidos de la página y obtener información de la oficina gubernamental..." [32]

---

[31] http://amiac.org.mx. ACADEMIA MEXICANA DE INFORMÁTICA, A. C. Cifras de la AMIAC sobre Hackers que Interfieren 835 sitios mexicanos en el 2002. Lunes 10/0303 23:42 p.m

[32] Atacan hackers sitio presidencial." Reforma. No. 3465. Año 10. México. DF. 12 de julio 2003. P. A25.

Lo que destaca, que la aplicación de Justicia en dichos ilícitos va estar a cargo de la Policía Federal Preventiva a través de la Unidad de Policía Cibernética México y Delitos Cibernéticos México (DC MÉXICO), ya que tan solo a un año de su creación, no se tiene información alguna de procedimiento que se haya llevado hasta el momento en dichas instituciones a cerca de conductas delictivas como robos, fraudes, narcotráfico, terrorismo, espionaje entre otros. Posteriormente se analizaran cada una de estas Instituciones y los respectivos delitos.

5.2.- Clasificación de los Delitos Informáticos.

Existen diversas clasificaciones acerca de estos ilícitos, empero la mas allegada y clara en base al tema tratado es la que a continuación se redacta:

5.2.1.- Como Instrumento o Medio.

Se refiere a las posibilidades que nacen al utilizar la informática como herramienta a la realización de determinadas acciones dolosas que puedan ser consideradas delictivas. Se tienen a las conductas criminógenas que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito.

5.2.2.- Como Fin u Objetivo.

Esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física del objeto o máquina electrónica o su material con la finalidad de dañarla.

5.2.3.- Como Método.

Son conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito. Ejemplo claro de ello lo podemos encontrar en los delitos que se cometen a través del Internet.

5.3.- Tipos de Delitos Informáticos.

Es impredecible el calculo de los diferentes delitos informáticos que hay en la actualidad, puesto que a cada momento dichos delitos van evolucionando.

Sin embargo, las Naciones Unidas, han reconocido un cierto número de delitos como de los cuales podemos mencionar:

5.3.1.- Fraudes cometidos mediante Manipulación de Computadoras.

La manipulación, de cualquier tipo o en cualquier forma, de los datos o informaciones contenidas en los archivos o soportes físicos informáticos ajenos, se dará cuando se persiga obtener un beneficio para la persona que la realiza, o para quien se realiza, y en perjuicio de otro. Dentro de ésta encontramos:

5.3.1.1.- Manipulación de los Datos de Entrada.

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

5.3.1.2.- Manipulación de Programas.

Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos

concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras; o insertar nuevos programas o nuevas rutinas.

Un método común utilizado por las personas que tienen conocimiento especializado en programación informática es el denominado Caballo de Troya, que consiste en introducir en un sistema conocido por el autor de la maniobra y desconocido por la víctima, un programa a través del cual el autor puede acceder a éste u otros programas del usuario.

5.3.1.3.- Manipulación de los Datos de Salida.

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.

Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usa ampliamente el equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito. Un ejemplo claro, es la clonación de tarjetas de crédito.

5.3.1.4.- Fraude efectuado por Manipulación Informática que aprovecha las Repeticiones Automáticas de los Procesos de Cómputo.

Es una técnica especializada que se denomina técnica de salami en la que rodajas muy finas apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

Esto consiste en alterar un programa que maneja cuentas bancarias y logra que sumas casi imperceptibles de algunas de ellas (generalmente centavos), se acrediten en otras cuentas manejadas por el autor, de las que luego extrae el dinero así obtenido.

5.3.2 .- Falsificaciones Informáticas.

Se presenta en la falsificación de documentos públicos, oficiales y de comercio y de los despachos telegráficos que presta, en gran medida, a ser realizado mediante elementos o medios informáticos, esto es que consiste en utilizar la computadora para falsificar documentos.

Ésta puede ser empleada como:

5.3.2.1.- Objeto.

Cuando se alteran datos de los documentos almacenados en forma computarizada. El ejemplo lo podemos encontrar en la alteraciones de los sistemas bancarios y del gobierno

5.3.2.2.- Instrumentos.

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

5.3.3.- Daños o Modificaciones de Programas o Datos Computarizados.

Dentro de esta clasificación tenemos:

5.3.3.1.- Sabotaje Informático.

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal de sus sistemas.

5.3.3.2.- Virus.

Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos.

Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

5.3.3.3.- Gusanos.

Se fabrica en forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede

regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno.

Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus; por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

5.3.3.4.- Bomba Lógica o Cronológica.

Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro.

Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño.

Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar donde se halla la bomba.

5.3.4.- Acceso no Autorizado a Servicios y Sistemas Informáticos.

Es el acceso no autorizado a sistemas informáticos por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (Hackers) hasta el sabotaje o espionaje informático.

"El acceso, malintencionado o no, de una persona no autorizada a los datos que se encuentran en soportes informáticos, se está produciendo cada vez más, motivado por la falta de seguridad de los sistemas y de formación de las personas que en ellos operan, facilitando más, si cabe, por las posibilidades que ofrecen las modernas técnicas de comunicación que permiten el conocimiento, manejo y transferencia de información entre sistemas, con máximas garantías y mínimo riesgo."[33]

El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los

---

[33] **DAVARA, RODRÍGUEZ, Miguel Ángel.** Op. Cit. P. 324-325

sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

5.3.5.- Reproducción no Autorizada de Programas Informáticos de Protección Legal.

La reproducción no autorizada de programas informáticos puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales como son Estados Unidos, Japón o Chile.

El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones moderna.

5.3.6.- Atentados contra el Software.

Dentro de los atentados contra el Software se encuentran los Accesos Fraudulentos y Daños a los sistemas "...consistiendo en que valiéndose de la confianza del titular del sistema y accediendo subrepticiamente al mismo y violando las defensas existentes, puede

ingresarse a los computadores y atentar el software allí contenido."[34]

Una vez producido el acceso fraudulento al sistema se pueden dar tres situaciones:

a) Que el autor sólo quiera conocer los datos privados del dueño del sistema. Esta acción, la mayoría de las veces tiene implicancias únicamente civiles.

b) Acceder subrepticiamente a través de la computadora a documentos o informaciones de carácter político, social, militar o económico que deban permanecer secretos en función de la seguridad, de la defensa o de las relaciones exteriores de la nación.

c) Alterar o destruir datos de los sistemas pertenecientes a particulares o bien la información contenida en ellos.

5.4.- Delitos cometidos en Internet.

Si bien es cierto el Internet ayuda a la difusión inmediata de los mensajes y permite el acceso a cualquier información introducida en la red, esta ventaja supone grandes inconvenientes.

---

[14] **DAVARA, RODRÍGUEZ, Miguel Ángel.** Op. Cit. P. 324.

El crecimiento exponencial del mismo desde su despegue comercial hasta la fecha ha sido increíble. No obstante su descomunal crecimiento, presenta sus flancos débiles relacionados con la seguridad. Los efectos de los delitos cometidos por Internet prospera en varias fronteras nacionales, lo que se denomina "Cross-Frointier Financial Crimes", en un lugar distinto al que físicamente está localizada una persona, es decir, no solo afecta a un país sino a varios.

Actualmente está produciendo un intenso debate respecto a la necesidad de prevenir y sancionar los malos usos de la red, por tanto hay argumentos a favor y en contra de la creación de una legislación sobre el uso de la red. Dentro de los Delitos cometidos en Internet Actuales encontramos los siguientes:

5.4.1.- Acceso no autorizado.

Es el uso ilegítimo de "Passwords" (contraseñas) y la entrada en un sistema Informático sin la autorización del propietario, aqui el bien jurídico protegido es la contraseña. Una muestra de ello, se presenta cuando alguna vez una persona haya "chateado", habrán escuchado la palabra "LAG", esto es la producción de un retardo tanto del acceso a la información como la emisión de la misma, se produce por las conexiones clandestinas usurpando la cuenta de los clientes, lo cual produce una congestión en el servidor.

5.4.2.- Actos Parasitarios.

Algunos usuarios incapaces de integrarse a grupos de discusión (Chat) o foros de debate On-Line (En linea), se dedican a obstaculizar las comunicaciones ajenas, interrumpiendo conversaciones de forma repetida, enviando mensajes con insultos personales.

5.4.3.- Ciberacoso (Cyberstalking).

Consiste en el acosar, hostigar, molestar, intimidar o amenazar personas o entidades usando medios informáticos. El Ciber Acoso puede ser definido como la conducta amenazante o aproximaciones no deseadas dirigidas a otra persona usando el Internet y otras formas de comunicación en línea.

5.4.4.- Ciber-Crimen.

Es cuando se utilizan computadoras o cualquier medio informático como herramienta, medio o como un cómplice para realizar un delito ya sea a un particular, a una entidad del sistema bancario o alguna dependencia del estado.

5.4.5.- Ciberterrorismo.

Son ataques o intrusiones contra computadoras o redes informáticas con el fin de intimidar, extorsionar o dañar a algún gobierno para reivindicar ideales políticos, religiosos o sociales.

El fin del "Ciberterrorismo" es la destrucción física y electrónica de la infraestructura de un gobierno y su nación.

Ahora bien, Schwartau Winn lo define como:

> "... El aprovechamiento de las redes informáticas, es decir el Internet para obtener información, fomentar o cometer actos de terrorismo."[35]

Hay cinco clases de terroristas que usan la computadora para dañar a sus enemigos: los religiosos, grupos de la nueva ola (ecologistas radicales, por ejemplo), etno-nacionalistas-separatistas, revolucionarios y organizaciones de extrema derecha. Por ahora, sólo los grupos terroristas religiosos tienen capacidad para hacer la ciberguerra, aseguran. Sin embargo, organizaciones de la nueva ola, como el Animal Liberation Front, poseen una gran capacidad para desplegar ataques continuos.

---

[35] **SCHWARTAU Winn.** Op. Cit. P. 55.

Los grupos extremistas, milicias y guerrillas pueden intentar ciberasaltos masivos (ataques a través de las red) contra el gobierno e infraestructura crítica de un país, como el transporte (aeropuertos, puertos marinos), la energía eléctrica, gas y servicios de emergencia.

5.4.6.- Corrupción de Menores y Pornografía Infantil.

Son crímenes cometidos en ofensa de menores a través de una computadora y otros medios han tenido un incremento sin precedentes, en estos tiempos de globalización.

Un efecto colateral de lo anterior, lo constituye el alarmante incremento de casos, tanto en México, como en el mundo, de organizaciones criminales de "pedófilos" que promueven y transmiten vía Internet, la pornografía infantil y la corrupción de menores. También se han detectado bandas internacionales de "prostitución" que utilizan los sistemas informáticos como medio de promoción y sobre todo de reclutamiento.

5.4.7.- Destrucción de Datos.

Son los daños causados en la red mediante la introducción de

virus, básicamente se destruye todos los datos interrelacionados, que son diseñados para satisfacer las necesidades de los usuarios.

5.4.8.- Espionaje.

Dentro de este encontramos casos de acceso no autorizado a sistemas de información gubernamentales e intercepción de correo electrónico del servicio secreto, así como aquellos en que el destinatario final de esa información fuese un gobierno u organización extranjera que como ya mencione son calificados de espionaje.

5.4.9.- Estafas Electrónicas.

La proliferación de las compras por la red permiten que aumenten también los casos de estafa. Se trataria en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de estafa, ya que además del engaño y el "Animus Defraudandi" existiría una engaño a la persona que compra. No obstante seguiría existiendo una laguna legal en aquellos países cuya legislación no prevea los casos en los que la operación se hace engañando al ordenador.

No existe en la actualidad una manera de prevenir totalmente este delito, años atrás se les decía a los usuarios de tarjetas de crédito que las compras realizadas en Internet, eran seguras, dado que los productos adquiridos llegaban al domicilio en donde se recibe le resumen de la tarjeta, pero actualmente se les permite a los compradores cambiar el domicilio de destino en el momento de celebrar al compra.

5.4.10.- Hacktivismo.

Es derivado del hacking. "Consiste en el uso de la red por grupos activistas de cualquier tipo (políticos, religiosos, pro-derechos humanos, ambientalistas, etc.) para promover ciber-desobediencia civil o ataques en contra del gobierno."[36]

La motivación del hacktivismo es la protesta enérgica en contra del gobierno, la cual puede estar caracterizada por actos de violencia electrónica.

5.4.11.- Hoaxes.

Son falsas alarmas de virus, noticias, u otro tipo de alertas y

---

[36] **SCHWARTAU Winn.** Op. Cit. P. 61.

mensajes que son transmitidos por correo electrónico, estos producen pánico, falsas alarmas, y desinformación.

Los hoaxes tratan de ganarse la confianza de los usuarios aportando datos que parecen ciertos y proponiendo una serie de acciones a realizar para librarse de la supuesta infección.

5.4.12.- Infracción a los Derechos de Autor.

"En general, son actividades infractoras aquellas en las que la utilización de una obra protegida tiene lugar en circunstancias determinantes de la violación de derechos de exclusiva integrados en la propiedad intelectual, no existiendo ninguna protección, respecto a las copias ilegales introducidas en el sistema."[37]

Como podemos observar consiste en la interpretación de los conceptos de copia, distribución, cesión, comunicación pública de los programas de ordenador utilizando la red y de reproducción en los supuestos de descargas en la memoria del disco duro del ordenador, un disquete o en papel por medio de su impresión. Esto claro sin la autorización del titular de los derechos de explotación.

---

[37] **DE MIGUEL ASENCIO Pedro Alberto.** Derecho Privado de Internet. Ed. Civita. 2ª Edición, Madrid. España. 2001. P. 253.

5.4.13.- Infracción del Copyright de Base de Datos.

No existe una protección uniforme de las bases de datos en los países que tiene acceso a Internet. El sistema de protección más habitual es el contractual. El propietario del sistema permite que los usuarios hagan "Downloads" (Descargas) de los ficheros contenidos en el sistema, pero prohíbe el recopilado de la base de datos o la copia masiva de información.

Actualmente se ha producido un nuevo fenómeno en la red, el acceso de los usuarios al programa llamado MP3, les permite bajar música de la red, la misma no es provista por las compañías discográficas, lo cual ha producido terribles inconvenientes económicos a las compañías discográficas, así como también a los artistas musicales.

5.4.14.- Intercepción de E-MAIL.

Es el descubrimiento o revelación de secretos, que alude expresamente a los mensajes de correos electrónicos.

Esto constituye una violación de correspondencia, y la intercepción de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.

5.4.15.- Jokes.

Es un programa inofensivo que simula las acciones de un virus informático en nuestro ordenador. Su objetivo no es atacar, sino gastar una broma a los usuarios, haciéndoles creer que están infectados por un virus y que se están poniendo de manifiesto sus efectos. Aunque su actividad llega a ser molesta, no producen realmente efectos dañinos.

Existen ciertos tipos de mensajes o de software que a veces son confundidos con virus, pero que no lo son en ningún sentido. Es muy importante conocer las diferencias para no sufrir las consecuencias negativas de una confusión.

5.4.16.- Narcotráfico.

Tanto el FBI como otros Organismos Internacionales, han alertado sobre la necesidad de medidas que permitan interceptar y decodificar "...los mensajes encriptados que utilizan los narcotraficantes para ponerse en contacto con los cárteles...",[38] también se ha destacado el uso de la red para la transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recorridos.

---

[38] **PALLAZZI, Pablo Andrés**. Op. Cit. P. 55

5.4.17.- Phreaking.

Es definido como el arte y ciencia de crackear una red telefónica (para, por ejemplo, hacer llamadas de larga distancia gratuitas). Por extensión, la violación de la seguridad en cualquier otro contexto, especialmente en redes de comunicaciones. Finalmente, en el concepto phreaking entrarían las técnicas de fraude en materia de telefonía analógica y digital.

En sentido general Phreaking es por definición:

> "Es el penetrar ilícitamente sistemas telefónicos o de telecomunicaciones con el fin de obtener beneficios o causar perjuicios a terceros."[39]

5.4.18.- Posesión Ilegal de Sistemas de Encriptado.

También conocido como Posesión Ilegal de Claves, dicho delito "consiste en tener Passwords o claves de acceso que pertenezcan a un sistema de seguridad a través de la red.

---

[39] **SCHWARTAU Winn.** Op. Cit. P. 61.

5.4.19.- Robo de Identidades.

Es el robo de nombres y números personales de Seguridad Social de una o varias personas con los que a través de ellos se identifican números de tarjetas de crédito e información de cuentas bancarias y son utilizados para hacer compras por teléfono y por vía Internet.

5.4.20.- Spam.

Reside en el no envío solicitado de correo electrónico. (e-mail), no importando que disfraz se le de al comunicado ó la excusa que utilicen para justificar el envío del correo-electrónico.

Esto se presenta cuando en la mayoría de las personas conectadas a la Internet no goza de una conexión que no les cueste, y adicionalmente reciben un cobro por uso del buzón. Por lo tanto el envío indiscriminado de este tipo de correo ocasiona costos al lector.

5.4.21.-Terrorismo.

Es la existencia de Hosts que ocultan la identidad del

remitente, convirtiendo el mensaje en anónimo. Ha podido ser aprovechado por grupos terroristas para remitirse consignas y planes de actuación internacional, como lo sucedido en los ataques terroristas sucedido en Estados Unidos, donde varias terroristas ocultaban sus identidades a través de Hosts.

5.4.22.- Transferencia de Fondos.

Este es el tipico caso en el que no se produce engaño a una persona determinada sino a un sistema informático. El engaño va ser producida por una persona que tenga conocimiento en la materia, y va realizar diferentes tipos de maniobras para enriquecerse en forma ilícita, todo ello a través de la red.

5.4.23.- Uso de Comerciales no Éticos.

Algunas empresas no han podido escapar a la tentación de aprovechar la red para hacer una oferta a gran escala de sus productos, llevando a cabo "mailings electrónicos.

Ello, aunque no constituye una infracción, es mal recibido por los usuarios de Internet, poco acostumbrados, hasta fechas recientes, a un uso comercial de la red.

5.5.- Organismos de Prevención de Delitos Informáticos.

La Dirección General de Inteligencia de la Policía Federal Preventiva, dependiente de la Secretaría de Seguridad Pública, que cuenta con un área especifica en materia de investigación y dedica la mayor parte de sus esfuerzos a los Delitos Informáticos, por ello creo la "Unidad de Policía Cibernética" y posteriormente el "DC MÉXICO", cuyas características son las siguientes:

5.5.1.- Unidad de Policía Cibernética.

Ejerciendo sus atribuciones legales, conforme a lo establecido en su Marco Jurídico, la Policía Federal Preventiva ha desarrollado en México la primera Unidad de Policía Cibernética, que además de las acciones preventivas en materia de "Delitos cometidos en Internet" y usando medios informáticos, cuenta con un área especifica en materia de prevención y atención de denuncias de Delitos contra menores, como existen en policías de países desarrollados.

Su misión va ser la siguiente:

"a) La identificación y desarticulación de organizaciones dedicadas al robo, lenocinio, tráfico y corrupción de menores,

así como la elaboración, distribución y promoción de pornografía infantil, por cualquier medio.

b) Localización y puesta a disposición ante autoridades ministeriales de personas dedicadas a cometer delitos informáticos.

c) Realización de operaciones de patrullaje antihacker, utilizando Internet como un instrumento para detectar a delincuentes que cometen fraudes, intrusiones y organizan sus actividades delictivas en la red.

d) Análisis y desarrollo de investigaciones en campo sobre actividades de organizaciones locales e internacionales de pedofilia, así como de redes de prostitución infantil.

e) Promover la seguridad en los sistemas de computo de usuarios y empresas para evitar robo de información, espionaje y sabotaje de sitios en Internet."[40]

Con todo ello le ha permitido detectar en México la circulación de correos electrónicos con imágenes de tipo sexual entre menores, o de adultos con menores, así como la identificación de sitios de internet que distribuyen ese material y detectar sabotajes en diferentes empresas mexicanas.

---

[40] http://www.derechosinfancia.org.mx/ediac/.htm "LOS ESPACIOS DE DESARROLLO INTEGRAL". Actividades de la Policía Cibernética. Miércoles 02/07/03 15:30 p.m

La Policía Cibernética va estar integrada por policías especializados en el manejo de computadoras, psicología y criminalística, cuya actividades son las siguientes:

I.- Integrar un equipo especializado en delitos cibernéticos a fin de hacer a este medio electrónico un lugar seguro para el intercambio de información.

II.- Analizar y atacar los diferentes tipos de delitos cibernéticos que se presentan en el ciberespacio, así como su modus operandi.

III.- Utilizar la Internet como un instrumento para identificar a los delincuentes que cometan este tipo de delitos.

IV.- Realizar patrullajes en la red a fin de localizar sitios que hayan podido ser vulnerados.

V.- Analizar y desarrollar estrategias para la identificación de los diversos delitos ocurridos en Internet.

VI.- Ofrecer seguridad en la navegación en la Internet para los menores ya que existen peligros en ella.

VII.- Identificar los procedimientos mediante los cuales los niños son explotados por personas mayores.

VIII.- Identificar la naturaleza, extensión y causas de los delitos cometidos en contra de mujeres y menores como son la corrupción y explotación sexuales.

IX.- Identificar y combatir al crimen organizado dedicado al tráfico de menores.

X.- Establecer técnicas adecuadas para la búsqueda y llocalización oportuna de niños extraviados, perdidos y/o robados.

XI.- Crear estrategias para combatir a las redes de delincuentes que se dedican a dañar a los menores de edad.

XII.- Desintegrar y poner a disposición del ministerio público a las bandas de pedófilos dedicadas a la explotación sexual de menores y a la pornografía infantil.

XIII.- En materia de delitos cibernéticos se mantiene un patrullaje sobre sitios y atención a los llamados de la ciudadanía cuando hay ataques de hackers o fraudes a través de la Internet. [41]

Actualmente las autoridades policiales de todo el mundo cuentan con un cuerpo policiaco especializado en delitos cometidos

[41] Loc. Cit.

por computadora y nuestro país no es la excepción, ya que se ha extendido por todo el país, cuyo objetivo principal es el detectar las mafias de prostitución infantil que operan desde México, pero realmente no es el único delito informático cometido en la red.

5.5.2.- DC MÉXICO (Delitos Cibernéticos México).

Como una medida para combatir "Delitos Informáticos en México, el 9 de Diciembre del Dos mil Dos fue creado el grupo DC México, que preside la Policía Federal Preventiva. Su objetivo es garantizar la seguridad y la capacidad reactiva conjunta para combatir ilícitos provocados por la acción humana en la Red "Internet" mediante el uso de sistemas de cómputo.

"El DC MÉXICO, es un cuerpo colegiado que concentrará la información necesaria, que permita la identificación, monitoreo, rastreo y localización de todas aquellas manifestaciones delictivas tanto en el territorio nacional como fuera de él. Como instancia de control y apoyado en la participación de las autoridades persecutoras de delitos, se convierte en un canal confiable de enfrentamiento inmediato y con seguimiento de toda denuncia de ilícitos informáticos en México y en el extranjero afectando intereses del país. También es el único punto de contacto oficial con sus contrapartes en los Estados Unidos, en términos de los acuerdos bilaterales con esa Nación y los que se propicien con otras entidades

internacionales."[42]

Va estar integrado por los siguientes miembros:

a) Entidades públicas del Poder Ejecutivo Federal,

b) Seguridad Nacional.

c) Poder Legislativo Federal a través de la Cámara de Diputados.

d) Gobiernos Estatales.

e) Universidades y Centros de Educación Superior.

f) Empresas privadas vinculadas a seguridad en sistemas de cómputo.

g) Organizaciones civiles comprometidas con la seguridad en Internet.

h) Proveedores de servicios de Internet en México.

---

[42] http://mx.yahoo.com/ "NOTICIAS." Funciones de la DC México. Miércoles. 21/01/03 21:30 p.m

5.6.- Propuestas para Adecuar la Legislación y la Justicia Mexicana ante los Delitos Informáticos Actuales.

Para el presente trabajo, señalo una serie de propuestas tanto en lo legislativo como en la aplicación de la justicia, estando conciente que con ello, no se van a eliminar a los "Delitos Informáticos", sino mas bien es una forma de prevenirlos, las cuales expongo de la siguiente manera:

PRIMERA.- Modificar el Código Penal Federal vigente, Titulo Noveno, Capítulo Segundo, cuyo título es el "Acceso ilícito a Sistemas y Equipos de Informática" que solamente protege a unos cuantos y aún no contempla muchos tipos de ataques informáticos como delitos y llamarlo "Delitos Informáticos".

Posteriormente reformar los artículos 211 Bis Uno al 211 Bis Siete, pertenecientes al Capitulo Segundo, para que se adicionen los siguientes:

ARTÍCULO 211 BIS UNO.-

Para los efectos de este presente capitulo se entenderá por:

I.- Computadora(s): Sistema electrónico, óptico, magnético o de cualquier otra tecnología que lleva a cabo operaciones de aritmética y de lógica a alta velocidad de acuerdo a las instrucciones internas, que son ejecutadas con intervención humana, además, tiene la capacidad de aceptar y almacenar datos de entrada, procesarlos y producir resultados de salida automáticamente, su función principal es procesar datos. Incluyendo también este termino las redes públicas o privadas de computadoras.

II.- Programa de Computo: la expresión original, en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora realice una tarea o función específica.

III.- Mecanismo de Seguridad: Dispositivo electrónico, palabra o clave, programa de computo cuyo función principal es proteger a una computadora, tanto en sus programas, como en su información contenida en la misma, de que se le de un uso ilícito.

IV.- Internet: Es la interconexión de redes informáticas que permite a las computadoras conectadas comunicarse

directamente. El término suele referirse a una interconexión en particular, de carácter planetario y abierto al público, que conecta redes informáticas de organismos oficiales, educativos y empresariales.

V.- Delitos Informáticos: Son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático. Por otra parte, debe mencionarse diferentes denominaciones para indicar dichas conductas ilícitas, tales como "delitos cibernéticos", "delitos electrónicos", "delitos relacionados con las computadoras", "crímenes por computadora", "delincuencia relacionada con el ordenador", delitos computarizados o delitos telemáticos.

VI.- Delitos Informáticos cometidos por el Internet: Son todas aquellas conductas ilícitas cometidas a través de la red.

VII.- Daño: Deterioro o menoscabo a la integridad, confidencialidad o disponibilidad de datos, información, programas de computo o computadoras.

VIII.- Información: Archivos o datos, contenidos o transmitidos

a través de una computadora o por medios electrónicos, ópticos o de cualquier otra tecnología.

IX.- Red: Conjunto de técnicas, conexiones físicas y programas informáticos empleados para conectar dos o más computadoras.

X.- Web: Es la forma de ofrecer información y el medio más potente. La información se ofrece en forma de páginas electrónicas conteniendo textos, imágenes, sonidos, videos y además, permite saltar de un lugar a otro en la Internet.

ARTÍCULO 211 BIS DOS.-

Come el delito informático, la persona(s) que con intención y sin derecho:

I.- Tenga acceso a una computadora y a la información contenida en ella sin autorización o llegue exceder su acceso autorizado.

Se le impondrá de seis meses a tres años de prisión y de

doscientos a seiscientos días multa.

II.-Intercepte, modifique, altere, borre, destruya, provoque daño o pérdida de información contenida en computadoras o programas de computo. Se le impondrá de tres a diez años de prisión y de cuatrocientos a mil días multa.

III. Conozca, copie, divulgue o distribuya a terceros información o comunicaciones no dirigidas a él, contenidas en computadoras. Se le impondrá de seis meses a tres años de prisión y de doscientos a seiscientos días multa.

IV.- Diseñe, introduzca, programe, distribuya o provoque la transmisión o ejecución de programas de computación , datos, información, códigos, conjunto de instrucciones o comandos que tengan los siguientes objetos.

a) Impedir el uso, funcionamiento apropiado, o causar daños a información, computadoras o programas de computación.

b) Alterar la información o programas de computación contenidas en una computadora.

c) Causar la negación de servicios de naturaleza informática

realizados por una computadora o una red de las mismas. Se le impondrá de tres a diez años de prisión y de cuatrocientos a mil días multa.

V.- Diseñe, programe, comercialice, trafique, transmita, haga disponibles o distribuya programas de cómputo , números de serie o registro, palabras clave o códigos de acceso o información de cualquier naturaleza que sirva para violar mecanismos de seguridad de computadoras o programas de los mismos. Se le impondrá de tres a diez años de prisión y de cuatrocientos a mil días multa y se aumentarán hasta en una mitad, cuando la información obtenida se utilice en provecho propio o ajeno.

VI.- Almacene, hostigue, intimide, aceche o cause terror a personas físicas o morales, mediante mensajes electrónicos, el uso de computadoras o por medio de otros mecanismos electrónicos. Se le impondrá de seis meses a tres años de prisión y de doscientos a seiscientos días multa.

VII.- Comercialice, trafique, transmita, difunda, distribuya o haga disponible a través de computadoras o redes de computadoras o dispositivos de almacenamiento magnéticos, ópticos, electrónicos, o de cualquier otra tecnología:

a) Pornografía infantil.

b) Información xenofóbica, racista o discriminatoria de cualquier naturaleza.

c) Incitaciones o provocaciones para cometer delitos de cualquier índole.

d) Información que explique cómo realizar cualesquiera de los delitos contemplados en el presente Capitulo.

Se le impondrá de seis meses a tres años de prisión y de doscientos a seiscientos días multa.

VIII.- Obtenga sin consentimiento o mediante engaños datos de información personal de individuos para usarla con fines comerciales , obtenga un lucro directo o indirecto de dicha información, o la use o aproveche para cometer cualquier actividad ilícita. Se le impondrá de seis meses a tres años de prisión y de doscientos a seiscientos días

IX.- Transmita, publicite, distribuya o haga disponible a través de computadoras o redes de computadoras datos o información personal de terceros sin su consentimiento o que la haya obtenido mediante engaños. Se le impondrá de seis

meses a tres años de prisión y de doscientos a seiscientos días

X.- Inserte, altere, borre o elimine información contenida en una computadora o programa de cómputo, lo cual resulten información autentica, independientemente de si la información sea directamente legible o accesible para su consulta. Se le impondrá de tres a diez años de prisión y de cuatrocientos a mil días multa.

XI.- Cause la pérdida de propiedad de una persona, o de cualquier otro daño patrimonial, mediante la inserción, alteración borrado o eliminación de información contenida en una computadora, o de cualquier interferencia en el funcionamiento de una computadora, con el propósito fraudulento o deshonesto de procurar, sin derecho, un beneficio económico en provecho propio o ajeno. Se le impondrá de tres a diez años de prisión y de cuatrocientos a mil días multa.

ARTÍCULO 211 BIS 3.-

Las penas previstas en este Capítulo se aumentarán hasta en

una mitad, para cualquiera de los casos previstos en artículo 211 Bis 2 cuando:

a) Las conductas sean cometidas por funcionarios, empleados o personas que presten sus servicios en la institución pública o crediticia, organización o empresa privada a la que se haya causado el daño;

b) El delito informático se haya cometido en contra de computadoras de gobierno o del sistema financiero.

c) Dos o más individuos hayan actuado coordinadamente para perpetrar alguno de los delitos de este título.

d) Para cometer el delito informático haya violado algún mecanismo de seguridad.

e) Con el fin de disimular su identidad o ubicación, se haya aprovechado de la computadora o datos de información personal de un tercero o haya usado datos falsos para realizar cualesquiera de las conductas tipificadas en este capítulo.

f) Cuando bajo engaños o aprovechándose del error en que se encuentra una persona, obtiene de ésta información, códigos o claves de acceso, o logra instalar en su computadora programas de cómputo, que le permitan

realizar cualesquiera de las conductas tipificadas en este capítulo.

ARTÍCULO 211 BIS 4.-

Las penas previstas en este capítulo se aumentarán hasta el doble cuando:

I.- Se hayan dado dos o más agravantes de las mencionadas en el Artículo 211 Bis 3.

II.- El delito informático haya sido motivado por cuestiones políticas, activistas o terroristas.

ARTÍCULO 211 BIS 5.-

Se impondrán de seis meses a dos años de prisión y de cien a trescientos días multa al que:

I.- Abra indebidamente una comunicación escrita que conste en medios impresos, materiales electrónicos, ópticos o de

cualquier otra tecnología, que no este dirigida a él.

II.- Indebidamente intercepte una comunicación escrita que conste en medios impresos, materiales electrónicos, ópticos o de cualquier otra tecnología, que no esté dirigida a él, aunque la conserve cerrada y no se imponga de su contenido.

ARTÍCULO 211 BIS 6.-

Comete el delito de difamación electrónica el que comunique por medios impresos, materiales electrónicos, ópticos o de cualquier otra tecnología, dolosamente una o más personas, la imputación que se le hace a otra persona física o moral en los casos previstos por la ley, de un hecho cierto o falso, determinado o indeterminado, que pueden causarle deshonra, descrédito, perjuicio o exponerlo al desprecio alguien. Se castigara con prisión hasta de dos años o multa de cincuenta a trescientos pesos, o ambas sanciones a juicio del juez.

ARTÍCULO 211 BIS. 7.-

Comete el delito de robo electrónico el que copie, sustraiga o se apodere de documentos, datos o archivos electrónicos,

ópticos o de cualquier otra tecnología que residan en computadoras o sistemas informáticos, o el aprovechamiento o utilización de dichos documentos, datos o archivos, sin derecho y sin consentimiento de la persona que pueda disponer de los mismos. Se sancionara con pena de tres a diez años de prisión y hasta mil días multa.

ARTÍCULO 211. BIS. 8.-

Comete el delito de fraude electrónico quien engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de una cosa material o un lucro indebido que conste en medios electrónicos, ópticos o de cualquier otra tecnología avanzada. La que se castigara con las siguientes penas:

I.- Con prisión de 3 días a 6 meses o de 30 a 180 días multa, cuando el valor de lo defraudado no exceda de diez veces el salario;

II.- Con prisión de tres a 6 años y multa de diez a cien veces el salario, cuando el valor de lo defraudado excediera de cien, pero no de quinientas veces el salario.

III.- Con prisión de tres a doce años y multa hasta de ciento veinte veces el salario, si el valor de lo defraudado fuere mayor de quinientas veces el salario.

SEGUNDA.- Modificar el Artículo Trescientos Ochenta y Seis de la Ley de las Vías Generales de Comunicación, donde se integre el Internet a los servicios de la red nacional, quedando esto en la siguiente forma :

Artículo 386.- La Red Nacional está integrada por las instalaciones de comunicaciones eléctricas pertenecientes a la Federación y destinadas al Servicio Público. Son servicios de dicha Red, la expedición de Telegramas, Giros, la Transmisión de Transferencias, Cotizaciones Mercantiles, Comunicaciones Telegráficas y todo lo es el Internet.

TERCERA.- Anexar al Artículo Cuarto Fracción XV, de Ley de la Policía Federal Preventiva, la atribución donde le permita a la Policía Federal Preventiva a través de la Unidad de Policía Cibernética, tener acceso a los registros de los proveedores del servicio de Internet con el fin de localizar de manera mas rápida a aquellos usuarios sospechosos de delitos informáticos cometidos a través del Internet, todo ello quedando de la siguiente forma:

Artículo 4°.- La Policía Federal Preventiva tendrá las atribuciones siguientes:

XV.- Acceder a los registros de los proveedores de servicio de Internet, con el fin de localizar actividades ilícitas.

CUARTA.- Crear a través de la Procuraduría General de la República, una Fiscalia Especializada en atención de Delitos Informáticos, para que opere en todos los Estados de la República teniendo una mayor eficacia en la aplicación de la justicia Informática.

QUINTA.- Capacitar a los organismos de prevención, cada Veinte días, como son la Unidad de Policía Cibernética y DC México (Delitos Cibernéticos México), para que estén a la par de los delitos informáticos en la actualidad.

CONCLUSIONES

CONCLUSIÓNES

Después de haber entrado en un análisis detallado de lo se refiere a los delitos informáticos y haber estudiado someramente el derecho comparado, así como el problema que ocasionan dichos delitos en México, considero necesario exponer las siguientes conclusiones:

PRIMERA.- Desde tiempos muy remotos el hombre, al verse en la necesidad de cuantificar sus pertenencias, animales, objetos de caza, pieles, etcétera, han tenido que procesar datos, limitándose en un principio al número de sus dedos, después a cuentas de granos y objetos similares, posteriormente, invento sistemas numéricos que le permitieron realizar sus operaciones con mayor confiabilidad y rapidez, inventando al paso de los siglos el ábaco, las tablas de logaritmos, la regla de cálculo, el telar de Jaquard, las tarjetas perforadoras, hasta la creación de la computadora como la computadora personal (PC), la laptop, palptop y las table PC, que son computadoras más pequeñas, pero se puede almacenar más información.

SEGUNDO.- El delito informático es cualquier acto ilicito penal en el que se hace un uso indebido de cualquier medio Informático efectuado por personas con amplios conocimientos

originando un fenómeno social a nivel nacional e internacional.

TERCERA.- El origen del Internet data del año 1969, creado exclusivamente para proyectos de Investigación Avanzada en Estados Unidos (ARPA), se desarrolló tan rápidamente creando lo que ahora conocemos como Internet en 1991, la cual es una red diseñada por uniones de redes de computo, con la capacidad de transmitir comunicaciones rápidamente sin el control de una persona o empresa determinada, traspasando fronteras.

CUARTA.- El Internet apareció en México en 1989, a través Telmex y su uso básicamente fue para fines académicos. Actualmente el Internet, puede ser utilizado por cualquier persona, ya sea para fines académicos, laborales, gubernamentales, bancarios o por diversión. También podemos encontrar la otra cara de la moneda, esto es, se puede presentar diferentes tipos de delitos que se comente a través del Internet afectando tanto a particulares, empresas, al gobierno u organismos del sistema bancario.

QUINTA.- Los delitos cometidos por el Internet, son los siguientes:

a) Acceso no autorizado.

b) Actos Parasitarios.

c) Ciberacoso.

d) Ciber-Crimen.

e) Ciberterrorismo.

f) Corrupción de Menores y Pornografía Infantil.

g) Destrucción de Datos.

h) Espionaje.

i) Estafas Electrónicas.

j) Hacktivismo.

k) Hoaxes.

l) Infracción a los Derechos de Autor.

m) Infracción del Copyright de Base de Datos.

n) Intercepción de E-Mail.

o) Jokes

p) Narcotráfico.

q) Phreaking.

r) Posesión Ilegal de Sistemas de Encriptado.

s) Robo de Identidades.

t) Spam.

u) Terrorismo.

v) Transferencia de Fondos.

w) Uso de comerciales no Éticos.

SEXTA.- La Legislación Vigente en nuestro país como el Código Penal Federal Vigente considera que el bien jurídico tutelado en los delitos informáticos es fundamentalmente el patrimonio, mientras la Ley Federal del Derecho de Autor considera que el bien jurídico es la propiedad intelectual.

SEPTIMA.- El Código Penal federal Vigente divide a los delitos informáticos como el acceso ilícito a sistemas y equipos de informática de particulares, del gobierno y del sistema financiero

mexicano, por lo que me atrevo afirmar, por la trascendencia que ha tenido a nivel nacional e internacional este ilícito, urge una reforma legal a fondo de dicho código, en su título noveno, capítulo segundo, adecuando a los tiempos modernos en esta materia.

OCTAVA.- Por una parte, hay que tener presente que en nuestro país, el único Estado que ha legislado a través de su Congreso Local sobre el tema, es Sinaloa contemplándolos como delitos en contra del patrimonio Es necesario que con objeto de que se evite un conflicto de competencia entre los Congresos Locales de los Estados de la Re-pública y el de la Unión, se reforme el Código Penal Federal Vigente, creando el delito informático como delito federal.

NOVENA.- Control que necesitamos, tal vez no sea únicamente un problema legal, sino también un problema social, moral y tecnológico. La ley sola, no nos podrá salvar del futuro de estos delitos, solamente lo hará si actúa a la vez con una norma social ampliamente aceptada y escudo tecnológicos.

DÉCIMA.- Podrán existir cifras de delincuencia informática cometidas en nuestro país, sin embargo es una realidad de que muchas de las empresas mexicanas no dan a conocer a luz pública

si han sido victimas de dichos delitos por el mismo hecho de no volver hacer blanco de las mismos.

DÉCIMA PRIMERA .- Tanto la Unidad de Policía Cibernética y DC México, son los encargados de la aplicación de la justicia Informática en nuestro país, ambas pertenecientes a la Policía Federal Preventiva, cuyas funciones básicamente, son investigar y perseguir los delitos cometidos a través de la red, pero lamentablemente su función básica, es enfocarse más a la pornografía infantil, y no solamente existe este delito en la red.

DÉCIMA SEGUNDA.- El camino es difícil, más sin embargo no imposible, los tiempos cambian y las leyes deben cambiar también, es labor de todos mantenerlas al día. Los delitos que se pueden cometer en la actualidad mediante el uso de la tecnología son múltiples y de tipos muy variados, nadie puede estar seguro de que uno no va a ser víctima de alguno de ellos y por lo anterior considero que tanto nosotros las personas que estamos sumergidos en los medios informáticos junto con los conocedores de las leyes debemos trabajar juntos con el fin de proporcionar un instrumento confiable que nos permita identificar y sancionar de una manera correcta los delitos que con el uso de la tecnología se puedan presentar.

GLOSARIO GENERAL

GLOSARIO

A continuación se definen los términos que pueden ofrecer dificultades de comprensión en el texto. El reiterado glosario permitirá aumentar el caudal léxico y relacionar los términos y sus diversas acepciones en la forma como se oponen las teorías contenidas en el presente trabajo.

ÁBACO: Es un tablero contador que sirve para enseñar los rudimentos de la aritmética. Se compone de un cuadro de madera con diez cuerdas o alambres paralelos yen cada uno de ellas otras tantas bolas movibles.

ACCESO: En informática, es localizar, cargar en la memoria o preparar para su ejecución alguna operación. El término 'acceso' se utiliza también para expresar el permiso que tiene un usuario en relación con discos, archivos, registros y procedimientos de entrada a las redes.

ALERTRA. Proveedor de servicios cuya función es la Supervisión de los Sitios Web.

ALGORITMO: En matemáticas, es el método de resolución de problemas complicados mediante el uso repetido de otro método de cálculo más sencillo. Un ejemplo básico es el cálculo de la división larga en aritmética. En la actualidad, el término algoritmo se aplica a muchos de los métodos de resolver problemas que empleen una secuencia mecánica de pasos, como en el diseño de un programa

de ordenador o computadora. Esta secuencia se puede representar en la forma de un diagrama de flujo para que sea más fácil de entender.

ALTAVISTA: Popular máquina búsqueda y traductora de idiomas en la Web.

AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI): Es la organización de grupos de la industria y la empresa de Estados Unidos dedicada al desarrollo de normas, para el comercio y las comunicaciones. A nivel internacional, representante en EEUU de la Organización Internacional de Normalización (ISO).

AMPERIO: Unidad básica de intensidad de corriente eléctrica, cuyo símbolo es A, llamada así en honor al físico francés del siglo XIX André Marie Ampère.

APPLE COMPUTER, INC: Fabricante estadounidense de ordenadores o computadoras personales con sede en Cupertino, California.

ARCHIVO O FICHERO: Es un conjunto completo de información identificado con un nombre. Puede ser un programa, un conjunto de datos utilizados por el programa o un documento creado por los usuarios. Los archivos son las unidades básicas de almacenamiento que permiten a la computadora distinguir entre los diversos conjuntos de información.

ARITMÉTICA: Parte de las matemáticas que estudia la cantidad discreta o discontinua.

BASE DE DATOS: Es cualquier conjunto de datos organizados para

su almacenamiento en la memoria de un ordenador o computadora, diseñado para facilitar su mantenimiento y acceso de una forma estándar. Los datos suelen aparecer en forma de texto, números o gráficos.

BIOELECTRÓNICA: Es una rama mucho más amplia ya que se encarga del estudio de la electricidad en cualquier proceso biológico, en el conjunto de un ser vivo (si se da en humanos englobaría a la electromedicina por tanto), en una parte del mismo o en una población de individuos (comunicación eléctrica entre una colonia de bacterias, por ejemplo).

BIT: Es la unidad mínima de información que maneja una computadora. El término proviene de la contracción de la expresión inglesa Binary Digit, que significa Dígito Binario. En informática, se considera el bit como la unidad de información más pequeña reconocida por una computadora.

BIT BINARIO: Un bit es un número binario que puede ser 0 ó 1.

BLASTER: Virus tipo gusano, cuyo objetivo principal es destruir los programas as de computadoras que cuentan con Microsoft, ya sea Windows 98, 2000 y XP. Siendo otra función fue la de destruir la compañía Microsoft, que preside Bill Gates.

BYTES: Unidad de información que consta de 8 bits; en procesamiento informático y almacenamiento, el equivalente a un único carácter, como puede ser una letra, un número o un signo de puntuación. Como el byte representa sólo una pequeña cantidad de información, la cantidad de memoria y de almacenamiento de una máquina suele indicarse en kilobytes (1.024 bytes) o en megabytes (1.048.576 bytes).

CABLE ELÉCTRICO: Medio compuesto por uno o más conductores eléctricos, cubiertos por un aislante y, en ocasiones, por un revestimiento o vaina protectora, utilizado para transmitir energía eléctrica o los impulsos de un sistema de comunicaciones eléctrico.

CALCULADORA: Máquina para realizar operaciones de cálculo automáticamente. Puede ser mecánica, electromagnética o electrónica

CANAL HACKER: Son portales en la Internet donde se reúnen Hackers para exponer sus ideas o conocimientos.

CARACTERES: Es una letra, un número, un signo de puntuación u otro símbolo o código de control. Un carácter no es necesariamente visible, en pantalla o sobre el papel. Por ejemplo, un espacio tiene la misma calidad de carácter que una 'a' o que cualquiera de los dígitos del 0 al 9.

CELOSÍA: es un método para multiplicar números enteros que inventó un matemático italiano, Luca Pacioli, en el siglo XV.

CIBER-ASALTOS: Ataques a través de la Red.

CIBER-CRIME: En español significa Delitos Informáticos.

CIBER-ESPACIO: Es un término para la realidad virtual inmersa, a veces usado para referirse a Internet.

CIRCUITOS DE LA LÓGICA: El término se utiliza principalmente para definir un trayecto continuo compuesto por conductores y dispositivos conductores, que incluye una fuente de fuerza electromotriz que transporta la corriente por el circuito. Un circuito de este tipo se denomina circuito cerrado, y aquellos en los que el trayecto no es continuo se denominan abiertos.

CÓDIGO (INFORMÁTICA): Término genérico para nombrar las instrucciones del programa, utilizadas en dos sentidos generales. El primero se refiere al código fuente, legible a simple vista, que son las instrucciones escritas por el programador en un lenguaje de programación. El segundo se refiere al código máquina ejecutable, que son las instrucciones convertidas de código fuente a instrucciones que el ordenador o computadora puede comprender.

CÓDIFO FUENTE: Comprende todas las funciones que diseña el programador para que la computadora muestre al usuario lo que necesita, y en la forma en que lo necesita.

CÓDIGO OBJETO: Llamado normalmente código maquina, tiene la misma función que el código fuente nada más que está escrito en un lenguaje especial, que es directamente ejecutable por la máquina. Este proceso se llama compilación.

COMPILACIÓN: Son todos los archivos y comandos desarrollados por el programador se convierten en un único archivo compilado, en un archivo ejecutable, o un programa.

COPIA DE SEGURIDAD: Copia de un programa informático, de un disco o de datos, realizada para archivar su contenido o para proteger archivos valiosos contra su pérdida en caso de que la copia activa se dañe o quede destruida. Una copia de seguridad puede considerarse como una medida de seguridad contra la pérdida de datos. Ciertos programas de aplicación realizan automáticamente copias de seguridad de archivos de datos, manteniendo en disco tanto la versión actual como la precedente. Además, es una buena medida hacer copias de seguridad de programas o de datos de difícil reconstrucción.

COPTOMETRO: Es una calculadora con columnas diferentes para los diversos dígitos (unidades, decenas y centenas).

COPYRIGHT: En español significa Derechos de Autor.

CRACKER: Es una persona o varias que interrumpe en sistemas computarizados. Usado también para denotar a alguien que realiza actividades ilegales.

CRIMINOGENO: Conducta antisocial.

CRIPTOANÁLISIS: Es el arte y la ciencia de transgredir y decodificar un texto encriptado, sin conocer las claves de acceso.

CRIPTOGRAFÍA: (kryptos, griego: Oculto) Disciplina referente a la construcción de sistemas de encriptamiento.

CRIPTOLOGÍA: Es la rama de las matemáticas relativa a la criptografía y el criptoanálisis.

CROSS-FROINTIER FINANCIAL CRIMES: En español significa en un lugar distinto al que físicamente está localizada una persona, es decir no solo afecta a un país sino a varios.

CHAT: Un Chat es un medio de comunicación en tiempo real se conoce también como IRC (Internet Relay Chat en inglés). Esto es, un lugar donde la gente puede comunicarse a través del lenguaje escrito con otros, es tan sencillo como escribir con el teclado para comunicarse. Con el Chat se puede conocer nueva gente, compartir gustos, preguntar dudas, etc... También es una forma sencilla de contactar con gente conocida que esté lejos, siempre que se puedan conectar a Internet.

CHIP: Utilizado habitualmente como sinónimo de procesador, se trata de una oblea de silicio sobre la que se imprime un microcircuito.

DATOS DE ENTRADA Y DE SALIDA: Son dos de las tres actividades (entrada, procesamiento y salida) que caracterizan un Ordenador o computadora. El término entrada/salida engloba las tareas complementarias de obtención de datos que procesa el microprocesador y de entrega de los resultados a través de un dispositivo, como la pantalla, la unidad de disco o la impresora. El teclado y el mouse o ratón son dispositivos de entrada que hacen llegar la información al ordenador o computadora. La pantalla y la impresora son dispositivos de salida con los cuales la computadora hace llegar sus resultados al usuario. Una unidad de disco es tanto un dispositivo de entrada como de salida, ya que puede proporcionar información almacenada o almacenar datos después de su procesamiento.

DATOS PERSONALES: Es cualquier información relacionada a una persona física identificada o identificable. Los datos personales usualmente contienen información que directa o indirectamente puede ser relacionada o ligada a una persona física o particular.

DC MÉXICO: Delitos Cibernéticos México./ Es un cuerpo colegiado que concentrará la información necesaria, que permita la identificación, monitoreo, rastreo y localización de todas aquellas manifestaciones delictivas tanto en el territorio nacional como fuera de él.

DERECHOS DE AUTOR: Los Derechos de Autor constituyen el reconocimiento del Estado en favor del creador de obras literarias y/o artísticas. El autor es la persona física que crea una obra; así, la Ley lo protege para estimular su creatividad y asegurar que su trabajo sea recompensado.

DÍGITOS: Se dice del número que se expresa con una sola cifra.

DIRECCIÓN: Valor que representa a una ubicación accesible en un ordenador o computadora. Las direcciones de un sistema pueden corresponder a distintos dispositivos como puede ser la memoria o a los puertos de entrada o de salida, de manera que los datos pueden leerse o escribirse sólo en dichas ubicaciones. Cada dirección es única y representa solamente un elemento en la memoria o un puerto, nunca los dos a la vez.

DIRIGIR, O DIRECCIONAR: Significa hacer referencia a una determinada ubicación de almacenamiento.

DIRECCIÓN DE INTERNET: Grupo de números que identifica univocamente a cada computadora en Internet. Consiste en cuatro números separados por puntos, en los que cada número puede variar entre 0 y 255 —por ejemplo, 123.456.78.90. Los servidores de nombres de dominio mantienen tablas que permiten traducir la dirección de Internet, también conocida como dirección IP, a una dirección del tipo cervantes.es.

DISQUETE: Disco flexible de reducidas dimensiones y muy manejable que se utiliza como dispositivo de almacenamiento. Existen dos tamaños estándar medidos en pulgadas: 5,25 y 3,5. El de 3,5 es el más extendido en la actualidad, y presenta, frente a los discos, de 5,25, importantes ventajas, que van desde su mayor fiabilidad y robustez a su mayor capacidad. Pueden presentarse en diferentes versiones: alta y baja densidad, y grabables en una o ambas caras. Los disquetes se introducen en un drive para su lectura y grabación mediante el uso de una o varias cabezas lectoras-grabadoras magnéticas.

DOWNLOAD (EN ESPAÑOL, DESCARGAR): En comunicaciones, es el proceso de transferir una copia de un archivo desde un ordenador o computadora remoto a la computadora solicitante mediante un módem o una red.

ECUACIÓN: Igualdad que contiene una o más incógnitas.

E-MAIL: También conocido como el "correo electrónico", se ha convertido en elemento imprescindible en las redes de comunicación de la mayoría de las oficinas modernas. Permite transmitir datos y mensajes de una computadora a otra a través de la línea telefónica, de conexión por microondas, de satélites de comunicación o de otro equipo de telecomunicaciones y mandar un mismo mensaje a varias direcciones. El correo electrónico puede enviarse a través de la red de área local (LAN) de la empresa o a través de una red de comunicaciones nacional o internacional. Los servicios de correo electrónico utilizan una computadora central para almacenar los mensajes y datos y enviarlos a su destino. El usuario de un PC que desee enviar y recibir mensajes escritos o hablados sólo necesita suscribirse a una red de correo electrónico pública y disponer de un módem y un teléfono. Dado el enorme volumen de correo electrónico potencial que puede generarse, se han desarrollado sistemas capaces de particularizar el correo para cada usuario.

ENCRIPTACIÓN: es un conjunto de técnicas que intentan hacer inaccesible la información a personas no autorizadas. Por lo general, la encriptación se basa en una clave, sin la cual la información no puede ser descifrada

ENGRANAJE: Conjunto de piezas que se enlazan o se traban.

ENGRANAJES DIFERENCIALES: Con este tipo de dispositivos mecánicos, podemos transportar el movimiento desde un punto hasta otro y conseguir efectos de variación de velocidad y par.

ELECTROMAGNÉTICO: Parte de la física que estudia las acciones y reacciones de las corrientes eléctricas sobre los imanes.

ELECTRÓNICA: Campo de la ingeniería y de la física aplicada relativo al diseño y aplicación de dispositivos, por lo general circuitos electrónicos, cuyo funcionamiento depende del flujo de electrones para la generación, transmisión, recepción y almacenamiento de información. Esta información puede consistir en voz o música (señales de voz) en un receptor de radio, en una imagen en una pantalla de televisión, o en números u otros datos en un ordenador o computadora.

ESPECTRO ELECTROMAGNÉTICO: Se refiere a un "mapa" de los diferentes tipos de energía de radiación y sus correspondientes longitudes de onda. Hay usualmente seis subdivisiones (ondas de radio, infrarroja, visible, ultravioleta, rayos X y rayos gama) de el espectro electromagnético.

FBI: abrev. Federal Bureau of investigation.(Organismo Federal de Investigación.)

FIBRA ÓPTICA: Es un cable de fibra de vidrio que causa muy poca pérdida de energía luminosa a través de largas distancias. El diámetro de la fibra debe ser muy pequeño con el fin de minimizar la transmisión reflectora. La fibra transmisora central es de vidrio de baja pérdida y con indice de refracción relativamente alto. Esta se cubre con vidrio de mayor pérdida, con menor indice de refracción,

para soporte y absorción de rayos que puedan escapar de la fibra central. La fuente de luz en el transmisor puede ser un diodo emisor de luz (LED) o un láser. El detector en el otro extremo es un fotodiodo o un fototransistor.

FIREWALL Una barrera de seguridad que ayuda a limitar los accesos no autorizados a un sistema de computadoras.

FLOPPY: Se conoce por este término inglés a los discos flexibles o disquetes.

GATEWAY: Es el conjunto de hardware y software que conecta redes que utilizan protocolos de comunicación diferentes, o que transmite datos por una red entre dos aplicaciones no compatibles. El gateway cambia el formato de los datos de manera que los pueda entender la aplicación que los recibe. El término se suele usar para describir cualquier computadora que transmite datos de una red a otra, pero esta acepción, técnicamente, no es correcta.

GB: Significa gabyte y equivale a 1,073,741, 824 bytes.

HACKER: Es un aficionado a los ordenadores o computadoras, un usuario totalmente cautivado por la programación y la tecnología informáticas. En la década de 1980, con la llegada de las computadoras personales y las redes de acceso remoto, este término adquirió una connotación peyorativa, refiriéndose a menudo a alguien que invade en secreto las computadoras de otros,

consultando o alterando los programas o los datos almacenados en las mismas. También se utiliza para referirse a alguien que, además de programar, disfruta desmenuzando sistemas operativos y programas para ver cómo funcionan.

HACKER DE UNÍS: Son expertos en programación y tienen conocimientos elevados sobre informática (sobretodo en redes y comunicaciones) y electrónica. Y además de tener conocimientos en el sistema operativo UNIX desarrollado en los Laboratorios Bell que es considerado como uno de los éxitos más notables del desarrollo de sistemas operativos.

La filosofía de este sistema fue la de crear sistemas apropiados para apoyar el desarrollo de programas, por lo que tienen un lenguaje de comandos simple pero poderoso, además de un sistema de archivos independiente del hardware del sistema.

HARDWARE: Equipo utilizado para el funcionamiento de una computadora. El hardware se refiere a los componentes materiales de un sistema informático. La función de estos componentes suele dividirse en tres categorías principales: entrada, salida y almacenamiento. Los componentes de esas categorías están conectados a través de un conjunto de cables o circuitos llamado bus con la unidad central de proceso (CPU) del ordenador, el microprocesador que controla la computadora y le proporciona capacidad de cálculo.

HÍBRIDA: Se dice de todo lo que es producto de elementos de distinta naturaleza

HOSTS: En el archivo de "HOSTS" se incluyen las direcciones de cada uno de los equipos de la red con su nombre y sus alias.

HYPERCARD: Es el software diseñado para los equipos Apple Macintosh que proporciona a los usuarios una herramienta de administración de información implementando muchos conceptos mediante hipertextos. Un documento HyperCard consiste en una serie de tarjetas agrupadas en una pila; cada tarjeta puede contener texto, imágenes gráficas y sonido. Los autores y usuarios de la pila pueden vincular elementos entre sí de muchas formas: desarrollando diversos tipos de búsquedas de textos, proporcionando controles que permitan viajar de tarjeta en tarjeta haciendo clic con el mouse o ratón en objetos llamados botones y a través de procedimientos (programas y rutinas) codificadas en un lenguaje orientado a objetos llamado HyperTalk

HTML: Acrónimo de Hypertext Markup Language, lenguaje de marcas de hipertexto. En informática, formato estándar de documentos de texto que se utiliza desde 1989 en World Wide Web (WWW). Los documentos HTML contienen dos tipos de información: la que se muestra en pantalla y códigos (tags o etiquetas), transparentes al usuario, que indican cómo mostrar esa información. HTML es un subconjunto de SGML (acrónimo de Standard Generalized Markup Language, lenguaje estándar de marcado de documentos), que es un estándar de descripción de página independiente del dispositivo.

INFORMÁTICA O COMPUTACIÓN: Ciencia que estudia los ordenadores o computadoras, incluyendo su diseño, funcionamiento y utilización para el procesamiento de información. La informática

combina los aspectos teóricos y prácticos de la ingeniería, electrónica, teoría de la información, matemáticas, lógica y comportamiento humano. Los aspectos de la informática cubren desde la programación y la arquitectura informática hasta la inteligencia artificial y la robótica.

INGENIERÍA DEL SOFTWARE: Es la rama de la ingeniería que aplica los principios de las ciencias de la computación y las matemáticas para lograr soluciones costo-efectivas a los problemas del desarrollo del software.

INTELIGENCIA ARTIFICIAL: Inteligencia artificial, término que, en su sentido más amplio, indicaría la capacidad de un artefacto de realizar los mismos tipos de funciones que caracterizan al pensamiento humano. La posibilidad de desarrollar un artefacto así ha despertado la curiosidad del ser humano desde la antigüedad. Con el avance de la ciencia moderna la búsqueda de la IA (inteligencia artificial) ha tomado dos caminos fundamentales: la investigación psicológica y fisiológica de la naturaleza del pensamiento humano, y el desarrollo tecnológico de sistemas informáticos cada vez más complejos.

INTERCONEXIONES: Ofrece registro de dominios y diseño de espacios en la Red

INTERFAZ GRAFICA : Son aquellas que incluyen cosas como menús, ventanas, teclado, ratón, los beeps y algunos otros sonidos que la computadora hace, en general, todos aquellos canales por los cuales se permite la comunicación entre el hombre y la computadora.

INTERNET: interconexión de redes informáticas que permite a las

computadoras conectadas comunicarse directamente. El término suele referirse a una interconexión en particular, de carácter planetario y abierto al público, que conecta redes informáticas de organismos oficiales, educativos y empresariales. También existen sistemas de redes más pequeños llamados intranet, generalmente para el uso de una única organización.

INTERNET EXPLORER: Es un navegador de Web creado por Microsoft..

JAVASCRIPT: Es un lenguaje de programación compacto y orientado al objeto destinado al desarrollo de aplicaciones Internet que actúa a modo de complemento del HTML.

KB-KILOBYTES: Kilobyte, abreviado KB, K o Kbyte. Equivale a 1.024 bytes.

LAPTOP: Computadora portátil, construida con una pantalla líquida, teclado integrado con mouse anexo. Estas computadoras tienen gran uso para las personas de negocios que deben de estar fuera de la compañía y gracias a un módem pueden estar conectados a la misma. Las Laptops son muy sostificadas y a la vez muy costosas.

LÁSER: Haz de luz monocromática, amplificada por la emisión estimulada de radiaciones en el aparato del mismo nombre, que permite obtener rayos de luz coherentes, intensos y penetrantes.

LENGUAJES DE PROGRAMACIÓN: Es cualquier lenguaje artificial que puede utilizarse para definir una secuencia de instrucciones para su procesamiento por un ordenador o computadora. Es complicado definir qué es y qué no es un lenguaje de programación. Se asume generalmente que la traducción de las instrucciones a un código que comprende la computadora debe ser completamente sistemática. Normalmente es la computadora la que realiza la traducción.

LENGUAJE HTML: Por medio del lenguaje HTML (HyperText Markup Languaje), podemos navegar por miles y miles de páginas a través de la WWW. Es un lenguaje que sirve para escribir hipertexto, es decir, documentos de texto presentado de forma estructurada, con enlaces (links) que conducen a otros documentos o a otras fuentes de información (por ejemplo bases de datos) que pueden estar en la propia máquina o en máquinas remotas de la red. Todo ello se puede presentar acompañado de cuantos gráficos estáticos o animados y sonidos seamos capaces de imaginar.

LOGARITMO: Los logaritmos fueron introducidos en las matemáticas con el propósito de facilitar, simplificar o incluso, hacer posible complicados cálculos numéricos. Utilizando logaritmos podemos convertir : productos en sumas, cocientes en restas, potencias en productos y raíces en cocientes.

LÓGICA: Ciencia que expone las leyes , modos y formas del conocimiento científico.

LÓGICA DIFUSA O LÓGICA FUZZY: Forma de lógica utilizada en algunos sistemas expertos y en otras aplicaciones de inteligencia artificial, en la que las variables pueden tener varios niveles de

verdad o falsedad representados por rangos de valores entre el 1 (verdadero) y el 0 (falso). Con la lógica fuzzy, el resultado de una operación se puede expresar como una probabilidad y no necesariamente como una certeza. Por ejemplo, además de los valores verdadero o falso, un resultado puede adoptar valores tales como probablemente verdadero, posiblemente verdadero, posiblemente falso y probablemente falso.

LUGAR EN LA WEB (EN INGLÉS, WEB SITE): Computadora que publica documentos (denominados 'páginas Web') en World Wide Web (WWW). Estos documentos están compuestos por texto, elementos multimedia (gráficos, sonido, video digital) y vínculos (punteros con la dirección de otras páginas Web, empleados para establecer una conexión automática). Un lugar en Web mantiene en ejecución un programa llamado 'servidor de páginas Web' que procesa las peticiones de información, típicamente solicitudes de páginas. Cada documento en uno de estos lugares tiene asignada una dirección única denominada URL.

MAILINGS ELECTRÓNICOS|: Es un envio comercial de carta, folletos, fotografías, listas de precios, ordenes de pedido y todo el material que uno desee, en formato digital, que va de ordenador a ordenador por medio de un módem, a través de las líneas telefónicas.

MÁQUINA: Artificio para aprovechar o regular la acción de una fuerza, o para producirla.

MÁQUINA ANALÍTICA: Máquina calculadora mecánica inventada

por el matemático y científico británico Charles Babbage en 1833, de la cual sólo se construyó una pequeña parte.

MÁQUINAS DE COMPUTO: Son equipos de Informática ya sea electrónico u óptico.

MATEMÁTICAS: Ciencia que trata de la cantidad.

MECANISMOS DE SEGURIDAD: Es cualquier dispositivo técnico utilizado para proteger un programa de cómputo contra su copiado, distribución o uso ilícito.

MEGA- (M): Prefijo que significa 1 millón (106). En informática, basada en el sistema binario (en base 2), mega- tiene un valor literal de 1.048.576, que es la potencia de 2 (220) más cercana a un millón.

MEGABYTE: En ordenadores o computadoras, tiene un valor de un millón de bytes o 1.048.576 bytes (220).

MICROPROCESADOR: Circuito electrónico que actúa como unidad central de proceso de un ordenador, proporcionando el control de las operaciones de cálculo. Los microprocesadores también se utilizan en otros sistemas informáticos avanzados, como impresoras, automóviles o aviones. En 1995 se produjeron unos 4.000 millones de microprocesadores en todo el mundo.

MICROSOFT: Fundada en 1975, Microsoft (Nasdaq "MSFT") es líder mundial en software para cómputo personal y empresarial. La compañía ofrece una amplia gama de productos y servicios diseñados para potenciar las capacidades de la gente por medio del mejor software, en cualquier lugar, en todo momento y con cualquier dispositivo.

MODEM: Equipo utilizado para la comunicación de computadoras a través de líneas analógicas de transmisión de datos. El módem convierte las señales digitales del emisor en otras analógicas susceptibles de ser enviadas por teléfono.

MONITOR: Elemento hardware que está constituido básicamente por un tubo de rayos catódicos, más sus conexiones a la CPU y dispositivos de encendido y apagado, controles de imagen, pantalla-display, etc. Los hay de muy diferentes tamaños y diseños. Su operación está gobernada por el sistema operativo.

Pantalla de visualización que se usa para presentar la salida de un computador, una cámara, una videograbadora u otro generador de video. La claridad del monitor se basa en el ancho de banda del video, la densidad de puntos, el índice de regeneración y la convergencia.

MOTOR ELÉCTRICO: Es un sistema basado en las leyes del electromagnetismo básicas, convierte la energía eléctrica en energía mecánica. Además es un sistema reversible.

MP3: Es un formato de archivo de sonido que tiene una alta calidad y con un tamaño muy reducido. Para poder reproducirlo hay que utilizar un ordenador.

El truco del MP3 radica en la compresión de datos, que reduce el espacio necesario para almacenar la información sonora. Además se utilizan técnicas muy complejas para eliminar algunos sonidos no perceptibles por el oído humano.

MULTIMEDIA, en informática, forma de presentar información que emplea una combinación de texto, sonido, imágenes, animación y vídeo. Entre las aplicaciones informáticas multimedia más corrientes

figuran juegos, programas de aprendizaje y material de referencia como la presente enciclopedia. La mayoría de las aplicaciones multimedia incluyen asociaciones predefinidas conocidas como hipervínculos, que permiten a los usuarios moverse por la información de modo intuitivo.

NEUROFISIOLOGÍA: Es una especialidad médica que, fundamentada en los conocimientos de las neurociencias básicas, tiene como objetivo la exploración funcional del Sistema Nervioso Central (encéfalo y medula espinal), Periférico (nervios y órganos de los sentidos) y Autonómico (simpático y parasimpático), utilizando tecnología altamente especializada con fines diagnósticos, pronósticos y de orientación terapéutica.

NOTEBOOCK: En Español significa "Agenda Electrónica".

OBRA LITERARIA: Es un libro, volumen, o volúmenes que contienen un trabajo literario completo.

ONDAS RADIOELÉCTRICAS: Son ondas electromagnéticas, que se propagan por el espacio sin guía artificial.

ONLINE: En Español significa en línea.

PÁGINAS WEB: Es un sitio en la Internet que contiene textos, imágenes, sonidos, videos, e incluso, mundos 3D y animación.

PALMTOP: Es un ordenador portátil.

PASSWORDS: En Español significa "Contraseña", siendo ello una medida de seguridad utilizada para limitar el acceso a sistemas informáticos y archivos confidenciales. Una contraseña (password) es una cadena de caracteres que el usuario introduce como código de identificación. El sistema compara este código con una lista almacenada de contraseñas y usuarios autorizados. Si el código es válido, el sistema permitirá el acceso del usuario en aquellos niveles de seguridad que hayan conferidos. Véase

PC: Acrónimo de Personal Computer (ordenador o computadora personal). Dependiendo del contexto, PC suele referirse a la gama de equipos personales de IBM. Por ejemplo, un compatible PC se refiere a un equipo en el cual pueden funcionar los mismos programas que en un PC de IBM. Véase Microcomputadora.

PEDOFILOS. Personas tendientes a la atracción sexual de menores de edad.

PFP: Policía Federal Preventiva./ Organismo encargado de aplicar la justicia en cada uno de los estados de la República.

PROCEDASOR: Es el cerebro de la computadora donde se llevan a cabo todos los cálculos matemáticos necesarios para que los programas funciones como redactar un texto, editar una fotografía o un video o simplemente jugar.

PROCESADOR ÓPTICO: Es el procesamiento que abarca tópicos como el reconocimiento de patrones , restauración de imágenes, holografía generada por la computadora , interconexiones de la computadora, etc.

PROCESADOR DE TEXTOS: Aplicación utilizada para la manipulación de documentos basados en texto. Es el equivalente

electrónico del papel, el bolígrafo, la máquina de escribir, el borrador y el diccionario.

PROCESAMIENTO DE DATOS: Se presenta cuando un procesador de archivos se mantiene un sistema operativo convencional, los registros son almacenados en varios archivos y se escriben diferentes programas de aplicación para extraer y añadir registros a los archivos correspondientes.

PROCESO FINITO: Continuación de una serié de cosas que tienen un fin.

PROGRAMA: Sinónimo de software, el conjunto de instrucciones que ejecuta un ordenador o computadora. El término puede referirse al código fuente original o a la versión ejecutable (en lenguaje máquina) de un componente de software. Cuando se habla de un programa se supone un cierto grado de terminación, o sea, se da por hecho que están presentes todas las instrucciones y archivos necesarios para la interpretación o compilación del programa. Por otro lado, se entiende que un programa ejecutable puede cargarse en un entorno determinado y ejecutarse independientemente de otros programas.

PROGRAMADOR: Persona que escribe y depura programas de ordenador o computadora, es decir, las secuencias de instrucciones, a menudo largas, que determinan el trabajo realizado por una computadora. Dependiendo del tamaño del proyecto y del ámbito de trabajo, un programador puede trabajar solo o formar parte de un equipo, estar implicado en parte o en todo el proceso, desde el diseño hasta la finalización, o escribir todo o parte del programa.

PROGRAMACIÓN: Esta orientada a objetos como un mecanismo de asignar responsabilidad a cada uno de los procesos involucrados. Se revisa asimismo la terminología básica y las técnicas de diseño que surgen o pasan a ocupar un lugar mas visible con esta disciplina.

RADAR: Aparato que permite describir la situación de un cuerpo que no se ve por medio de la emisión de ondas electromagnéticas de altísima frecuencia que pueden ser dirigidas en forma de rayos como los de la luz.

RATÓN O MOUSE: Dispositivo señalador muy común, popularizado gracias a estar incluido en el equipamiento estándar del Apple Macintosh.

REALIDAD VIRTUAL: Sistema que permite a uno o más usuarios ver, moverse y reaccionar en un mundo simulado por ordenador o computadora. Los distintos dispositivos de interfaz permiten al usuario ver, tocar y hasta manipular objetos virtuales. Los mundos virtuales y todo lo que contienen (incluyendo imágenes computerizadas de los participantes) se representan con modelos matemáticos y programas de computadora.

RED: Conjunto de técnicas, conexiones físicas y programas informáticos empleados para conectar dos o más computadoras. Los usuarios de una red pueden compartir ficheros, impresoras y otros recursos, enviar mensajes electrónicos y ejecutar programas en

otros ordenadores. Una red tiene tres niveles de componentes: software de aplicaciones, software de red y hardware de red.

RED DE TELECOMUNICACIONES: Se denomina a la infraestructura encargada del transporte de la información, ya sea por acceso a la red telefónica, telégrafo, radio o televisión.

REFORMA: Periódico que circula en el Distrito Federal.

ROBÓTICA: Es una nueva tecnología, que surgió como tal aproximadamente hacia el año 1960, Podemos contemplar la robótica como una ciencia que aunque se han conseguido grandes avances todavía ofrece un amplio campo para el desarrollo y la innovación y es precisamente este aspecto el que motiva a muchos investigadores y aficionados a los robots a seguir adelante planteando cada vez robots más evolucionados.

SATÉLITES: Son artefactos construidos por el hombre para la exploración del espacio, para las comunicaciones y la observación meteorológica.

SEGURIDAD INFORMÁTICA: Técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados. Estos daños incluyen el mal funcionamiento del hardware, la pérdida física de datos y el acceso a bases de datos por personas no autorizadas. Diversas técnicas sencillas pueden dificultar la delincuencia informática. Por ejemplo, el acceso a información confidencial puede evitarse destruyendo la información impresa, impidiendo que otras personas puedan observar la pantalla del ordenador, manteniendo la información y los

ordenadores bajo llave o retirando de las mesas los documentos sensibles. Sin embargo, impedir los delitos informáticos exige también métodos más complejos.

SERVIDOR: Se presenta cuando una computadora conectada a una red que pone sus recursos a disposición del resto de los integrantes de la red. Suele utilizarse para mantener datos centralizados o para gestionar recursos compartidos. Internet es en último término un conjunto de servidores que proporcionan servicios de transferencia de ficheros, correo electrónico o páginas WEB, entre otros.

SILOGISMO: Operación mental que permite de conocimientos generales obtener conocimientos nuevos sin recurrir a la práctica.

SISTEMA: Es un conjunto de dispositivos que colaboran en la realización de una tarea. En informática, la palabra sistema se utiliza en varios contextos. Una computadora es el sistema formado por su hardware y su sistema operativo. Sistema se refiere también a cualquier colección o combinación de programas, procedimientos, datos y equipamiento utilizado en el procesamiento de información: un sistema de contabilidad, un sistema de facturación y un sistema de gestión de base de datos

SISTEMA DE LOGARITMO: Conjunto de propiedades para resolver ecuaciones trascendentes con una incógnita.

SOFTWARE: Son las instrucciones responsables de que el hardware (la máquina) realice su tarea. Como concepto general, el software puede dividirse en varias categorías basadas en el tipo de trabajo realizado. Las dos categorías primarias de software son los sistemas operativos (software del sistema), que controlan los trabajos del ordenador o computadora, y el software de aplicación,

que dirige las distintas tareas para las que se utilizan las computadoras. Por lo tanto, el software del sistema procesa tareas tan esenciales, aunque a menudo invisibles, como el mantenimiento de los archivos del disco y la administración de la pantalla, mientras que el software de aplicación lleva a cabo tareas de tratamiento de textos, gestión de bases de datos y similares.

SSP FEDERAL: Secretaría de Seguridad Pública Federal. / Secretaria de estado, cuya función es la aplicación de justicia en toda la República.

SUBSTRACCIÓN O RESTA: Halla la diferencia entre dos cantidades.

TARJETA: Término utilizado generalmente para referirse a una placa de circuito impreso o a un adaptador que puede conectarse a un equipo para ampliar su funcionalidad o conferirle nuevas capacidades. Estas tarjetas proporcionan servicios especializados, como compatibilidad con el ratón o mouse y capacidades de módem, que no están incluidas originalmente en el equipo.

TECNOLOGÍA: Término general que se aplica al proceso a través del cual los seres humanos diseñan herramientas y máquinas para incrementar su control y su comprensión del entorno material. El término proviene de las palabras griegas tecné que significa 'arte' u 'oficio', y logos, 'conocimiento' o 'ciencia', área de estudio; por tanto, la tecnología es el estudio o ciencia de los oficios

TECLADO: Conjunto ordenado de teclas de una computadora.

TELECOMUNICACIÓN: Transmisión de palabras, sonidos,

imágenes o datos en forma de impulsos o señales electrónicas o electromagnéticas. Los medios de transmisión incluyen el teléfono (por cable óptico o normal), la radio, la televisión, las microondas y los satélites. En la transmisión de datos, el sector de las telecomunicaciones de crecimiento más rápido, los datos digitalizados se transmiten por cable o por radio.

TUBOS DE VACÍO O VÁLVULAS DE VACÍO: Dispositivos electrónicos que consisten en una cápsula de vacío de acero o de vidrio, con dos o más electrodos entre los cuales pueden moverse libremente los electrones. El diodo de tubo de vacío fue desarrollado por el físico inglés John Ambrose Fleming. Contiene dos electrodos: el cátodo, un filamento caliente o un pequeño tubo de metal caliente que emite electrones a través de emisión termoiónica, y el ánodo, una placa que es el elemento colector de electrones.

TRANSISTOR: En electrónica, es la denominación común para un grupo de componentes electrónicos utilizados como amplificadores u osciladores en sistemas de comunicaciones, control y computación (véase Electrónica).

TRANSMISIÓN DE DATOS: Es la transmisión de información de un lugar a otro, tanto dentro de un ordenador o computadora (por ejemplo, desde una unidad de disco a la memoria de acceso aleatorio), como entre éste y un dispositivo externo (dos ordenadores o un servidor de archivos, o un ordenador perteneciente a una red). La velocidad de transmisión de datos se denomina también coeficiente de transmisión o velocidad de transferencia de datos y suele medirse en bits por segundo.

TRÍODO: Es una válvula electrónica con tres elementos, de ahí el

nombre de tríodo. El primero es el filamento, que al calentarse produce electrones. El segundo es el ánodo, que está cargado positivamente y, por tanto, atrae a los electrones. El tercero es la rejilla que se sitúa entre el filamento y el ánodo.

YAHOO: Popular máquina de búsqueda en Web. / Proveedor de servicios Internet compañía u organización que proporciona acceso a Internet

UNIDAD DE POLICÍA CIBERNÉTICA: Organismo encargado de vigilar y aplicar la justicia ante los delitos cometidos en Internet, usando medios informáticos.

VIRUS (INFORMÁTICA): Programa de ordenador que se reproduce a sí mismo e interfiere con el hardware de una computadora o con su sistema operativo. Los virus están diseñados para reproducirse y evitar su detección. Como cualquier otro programa informático, un virus debe ser ejecutado para que funcione: es decir, el ordenador debe cargar el virus desde la memoria del ordenador y seguir sus instrucciones. Estas instrucciones se conocen como carga activa del virus.

XENOFOBIA: Odio, repugnación u hostilidad hacia los extranjeros.

WEB: El World Wide Web o WWW o W3 o simplemente Web consiste en ofrecer una interfase simple y consistente para acceder a la inmensidad de los recursos de Internet. Es la forma más moderna de ofrecer información. el medio más potente. La información se ofrece en forma de páginas electrónicas y además, permite saltar de un lugar a otro en pos de lo que no interesa. Lo más interesante es que con unas pocas ordenes se puede mover por toda la Internet.

WINDOWS: Nombre común o coloquial de Microsoft Windows, un entorno multitarea dotado de una interfaz gráfica de usuario, que se ejecuta en computadoras diseñadas para MS-DOS. Windows proporciona una interfaz estándar basada en menús desplegables, ventanas en pantalla y un dispositivo señalador como el mouse (ratón). Los programas deben estar especialmente diseñados para aprovechar estas características.

BIBLIOGRAFIA

BIBLIOGRAFÍA

DOCTRINA

1.- **ALCALDE, Eduardo y GARCÍA, Miguel**, Informática Básica. Ed. Mc Graw-Hill. 2ª ed. México. 1998.

2.- **ALTMARK, Daniel, BIELSA, Rafael Antonio,** Informática y Derecho. Aportes de Doctrina Internacional. Ed. Depalma Buenos Aires. 2ª ed. Argentina 1991.

3.- **ANTONAKOS, James L. & MANSFIEL, Kenneth C. Jr.** Programación Estructurada en Computación. . Ed, Prentice Hall. México. 1995.

4.- **AZPILCUETA HERMILIO, Tomás.** Derecho Informático. Ed. Abeledo-Perrot. Argentina 1987.

5.- **BARRY M. Leiner, VINTON G. Cerf, DAVID D. Clark,** y KLEINROCK Leonard, Una breve historia de Internet, 13ª ed. Ed. Planeta, 1997.

6.- **BEEKMAN, GEORGE.** Computación e Informática, Hoy una mirada a la tecnología de mañana. Ed, Adisson Wesley Longman. México. 1983.

7.- **BAUER, F. L.** Secretos Descifrados, Métodos y Máximas

de la Criptologia. 2a ed. Ed. Springer Verlag. 2000.

8.- **BOYCE, Jim.** Conozca y Actualice su PC Guía Ilustrada. Ed, Prentice-Hall. México. 1998.

9.- **CABALLERO, Pino.** Seguridad Informática Técnicas Criptográficas. Ed. Alfaomega GPO EDR. México.1997.

10.- **CORREA, Carlos A.** Competencia y propiedad intelectual en la industria microelectrónica, doc. del Programa Regional de Cooperación en Informática y Microelectrónica (PNUD-UNIDO). Ed. Depalma. Buenos Aires (Argentina), 1988 .

11.- **CORREA, Carlos M., BATTO Hilda N., CZAR DE ZALDUENDO Susana**. "Derecho Informático". E.d Depalma. Buenos Aires. Argentina. 1987

12.- **CREUS, Carlos.** "Derecho Penal". Parte especial, t. I. Ed. Astrea. Buenos- Aires, Argentina. 1990.

13.- **DAVARA, RODRÍGUEZ, Miguel Ángel.** "Derecho Informático. Ed, Aranzadi. 2ª ed. Madrid. España. 1993.

14.- **DE MIGUEL ASENCIO Pedro Alberto.** Derecho Privado de Internet. Ed. Civita. 2ª ed. Madrid. España. 2001.

15.-**DEL PESO Emilio Y FERNÁNDEZ Isabel,** "Auditoria Informática", Un enfoque practico 2ª ed. Alfaomega. España 1994.

16.- **DERRIEN, Yann.** Técnicas de la Auditoria Informática. Ed, Alfaomega GPO EDR. México. 1995.

17.- **DUFF, Tim.** Introducción a la Informática. Ed, Ibero América. México. 1998.

18.- **ERBSHLOE Michael,** "Información de ¿Cómo sobrevivir a los Ciberataques?." Computer World Books. Estados Unidos. 2001.

19.- **FIX FIERRO, HÉCTOR**, Informática y Documentación Jurídica. Ed. Universidad Nacional Autónoma de México. (Colección Instituto de Investigaciones Jurídicas). México. 1993.

20.- **FOURNIER, María de Lourdes**, Computación. Ed, Limusa, 11ª ed. México. 2002.

21.- **GRUN, Ernesto.** Una Visión Sistémica y Cibernética del Derecho (Lexis Nexis). Ed, Abeledo Perrot. Argentina.1995.

22.- **LEVINO, Guillermo,** Introducción a la Computación y a la Programación estructurada Ed, Mc Graw-Hill. México. 1996.

23.- **LOSANO, Mario G.,** Curso de Informática Jurídica. Ed. Tecnos. 3ª ed. Madrid. 1987.

24.- **MEJAN, Luis Manuel C.** El Derecho a la Intimidad y la Informática. 2ª ed. Ed, Porrúa. México. 1996.

25.- **MIR PUIG,S** (Comp.) Delincuencia Informática. Ed, Promociones y Publicaciones Universitarias. España. 1992.

26.- **OROZCO GOMEZ, Javier.** Marco jurídico de los Medios Electrónicos (Colección Biblioteca jurídica Porrúa S. Grande CL.) Ed Porrúa. México. 2001.

27.- **PALAZZI, Pablo Andrés.** Delitos Informáticos. Ed, AD.HOC. Argentina. 2000.

28.- **PALAZZI, Pablo Andrés.** Virus informáticos y Responsabilidad Penal. Ed, AD.HOC. Argentina. 1992.

29.- **PEREZ LUÑO, Antonio Enrique.** Ensayos de Informática Jurídica. 2ª ed. Ed. DIBS Fontamara. (Colección Bib Ética Filos.Dere.y Politi). México. 1996.

30.- **PFAFFENBERGER, Bryan**. "Diccionario para Usuarios de Computadoras e Internet". Ed. Prentice-Hall. Usa. 1999.

31.- **POWER Richard**, "Tangled web" Cuentos del crimen

digital de las sombras del ciberspace . Computer world Books. Estados Unidos. 2001

32.- **RIOS ESTAVILLO, Juan José.** Derecho e Informática en México. Ed, Universidad Nacional Autónoma de México. Serie e/UNAM.. México. 1999.

33.- **ROSCNOHER, Jonathan.** "Ciber Law". The law of the Internet. United States. Computer World Boock 2002.

34.- **SANDERS, Donald.** "Informática Presente y Futuro", México, 3ª ed. Mc Graw-Hill. 1998.

35.- **SCHWARTAU Winn.** "Cybershock". Surviving, Hackers, Phreakers, identy Thieves, Interten terrorists and weapon of mas disruption. Computer world Books. 2002.

36.- **TÉLLEZ VALDÉS, Julio.** Derecho Informático. 2a. ed. México. Ed. Mc Graw- Hill 1996.

37.- **TIZNADOS, Marco Antonio,** "Informática. Ed, Mc Graw-Hill. 2ª Edición, México. 1997.

38.- **ZAVALA, Antelmo.** El impacto social de la informática jurídica en México. Tesis. México. UNAM. 1996.

39.- **ZAVALA ALARDIN, Gonzalo.** La sociedad informatizada

¿Una Nueva Utopía?. Ed. Trillas . México. 1990.

LEGISLACIÓN

1.- **CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS. Ed. PORRUA**. (Colección Códigos y Leyes Porrúa). 23ª Edición México. 2003.

2.- **CÓDIGO PENAL FEDERAL. Ed. Porrúa.** (Colección Codigos y leyes Porrúa) 23ª Edición. México. 2003

3.- **LEY FEDERAL DEL DERECHO DE AUTOR. Ed. Porrúa.** (Colección Códigos y Leyes Porrúa) México. 23ª Edición. 2003.

4.- **LEY DE LAS VÍAS GENERALES DE COMUNICACIÓN.** Ed. Porrúa. (Colección Códigos y Leyes Porrúa) México. 23ª Edición. 2003.

5.- **LEY DE LA POLICIA FEDERAL PREVENTIVA.** Ed. Ediciones Fiscales ISEF. 3ª Edición. México. Enero 2002.

6.- **LEGISLACIÓN PENAL PROCESAL DEL ESTADO DE SINALOA.** Ed. SISTA. ISBN. México. 2003.

7.- **LEY N° 19.223,** Relativa a Delitos Informáticos. Ed.

Jurídica de Chile. Santiago, Chile . 1999.

OTRAS FUENTES DE INFORMACIÓN.

ENCICLOPEDIAS

1.- **DICCIONARIO DE INFORMÁTICA (SM)** SIN AUTOR. Ed. Acento. Colección. Flash. México 2002

2.- **DICCIONARIO ENCICLOPÉDICO EVEREST.** Ed. Everest S.A. México. 1993. Vols. I, II, III, IV Y V.

3.- **ENCICLOPEDIA ENCARTA MICROSOFT 2003.**

4.- **ENCICLOPEDIA EVEREST DE LAS CIENCIAS.** Ed. Everest., S. A. México. 1995.

OTRAS FUENTES DE INFORMACIÓN.
HEMEROGRAFÍA

1.- **AMOROSO FERNÁNDEZ, Yarina**. "La informática como objeto de derecho. Algunas consideraciones acerca de la

protección jurídica en Cuba de los Datos Automatizados" en Revista Cubana de Derecho. Unión Nacional de Juristas de Cuba. No. 1. Habana, Cuba. 1991. P.43.

2.- **ARTEGA S., Alberto.** El delito informático: algunas consideraciones jurídicas penales. Revista de la Facultad de Ciencias Jurídicas y Políticas. No. 68 Año 33. Universidad Central de Venezuela.. 1987. Caracas, Venezuela. P. 125-133.

3.- **FERNÁNDEZ CALVO, Rafael.** El tratamiento de llamado Delito Informático en el proyecto de ley Orgánico del Código Penal: reflexiones y propuestas de la CLI (Comisión de libertades e informática y Derecho. España. 1988. P.1150.

4.- **PÉREZ MIRANDA, Rafael**. Propiedad intelectual y medio ambiente en México (apuntes preliminares). Revista Alegatos. No. 37/38, México, D.F., año 1997/98, Pp. 348-49.

5.- **REFORMA.** Atacan hackers sitio presidencial. No. 3465. México. D.F; Año 10. P. A25. 12 de Julio del 2003.

6.- **SARZANA, Carlos.** Criminalití e tecnologia en Computers Crime. Rassagna Penitenziaria e Criminologia. Nos. 1-2 Año 1. Roma, Italia. 1988. P.53.

OTRAS FUENTES DE INFORMACIÓN.
INTERNET

1.- http://amiac.org.mx. "ACADEMIA MEXICANA DE INFORMÁTICA, A.C." Cifras de la AMIAC sobre Hackers que Interfieren 835 sitios Mexicanos en el 2002. **Lunes 10/0303 23:42 p.m**

2.- http://www.alertra.com/ "ALERTRA WEB SITE MONITORING." Get Notified Anytime Your Website Goes Down!. **Miércoles 30/04/03 21:30 p.m**

3.- http://altavista.com/ "TRADUCCIÓN DE INGLES A ESPAÑOL" Lunes 01/07/03 7:30 a.m

4.- http://cyberatlas.internet.com/ THE WORLD'S ONLINE POPULATIONS. Relación de países con acceso a Internet. Miércoles 10/04/03. 13:15 p.m.

5.- http://www.derechosinfancia.org.mx/ediac/.htm "LOS ESPACIOS DE DESARROLLO INTEGRAL". Actividades de la Policía Cibernética. Miércoles 02/07/03 15:30 p.m

6.- http://www.studiocelentano.it/codici/cp/codicepenale.htm "CODICE PENALE". Libro Secondo. DEI DELITTI IN PARTICOLARE. Titoli VIII e XIII. **Lunes 03/03/03 21:30 pm**

7.- http://www.nii.ac.jp/sokuho/articles/ncid/.html

法學論叢 (Kyoto- Law Review) / 京都帝國大學法科大學

Domingo. 26/01/03 17:08 p.m

8.http://www.usdoj.gov/criminal/cybercrime/compcrime.html

"COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION CCIPS" Lunes 03/03/03 19:32 p.m

9.- http://mx.yahoo.com/ "NOTICIAS." Funciones del DC México. Miércoles. 21/01/03 21:30 p.m